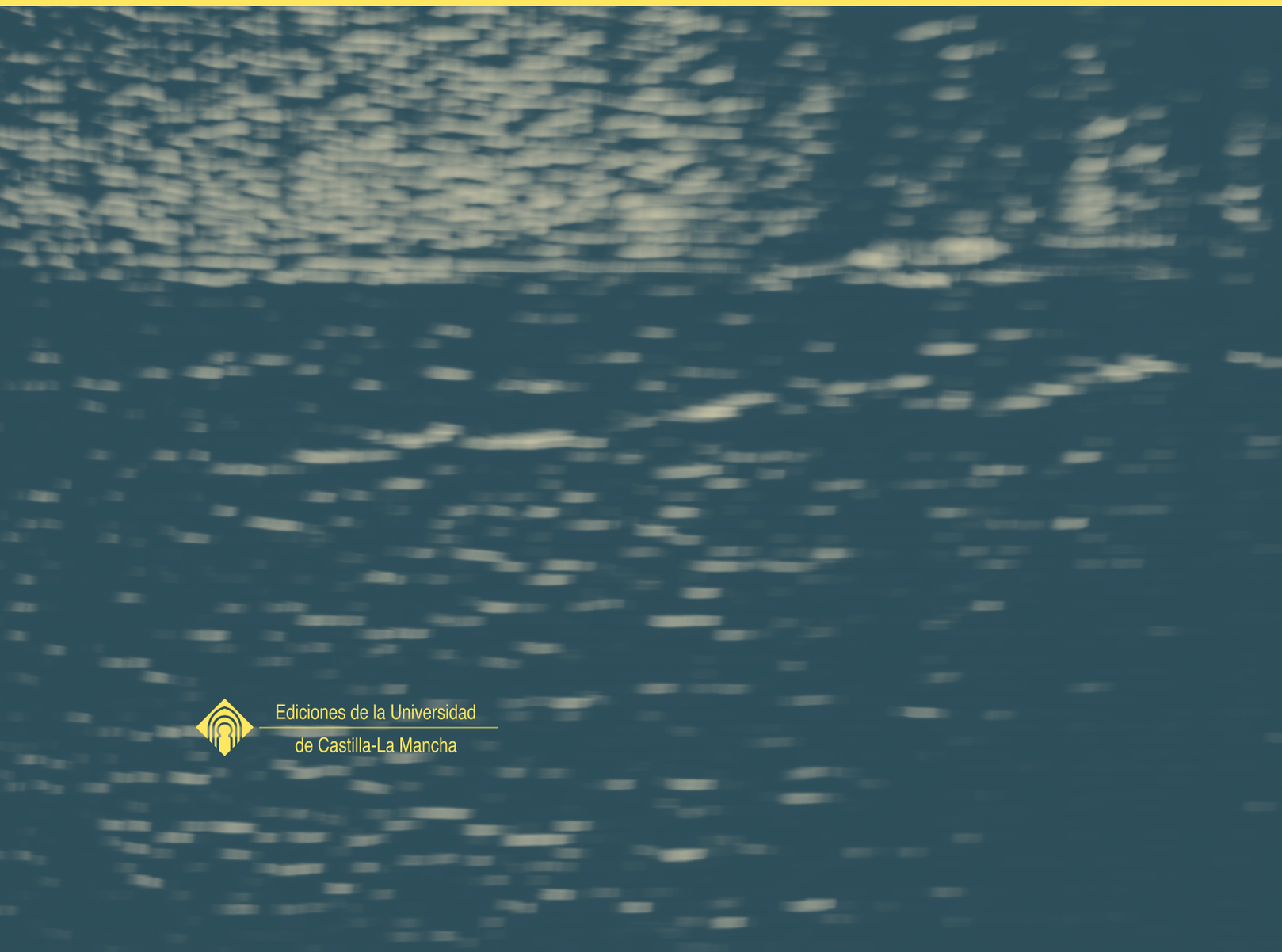
Ciberseguridad y Comunicación

Guía para una comunicación segura

Juan Ignacio Cantero de Julián (coord.)



Ediciones de la Universidad de Castilla-La Mancha

Edita: Ediciones de la Universidad de Castilla-La Mancha.

Colección DIVULGATIO n.º 6.

Diseño de cubierta: CIDI (UCLM).

Esta editorial es miembro de la UNE, lo que garantiza la difusión
y comercialización de sus publicaciones a nivel nacional e internacional.

ISSN: 2697-0759
I.S.B.N.: 978-84-9044-461-0 (Edición electrónica)
D.O.I.: http://doi.org/10.18239/divulga_2021.06.00

Esta actividad ha recibido una subvención de la Secretaría General de Política de Defensa del Ministerio de Defensa.

Diseño y maquetación: CIDI (UCLM)
Hecho en España (U.E.) – *Made in Spain (E.U.)*

Ciberseguridad y Comunicación

Guía para una comunicación segura

Juan Ignacio Cantero de Julián (coord.)

Ediciones de la Universidad
de Castilla-La Mancha

Índice

Ciberseguridad 2020: la consolidación de la disciplina	7
El porqué de esta guía	9
Normativa actual	11
¿Cómo investigar con datos?	15
El Big Data al servicio de la ciberseguridad	17
Propaganda, emociones y ciberseguridad	18
Relatos transmedia e interferencias híbridas	19
Cómo (des)viralizar la (des)información	20
Fake news, desinformación y fact – checking	21
Ejemplos concretos de fake news	24
¿Cómo saber si una información es fiable?	26
Objetivos de la ciberseguridad	28
Principales amenazas de la ciberseguridad	29
¿Dónde formarse en ciberseguridad?	30
Ciberseguridad 2014 – 2020	31
Los expertos de las jornadas	36
25 ideas de ciberseguridad	37
Recursos y enlaces para mejorar la seguridad y la privacidad	44
Decálogo de ciberseguridad	48
Conceptos útiles en ciberseguridad	49
Los autores	51

Ciberseguridad 2020: la consolidación de la disciplina

Juan Luis Manfredi

La ciberseguridad ha madurado. Tan de golpe, que apenas hemos tenido tiempo para asimilar la génesis, la evolución o las futuras líneas de actuación en la definición e implementación de las políticas públicas. Lejos queda la visión romántica, incluso idealizada, de unos ataques realizados por adolescentes desde el cuarto de casa con una pésima conexión. Hoy tenemos –literalmente- ejércitos de soldados virtuales que toman posiciones, capturan enemigos, contaminan el río con información falsa y se apropian de bienes ajenos. No es tiempo para los juegos de guerra de la generación de *Stranger Things*.

La ciberseguridad es conocimiento, espectáculo y poder, a la manera de la geografía política de Yves Lacoste. En la dinámica interna de los Estados, tiene interés en especial la seguridad electoral, porque representa el corazón de la democracia deliberativa y las sociedades abiertas. El hecho de que se falseen los resultados o bien se manipulen los procesos electorales abre una nueva generación de amenazas a la convivencia.

En la dimensión externa, los efectos se identifican en el rediseño de las fronteras reales y virtuales, en la capacidad de ejecución efectiva de las políticas y las nuevas – o ¿eran viejas? – propagandas. Su éxito reside en que no la reconocemos. Las noticias falsas han alterado nuestra capacidad de análisis, ha dificultado la comprensión de los fenómenos internacionales y ha dinamitado la credibilidad de la prensa como intermediaria autorizada.

La dimensión económica de la ciberseguridad representa un riesgo real de no mercado. Es fuente de conflicto en la manipulación de las divisas mediante operaciones no transparentes. El dinero virtual sirve para financiar el terrorismo global y su persecución es aún más compleja. La «securitización» de la economía desincentiva la innovación y la competencia global.

El tercer eje de estudio afecta a las políticas públicas. La ciberseguridad tiene efectos en la defensa, la salud, las infraestructuras o la competencia. Es necesario dotarse de un nuevo aparato instrumental que con autoridad pública – con criterios de política democrática – consiga los efectos deseados. Es el tiempo de una implementación innovadora, sea a través de la colaboración público y privada, el control de las infraestructuras o la intervención en la elección de las tecnologías. Estamos ante una política de largo alcance que afecta al desarrollo individual y al ejercicio de las libertades.

La ciberseguridad es un territorio que combina el territorio natural, el entorno humano y la dimensión digital. Por eso, es cambiante. Por eso, necesitamos nuevas metodologías que nos permitan avanzar. Por eso, estamos aquí. Es un tiempo maravilloso.

El porqué de esta guía

Todos dependemos cada vez más de internet y la comunicación digital. Esta dependencia de individuos y organizaciones nos hace vulnerables a todo tipo de ataques cibernéticos.

La seguridad cibernética se define como un conjunto de pautas, tecnologías y capacitación que brindan protección a los datos e infraestructuras informáticas y de comunicación digital.

Según los resultados del European Communication Monitor 2020, más de la mitad de los profesionales de la comunicación europeos ya han sufrido ciberataques en sus organizaciones. En general, estos profesionales están implicados en la gestión de problemas de ciberseguridad, pero sólo una minoría tiene asumida la labor de fortalecer la resiliencia de los empleados para hacer frente a este tipo de crisis. Las empresas han ido incorporando diferentes medidas y protocolos y han reforzado sus sistemas de ciberseguridad para proteger tanto su negocio como la reputación de la organización, pero otras muchas compañías aun no cuentan con protocolos concretos de comunicación para responder a ellos.

Los periodistas también se enfrentan al reto de proteger sus comunicaciones en el marco del ejercicio de la profesión. La información y las fuentes pueden verse comprometidas en un mundo donde la vigilancia es cada vez más omnipresente y la privacidad cada vez menos perceptible. Los periodistas han de hacer más seguras sus comunicaciones y protegerse contra ataques que dañen su información digital.

Esta publicación viene a ser un repaso de todo lo expuesto y analizado en el Seminario permanente sobre Ciberseguridad, organizado desde la Facultad de Periodismo de Cuenca y la Facultad de Ciencias Jurídicas y Sociales de Toledo, con el apoyo del Centro de Estudios Europeos «Luis Ortega Álvarez» de la Universidad de Castilla-La Mancha y financiación de la Secretaría General de Política de Defensa del Ministerio de Defensa.

Concebido como espacio de reflexión transdisciplinar, por él han pasado diferentes ponentes para tratar asuntos sobre ciberseguridad, transparencia y periodismo, redes sociales y propaganda, big data, drones y guerras del futuro, guerras virtuales y periodismo internacional y seguridad y ciclos electorales.

Normativa actual

Ana M. López Cepeda

Para asegurar una buena ciberseguridad es imprescindible saber cómo se regula este tema. Conocer la normativa vinculada puede ayudar a proteger a ciudadanos, empresas y otros organismos de los ataques cibernéticos, en la medida de lo posible.

Actualmente, en España existe un **Código de Derecho de la Ciberseguridad**, que está publicado en el BOE (Boletín Oficial del Estado)[1], que nombra las normas más principales que se deben tener en cuenta para la protección del ciberespacio.

A continuación, atendiendo a este Código, cuya última actualización es del 11 de septiembre de 2020, se enumeran la normativa de ciberseguridad más significativa. No obstante, se recomienda consultar el código para ampliar el listado.

Protección de datos

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Seguridad nacional

- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, que regula los principios y organismos clave así como las funciones que deberán desempeñar para la defensa de la Seguridad Nacional.
- Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.
- Decreto 242/1969, de 20 de febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, de 5 de abril sobre Secretos Oficiales.
- Ley 1/2019, de 20 de febrero, de Secretos Empresariales.
- Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional.

Seguridad

- Orden INT/28/2013, de 18 de enero, por la que se desarrolla la estructura orgánica y funciones de los Servicios Centrales y Periféricos de la Dirección General de la Policía. [Inclusión parcial].
- Ley 5/2014, de 4 de abril, de Seguridad Privada.
- Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.

1. https://www.boe.es/legislacion/codigos/codigo.php?id=173_Codigo_de_Derecho_de_la_Ciberseguridad&modo=1

Telecomunicaciones y usuarios

- Real Decreto 381/2015, de 14 de mayo, por el que se establecen medidas contra el tráfico no permitido y el tráfico irregular con fines fraudulentos en comunicaciones electrónicas.
- Real Decreto 1163/2005, de 30 de septiembre, por el que se regula el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico, así como los requisitos y el procedimiento de concesión.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Real Decreto 123/2017, de 24 de febrero, por el que se aprueba el Reglamento sobre el uso del dominio público radioeléctrico.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Ciberdelincuencia

- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [Inclusión parcial].
- Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores. [Inclusión parcial].
- Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. [Inclusión parcial].

Infraestructuras críticas

- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
- Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos.

Equipo de respuesta a incidentes de seguridad

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. [Inclusión parcial].
- Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional.
- Real Decreto 521/2020, de 19 de mayo, por el que se establece la organización básica de las Fuerzas Armadas. [Inclusión parcial].
- Orden DEF/710/2020, de 27 de julio, por la que se desarrolla la organización básica del Estado Mayor de la Defensa. [Inclusión parcial].

Relaciones con la Administración Pública

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. [Inclusión parcial].
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. [Inclusión parcial].

El ciberespacio ha adquirido una gran importancia en los últimos años, relevancia acentuada por la Covid-19, que ha puesto de relieve que la «la transformación digital será un componente esencial de la respuesta de la UE a la crisis económica generada por la pandemia» (Consejo de la UE, 09 de junio de 2020). En este contexto se incrementa la preocupación por la ciberseguridad en el ámbito internacional.
En la UE las principales políticas en torno a esta materia se localizan a principios de la década del 2010. La Comisión Europea publica en 2013 la Estrategia de Ciberseguridad de la UE, en la que se plantean como objetivos reducir el cibercrimen, desarrollar nuevos recursos tecnológicos e industriales para la ciberseguridad y establecer una política internacional para el ciberespacio (Demurtas, 2020).

Este plan se actualiza en 2016 con la aprobación de la Estrategia Global para la Política Exterior y de Seguridad de la UE que señala como prioridades, entre varios objetivos, la lucha contra el terrorismo, la ciberseguridad y la mejora de las comunicaciones estratégicas de la unión. Tal y como señala Demurtas (2020) en este documento, «la ciberseguridad se configura como una política transversal» por lo que «la UE debe fortalecer la cibergobernanza multinivel» a todas sus medidas y actuaciones.

La estrategia se completa con otras políticas como la Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, de 2016 o el Reglamento sobre la Ciberseguridad, de 2019.

En la primera, se considera indispensable la creación por parte de cada Estado miembro de «una estrategia nacional de seguridad de las redes y sistemas de información» (art. 7 Directiva NIS). El reglamento establece un marco para la creación de esquemas europeos de certificación de la ciberseguridad; y consolida los objetivos de la Agencia de la UE para la Ciberseguridad (ENISA).

Este texto, en consonancia con las políticas anteriores señala la necesidad de que los Estados miembros estén respaldados por «un enfoque más global y transversal en lo que se refiere a la creación de ciberresiliencia».

Referencias bibliográficas

Consejo de la UE (09 de junio de 2020). La configuración del futuro digital de Europa.

Conclusiones del Consejo. Recuperado de **https://www.consilium.europa.eu/es/council-eu/**

Demurta, A. (2020). «La evolución normativa de la ciberseguridad en la Unión Europea y su impacto político a nivel de actores, objetivos y recursos». *Revista Análisis Jurídico-Político*, vol. 2, núm. 3, pp. 93-114.

Políticas de la UE sobre ciberseguridad consultadas

COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES. Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro.

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.

Estrategia global para la política exterior y de seguridad de la Unión Europea. Una visión común, una actuación conjunta: una Europa más fuerte, 2016.

REGLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.o 526/2013 («Reglamento sobre la Ciberseguridad»).

¿Cómo investigar con datos?

Según el periodista **Paul Bradshaw**, autor del *Online Journalism Blog*, son cinco las etapas para trabajar periodísticamente con datos:

1. Recojo los datos, ***Scraping***
Se debe saber el formato de los archivos con información y las herramientas que se pueden emplear para conseguirlos. Con un *script* se pueden obtener datos masivos a través del proceso de *scraping*.

Las preguntas que deben hacerse:
- ¿Hay bases de datos sobre el tema? ¿Cómo y para qué fueron hechas? ¿Están en una web oficial o debo hacer un pedido de acceso a la información?
- Si la base está en una web, ¿es descargable o debo hacer *scraping*?
- ¿Cuál es el mejor formato (Excel, CSV, Json) para solicitar una copia de esas bases de datos? Si la información está en PDF o JPG, ¿cómo la paso a un Excel?
- Si debo construir una nueva base, ¿qué variables debo incluir y qué podré demostrar?

2. Depuro y contextualizo, **Limpiar la Data**
Que haya errores de diferente procedencia es muy común (registros duplicados, palabras mal escritas, casillas sin toda la información...). Por ello son necesarias herramientas que identifiquen y resuelvan esos contratiempos (limpiar la data).

Las preguntas que deben hacerse:
- ¿La base de datos está completa? ¿Cuántas líneas de información tiene? ¿Puedo limpiarla con Excel u Open Refine? ¿En qué casos debo hacerlo a mano? ¿En qué caso debo usar gestores con más capacidad, como MongoDB?
- ¿Conozco y entiendo todos los términos, variables y siglas que aparecen en las bases? ¿Son los mismos que los usados en bases similares? ¿Los criterios apuntan al sentido de la pregunta que quiero responder o necesito ver esos mismos datos en sentido inverso?

3. Analizo los hallazgos, **Cruzar bases**
El valor de los hallazgos depende de la calidad de las preguntas y de la combinación de dos o más registros para encontrar coincidencias que revelen información.

Las preguntas que deben hacerse:
- ¿Tienen mis bases de datos un concepto o código común que me permita cruzarlas: DNI, RUC, nombres completos?
- ¿El cruce de las bases de datos muestra tendencias, patrones, procesos evolutivos en un periodo determinado? ¿En qué contexto?
- O, por el contrario, ¿revela comportamientos atípicos? ¿En qué contexto?

4. Verifico los hallazgos, **Metodología**
El periodista de investigación debe ir a los lugares necesarios, entrevistar a las personas involucradas, revisar nuevos documentos para detectar las debilidades y fortalezas de la base de datos.

- Las preguntas que deben hacerse:
- ¿Reflejan los datos la condición real de las personas? ¿Ha variado algo en la vida del aludido, en su salud, estabilidad económica, situación legal o sus vínculos?
- ¿Influye eso en el sentido del hallazgo? ¿Confirma su relevancia, la acentúa o la relativiza?

- ¿Con qué experto puedo validar la metodología del cruce? ¿Es posible que el hallazgo sea correcto, pero admita más de una interpretación?

5. Presento los resultados, **dar forma**
Hay que pensar desde el inicio en la forma más eficiente de presentar los resultados.
Existen librerías como *d3js.org* y repositorios de software como *Github*, con ejemplos que uno puede adaptar a lo que necesita.

Las preguntas que deben hacerse:
- ¿Conviene más una visualización o una aplicación? ¿Cuál aporta al sentido de la historia?
- ¿Cómo debe ser la experiencia del usuario? ¿Qué es lo que el gráfico o la herramienta debe generar en el lector? ¿Qué elementos de mi aplicación o visualización la hacen necesaria para el usuario?
- ¿Es responsiva? ¿Se verá bien en teléfonos móviles y tablets? ¿Se puede compartir? ¿Se puede embeber?

El *Big Data* al servicio de la ciberseguridad

Rubén Ramos Antón

La estadística se concibió como «ciencia del Estado», por el carácter revelador que manifiesta con respecto a cómo se comporta una determinada sociedad. Una herramienta que aspira a disponer de una mirada holística, que ayude a comprender el comportamiento de individuos y colectivos, a interpretar las tendencias sociales y otorgarles un significado, anticipándose incluso a los cambios que se puedan producir en el futuro. La convergencia de esta «ciencia del Estado» con la revolución experimentada por las tecnologías de la información en los últimos años ha supuesto una nueva oportunidad para el conocimiento y la interpretación de la sociedad a través de los datos que esta produce y registra. Este proceso de convergencia se plasma en lo que se ha venido a denominar como Big Data. Esto es, la generación de grandes cantidades de bancos de datos que abordan los asuntos más dispares sobre personas y colectivos.

El desarrollo del Big Data y su puesta en disposición de instituciones públicas, corporaciones privadas e incluso entre la ciudadanía ofrece numerosas oportunidades, pero también provoca grandes interrogantes. Son diversos, también, los aspectos e implicaciones que resulta necesario tener en cuenta sobre su tratamiento y, sobre todo, su custodia.

Por un lado, el Big Data ofrece una oportunidad innegable para interpretar la realidad, ya que la cantidad de datos a nuestra disposición aumenta constantemente, alcanzando prácticamente todos los aspectos de la vida. De ahí se traduce, por ejemplo, el interés que para determinadas disciplinas suscita el tratamiento de esta cantidad ingente de datos, desde la sociología al periodismo, pero también la investigación de mercados.

Un material tan valioso ofrece al mismo tiempo numerosas amenazas e incógnitas, por la forma en la que estos datos pueden ser tratados, los propósitos para los que sirven e incluso sobre el derecho de la ciudadanía para conocer los datos que sobre ella circulan, las entidades que trafican con ellos y la capacidad a gestionarlos, incluyendo la posibilidad de eliminarlos.

Todos estos aspectos suscitan el interés de la investigación académica, para que, desde una mirada crítica, se pueda aportar conocimiento y reflexión que redunde en la seguridad de la ciudadanía ante las amenazas que sobre ella se ciernen.

Propaganda, emociones y ciberseguridad

Juan Luis Manfredi Sánchez

La digitalización ha transformado la estructura de la información global y no solo la periodística, sino cualquier fuente de datos y documentación. La proliferación de plataformas, dispositivos y contenidos ha multiplicado la oferta de contenidos disponibles, al mismo tiempo que la digitalización ha abaratado los costes de creación, producción, distribución y almacenamiento de información periodística, propaganda y contenido de cualquier naturaleza. Oferta y demanda se han retroalimentado hasta el punto de crear un mercado de la propaganda rentable por su audiencia global y la participación activa de bots, trols y otros autómatas (Bradshaw y Howard, 2017).

Este ejército invisible de máquinas de propaganda ha afectado a la deliberación pública, sobre todo en las redes sociales, donde es cada vez más complicado encontrar información fiable. La degradación del espacio público digital ha favorecido la polarización social y, con ella, las posiciones políticas más extremas.

Asimismo, el ataque ordenado contra la credibilidad de las instituciones y las personas que la representan contribuyen a disminuir la confianza social. Ese grupo de personas es amplio: políticos, periodistas, académicos, pensadores o disidentes son «troleados» hasta su expulsión de la esfera digital, de modo que se disminuye la pluralidad de voces para la audiencia.

Se define, pues, esta amenaza a la ciberseguridad como la creación de un entorno de incertidumbre informativa que agita las posiciones políticas más extremas con el ataque deliberado contra las voces independientes o más templadas. Las cámaras de eco o las burbujas informativas delineadas por Pariser (2011) son menos relevantes que el hecho mismo de aglutinar voces para que las «nuestras» parezcan más sensatas. Stroud, Thorson y Young explican que «cuando la gente está inundada por información, aquella que coincide con nuestro interés se percibe como de mayor calidad y es más propicia para ser consumida» (2017: 46).

Esta técnica de desinformación no consiste en la producción de información periodística, sino en la difusión de mensajes basados en la emoción y los valores, como ideas abstractas de un «nosotros» frente a «ellos». La gestión de la propaganda distribuye y crea el marco mental de la realidad a través de la información periodística y de las ficciones.

En el nuevo ecosistema digital, ambas técnicas contribuyen a moldea la percepción de los asuntos internacionales. Del Fresno y Manfredi apuntan a esta técnica de ficción y emotividad en la crisis catalana: «las emociones y los sentimientos son reales, se concluye que los objetivos también son reales y, por lo tanto, las emociones compartidas son importantes. Es decir, la emoción y los sentimientos se equiparan a la verdad y la legalidad. Así es como se fabrica la epistemología, y también la legalidad de la post-verdad» (2018: 1232). No es un asunto menor en la construcción de un relato emocional que persigue la identificación de las audiencias con un banco de valores sociales.

El análisis de la situación arroja un balance negativo, porque es una batalla perdida. As stated by H. Akin Ünver, «Balance of power in computational propaganda – like cyber war- favors the offensive side as costs of defending against such attacks require greater resources and better coordination. Even when the defender is successful (i.e. corrects disinformation quickly), psychological processes of digital information consumption still linger on» (2017:7).

El fenómeno no tiene visos de decrecer, sino antes al contrario la automatización favorece la difusión de contenidos sin importar la precisión o la veracidad. La confusión terminológica (realidad virtual, big data, algoritmos, deep fakes) dificulta el diseño de una estrategia que combata la desinformación desde los poderes públicos con el apoyo de los periodistas, los think tanks, las plataformas y otros instrumentos relevantes para la configuración de la opinión pública.

Relatos transmedia e interferencias híbridas

Luis Mauricio Calvo

Sun Tzu dijo que someter al enemigo sin necesidad de pelear es la mayor habilidad. Esta posibilidad es factible a través de la comunicación. El ciberespacio se ha convertido en un nuevo campo de batalla en el que los oponentes buscan la hegemonía de su relato y la desestabilización social, un terreno donde se puede ganar sin combatir cuerpo a cuerpo.

Las sociedades democráticas se enfrentan a nuevas amenazas en forma de interferencias híbridas –entendidas como el uso coordinado de medios no militares para propiciar la división en una sociedad- en las que la comunicación juega un papel fundamental.

La confluencia de los medios de comunicación tradicionales en un entorno digital con nuevos actores con capacidad de difundir mensajes masivos posibilita la lucha por la supremacía entre diversas visiones de la realidad afines a intereses particulares -de gobiernos, grupos de poder, empresas, colectivos o individuos- que no siempre dejan a las claras sus objetivos En esta zona gris, al margen de las actividades armadas, la intimidación militar o el conflicto abierto, se disputa hoy buena parte del poder geopolítico.

Los relatos son las nuevas unidades de combate. En un entorno hiperconectado, los mensajes se enfrentan buscando la mayor credibilidad y expansión posible con el fin de alinear a la opinión pública alrededor de la particular visión de la realidad de sus emisores. La desinformación es el eje vertebrador de muchas de estas campañas que aprovechan las estrategias narrativas transmedia, que se adaptan al nuevo encorno comunicativo, para lograr la mayor eficiencia.

El problema preocupa a los gobiernos que deben velar por la integridad de los sistemas democráticos, pero también a los ciudadanos. El 83% de los europeos considera que la desinformación, en forma de lo que se han denominado «noticias falsas», es una amenaza a la democracia, según el Flash Eurobarómetro de abril de 2018.

Las sociedades democráticas se enfrentan a un reto de gran magnitud que requiere de un doble frente de actuación: el individual para evitar la manipulación y la difusión y el global para implementar las políticas necesarias para detectar y neutralizar las injerencias orquestadas.

Cómo (Des)viralizar la (Des)información

José María Herranz de la Casa

Internet, las redes sociales y los smartphones se han convertido en las herramientas hegemónicas que aceleran la distribución y socialización de la información. Se ha pasado de la era Gutemberg (Imprenta) a la era Zuckerberg (Facebook), de la era del limitado acceso a la información a la era de la sobreinformación, sin que los ciudadanos hayan aprendido todavía en muchos casos a adaptarse a este nuevo ecosistema (Herranz y Cantero, 2019, 29). En este contexto se confunden las fronteras entre los conceptos de veracidad (artículo 20.1.d de la Constitución española) que se contrapone a engañoso y verdadero que se opone a falso o erróneo (Grijelmo, 2012, 397). Y la consecuencia es que se llega a generar un marco de desinformación donde subsisten sin control las *fake news*, *deep fake*, noticias falsas, bulos y leyendas urbanas. La organización FirstDraft ha desarrollado una serie de guías para explicar el fenómeno y describe tres conceptos relacionados con la desinformación:

- ***Misinformation***: Cuando se comparte la *disinformation* y la persona desconoce que es falsa o engañosa.
- ***Disinformation***: Contenido intencionalmente falso y diseñado para causar daño. Motivado por tres factores distintos: ganar dinero; tener una influencia política; o causar problemas.
- ***Malinformation***: Información que se comparte con la intención de causar daño.

También proporciona una gradación que puede llegar a ser poco dañina y con un objetivo cómico (Noticias de medios como El Mundo Today o Revista Mongolia) hasta fabricar contenidos y noticias falsas con un objetivo claro de engañar. La periodista Carole Cadwalladr investigó la campaña del Brexit y descubrió los resultados de un aluvión de anuncios engañosos de Facebook dirigidos a votantes vulnerables que pudieron decantar la votación final: el caso de Cambridge Analytica. Es por ello que la labor de los periodistas como verificadores de la información cobra mayor relevancia y proyectos como Maldito Bulo o Newtral ponen de manifiesto el trabajo de los periodistas: contrastar la veracidad de la información que manejan para difundirla y dar seguridad informativa a los ciudadanos.

Referencias bibliográficas

Alandente; D. (2019). Fake news: la nueva arma de destrucción masiva. Barcelona: Deusto.

Amores, M. (2018). Fake news. La verdad de las noticias falsas. Barcelona: Plataforma Actual.

FirstDraft (2019) Understanding Information disorder.

Grijelmo, A. (2012). La información del silencio. Cómo se miente contando hechos verdaderos. Madrid: Taurus.

Herranz, J.M. y Cantero, J.I. (2019). El tratamiento informativo de los colectivos vulnerables en los medios de comunicación. ¿Veracidad, desinformación o estereotipos? En E. Gómez (coord.) Imagen, Estigma y Derechos humanos: Claves para abordar la vulnerabilidad y la exclusión social desde el trabajo social y la comunicación, pp. 29-62. Valencia: Editorial Tirant Lo Blanch.

Jiménez, I. (2020). La nueva desinformación. Veinte ensayos breves contra la manipulación. Barcelona: Editorial UOC.
Magallón, R. (2019). Unfaking news. Cómo combatir la desinformación. Madrid: Pirámide.

Fake News, desinformación y *Fact-checking*

Juan Ignacio Cantero de Julián

En Internet ha triunfado la instantaneidad: un campo de cultivo propicio para que se dé un contexto donde mentiras, bulos o rumores tengan más opciones de convertirse en noticia y de propagarse.

La palabra del año del Diccionario Oxford en 2016 fue posverdad y fake news en 2017. Según la terminología inglesa, son las llamadas noticias falsas que definen la información distorsionada que se modifica, y se somete a nuevas interpretaciones para llevar al engaño. Incluso en diciembre de 2017 en España, el Consejo de Ministros aprobaba la «Nueva Estrategia de Seguridad Nacional» para analizar «campañas de desinformación» con la creación de una comisión de expertos y editores.

Las noticias falsas empezaron a sonar con más frecuencia después de que el presidente de EEUU, Donald Trump, utilizara el término durante su campaña electoral para poner en duda la veracidad de las informaciones de algunos medios y periodistas. También jugaron un papel destacado en el referéndum del Brexit, en las presidenciales francesas o en la crisis catalana. Por ejemplo, la injerencia de Cambridge Analytica en las elecciones de EEUU del 2016 y en el referéndum del Brexit gracias a la recopilación de datos y una buena campaña de mercadotecnia.

Tras las elecciones en EEUU y en Francia diferentes estudios han incidido sobre la tendencia en Twitter de que se alberguen millones de usuarios ficticios, activos en momentos muy concretos con el objetivo manipular la opinión pública. Esto lleva a pensar que los bots se utilizan para influir y manipular a la opinión pública en los procesos electorales democráticos.

El contenido –en muchas ocasiones sensacionalista– de las noticias falsas se propaga más rápidamente que una noticia real. La noticia falsa se distribuye como verdadera a pesar de haberse desmentido y circula como la pólvora compartida una y otra vez.

La desinformación en Internet y sobre todo en las redes sociales, se produce principalmente por la interactividad y permeabilidad del entorno digital lo que hace difícil distinguir entre información, rumor, bulo etc.

La necesidad de atajar este problema ha dado lugar al fact-checking, también conocido como verificación de datos, una actividad que aplica técnicas del periodismo de datos para desentrañar errores, ambigüedades, mentiras, falta de rigor o inexactitudes de algunos contenidos publicados en los medios de comunicación. Ejerce por tanto como un filtro que garantiza que los textos periodísticos están contrastados a partir de fuentes fiables y contrastadas.

La desinformación puede partir de la intención política de los Estados, pero también de otros actores con otras motivaciones. Los conceptos de transparencia y privacidad, público y privado se han ido diluyendo y confundiendo y las acciones políticas se llevan a cabo a través de nuevas herramientas más allá de las tradicionales.


FAKE

Fake News

María José Ufarte Ruiz

Las noticias falsas, o fake news según la terminología anglosajona, no constituyen una característica propia y exclusiva del momento actual, sino que han estado presentes a lo largo de la historia de la Comunicación.

Sin embargo, el nuevo ecosistema mediático, caracterizado por ser un contexto de desorden informativo debido a la eclosión de las redes sociales, ha contribuido a la proliferación de este tipo de contenidos, que están producidos con apariencia de informaciones periodísticas, pero que cuentan con datos erróneos, exagerados o manipulados y altos niveles de facticidad y engaño, con el fin de crear nuevas interpretaciones y favorecer intereses ideológicos o económicos.

Como respuesta a esta crisis de confianza, ha emergido la verificación de la información o fact-checking, una práctica periodística basada en la comprobación a posteriori de informaciones publicadas por los medios de comunicación, con el objetivo de contribuir de forma más eficaz a la exigencia de responsabilidad de los representantes públicos y a la mejor información de los ciudadanos, un punto clave para fortalecer la democracia.

Además, esta práctica ha dado lugar a un nuevo perfil profesional: los verificadores de la información o fact-checkers, que se sirven de técnicas de comprobación y herramientas tecnológicas para aclarar y arrojar luz a todas aquellas informaciones construidas de forma no adecuada.

Ejemplos concretos de *Fake News*

Conflicto Ucrania

Durante la crisis de Ucrania en 2014, noticias manipulativas y a menudo totalmente inventadas fueron vertidas desde la televisión rusa y desde páginas web a periódicos locales favorables.

«Una refugiada de Sloviansk recuerda cómo un niño pequeño y la esposa de un miliciano fueron ejecutados frente a ella»

tituló el canal estatal Channel One Russia el 12 de julio de 2014, en medio de la recién estallaba guerra del Donbás (este de Ucrania).

La mujer aseguraba que los soldados ucranianos habían crucificado públicamente a un niño de tres años en frente de su madre, pero todo era mentira. El lugar también fue inventado: dijeron que el ejército acorraló a los residentes locales en la Plaza Lenin, en la ciudad de Sloviansk, pero esa plaza no existe.

A pesar de ello, este episodio tuvo gran alcance y fue reflejado en varios medios de comunicación de masas.

Procés Cataluña

Cuando el Pleno del Parlament aprobó la resolución de Junts pel Sí y la CUP para declarar «Cataluña como Estado independiente en forma de república», iniciar un proceso constituyente y que el Govern desarrollase la ley de transitoriedad jurídica y fundacional de la República.

A raíz de esta noticia, las redes sociales recogieron como numerosos bulos que la cuenta de Twitter @malditobulo se dedicó a desmentir.

«Estonia no ha reconocido la república catalana»

«El Fútbol Club Barcelona no ha felicitado al presidente del Govern tras declarar la independencia, es un tuit de enero de 2016»

«Gambia no ha reconocido a Cataluña como Estado»

Elecciones Estados Unidos

«El Papa Francisco sorprende al mundo y apoya a Donald Trump para la presidencia»

El texto incluso citaba un supuesto comunicado en el que el Papa habría escrito que «necesitamos una América fuerte y libre para mantener un mundo fuerte y libre. (...) EL FBI, al negarse a recomendar que se procesara a la Secretaria Clinton después de admitir que ha quebrado la ley en muchas ocasiones, ha quedado en evidencia como una entidad corrupta». Incluso citaba a «fuentes del Vaticano».

«Wikileaks CONFIRMA que Hillary vendió armas a ISIS... Después dejó caer otra BOMBA»

Según la página, Wikileaks iba a confirmar que Clinton «autorizó el envío de armas fabricadas en Estados Unidos a Qatar, un país sometido a la Hermandad Musulmana y amigo de los rebeldes libios». El propio Julian Assange habría dicho que «había 1.700 correos electrónicos que conectaban a Clinton con Libia, Siria, Al Qaeda e ISIS». Aunque Wikileaks filtró correos electrónicos de Clinton, ninguno decía tal cosa.

«SE ACABÓ: Se ha filtrado un correo electrónico de Clinton sobre ISIS y es peor de lo que todo el mundo imaginaba»

Según Ending the Fed (que coló cuatro temas entre las diez noticias falsas más compartidas, según Buzzfeed), Clinton habría admitido en un correo electrónico que «era la fundadora de ISIS y que además estaba al frente del grupo terrorista».

«Solo tienes que leer la ley: Hillary no puede ejercer ningún cargo público federal»

El texto cita unas declaraciones de un exfiscal general en las que decía que «el uso de un servidor privado para el correo electrónico de su cargo como Secretaria de Estado la invalidaba legalmente para ejercer cargos públicos». Este fiscal rectificó unos días más tarde, cuando se publicó que su interpretación de la ley no era la correcta, tal y como recogió Snopes.

«Aparece muerto en su apartamento el agente del FBI sospechoso de la filtración de los correos electrónicos de Hillary en lo que parece un asesinato y suicidio»

La noticia ya está borrada y toda la web está desactivada y ya no existen sus cuentas ni en Twitter ni en Facebook. «El Denver Guardian -explicaba Snopes- es simplemente una web de noticias falsas que se presenta como la versión online de un diario inexistente».

Crisis COVID-19

«Johnson & Johnson está esparciendo el virus»

El origen del virus está en un mercado de animales vivos de Wuhan, no siendo esparcido por ninguna compañía farmacéutica. El virus se transmite persona a persona a través de gotículas. Además, puede transmitirse si una persona toca una superficie contaminada por el virus.

«El evento 201 simuló el brote de coronavirus de Wuhan»

Estos eventos realizan una simulación con enfermedades que se conoce que potencialmente podrían ser un peligro en el futuro, y en este, se escogió al virus coronavirus. Estos eventos son necesarios y recomendados por la OMS para entrenar la capacidad de respuesta, control y comunicación dentro de las organizaciones de un país para controlar un posible futuro brote de esa enfermedad simulada o cualquier otra.

¿Cómo saber si una información es fiable?

En los últimos tiempos se han desarrollado numerosas acciones que buscan que las personas incrementen su nivel de atención y discernimiento sobre las noticias que reciben, a fin de detectar las fake news y evitar su divulgación.

La **Federación Internacional de Asociaciones e Instituciones de Bibliotecas (IFLA)** publicó un resumen en forma de diagrama para ayudar a las personas a reconocer las noticias falsas. Sus puntos principales son:

1. **Considerar la fuente** (para comprender su misión y propósito).
2. **Leer más allá del titular** (para comprender toda la historia).
3. **Verificar los autores** (para ver si son reales y creíbles).
4. **Evaluar las fuentes de apoyo** (para asegurarse de que apoyan las afirmaciones).
5. **Verificar la fecha de publicación** (para ver si la historia es relevante y está actualizada).
6. **Preguntar si es una broma** (para determinar si está destinado a ser una sátira).
7. **Revisar los propios prejuicios** (para ver si están afectando el juicio).
8. **Preguntar a los expertos** (para obtener la confirmación de personas independientes con conocimientos).

EUROPA PRESS también aporta una serie de indicaciones para no ser engañado al informarse por internet:

1. Páginas web de verificación. Existen varias webs en activo que se dedican sistemáticamente al desmentido y la verificación de noticias que circulan en la red. Entre las que destacan Maldito Bulo y Newtral a nivel nacional. A nivel internacional destacan PolitiFact y AFP Factual.
2. Observar qué URL tiene la noticia. Normalmente las páginas de contenido falso imitan la dirección de páginas reales para no llamar la atención sobre esto, pero se aprecia la diferencia.
3. La fecha de publicación del contenido. Las noticias reales se producen en una hora cercana a los hechos, mientras que muchas noticias falsas son escritas días después de lo ocurrido.
4. Formato y titulares. Las páginas falsas suelen tener diseños poco comunes y titulares muy llamativos, con exclamaciones, algunos con faltas ortográficas.
5. La fotografía de la noticia. Existe una aplicación llamada TinEye que al mostrarle una imagen te dice exactamente cuando y donde fue publicada. En muchas fake news basta con arrastrar la imagen al buscador de Google para descubrir de dónde viene la fotografía. Esto delataría la falsedad de esa publicación.

¿Cómo detectar imágenes y videos manipulados con Photoshop?

A veces para engañar al usuario no hace falta elaborar una noticia entera. En ocasiones produce mucha más confusión una fotografía manipulada de un evento concreto, como si la hubiera sacado una persona con su móvil.

Para descubrir esto existen páginas que permiten analizar fotografía para averiguar si han pasado por Photoshop u otras aplicaciones. Una página para esto es Truepic.

Además, existen una serie de métodos para averiguar a simple vista si una foto ha sido manipulada:

A. La iluminación. Esto es lo más difícil de retocar y a veces prácticamente imposible, sobre todo en fotos relacionadas con un desastre meteorológico o algún hecho similar.

B. Ropa de la gente. La vestimenta de la gente muchas veces no coincide con la época. Por ejemplo, en el caso de un huracán, cuando se falsifican fotos suele verse gente en manga corta.

C. La calidad de la imagen. Hay que tener en cuenta que una muy buena calidad de una foto sacada por un usuario es algo extraño.

FACEBOOK distribuyó un decálogo de claves para identificar contenido falso:

1. **Desconfía de los titulares.** A menudo las noticias falsas tienen titulares llamativos e impactantes en mayúsculas con signos de exclamación.
2. **Examina la URL.** Muchos de los sitios web de noticias falsas imitan fuentes de noticias auténticas con pequeños cambios en la URL. Puedes ir al sitio web para comparar la URL con las fuentes oficiales.
3. **Investiga la fuente de la noticia.** Asegúrate de que la historia provenga de una fuente de confianza y que cuente con una buena reputación por su veracidad.
4. **Presta atención al formato.** Muchas noticias falsas tienen faltas de ortografía o un diseño extraño.
5. **Presta atención a las fotos.** Las noticias falsas suelen contener imágenes o vídeos manipulados. En ocasiones, la foto puede ser auténtica, pero haber sido sacada de contexto.
6. **Revisa las fechas.** Las noticias falsas pueden tener una cronología sin sentido o incluir fechas que han sido alteradas.
7. **Verifica los hechos.** Verifica las fuentes del autor para confirmar que son exactas.
8. **Consulta otras noticias.** Si ninguna otra fuente de noticias informa de la misma historia, es posible que sea falsa.
9. **¿La historia es una broma?** Comprueba si la fuente de la noticia es conocida por sus parodias, y si los detalles de la historia sugieren que se ha escrito con humor.
10. **Algunas historias son falsas de forma intencionada.** Mantén una actitud crítica cuando leas una historia y comparte solo las noticias que pienses que son creíbles.

Objetivos de la ciberseguridad

Las herramientas tecnológicas están sufriendo un crecimiento bestial, sobre todo si se atiende al tipo de sociedad en la que nos encontramos: la de la información.

La Política Nacional de Ciberseguridad tiene como principal objetivo diseñar, implementar y poner en marcha medidas para que los usuarios del ciberespacio naveguen libremente de forma segura.

Los riesgos y amenazas en el ciberespacio son un hecho incuestionable, para lo que se deben adoptar medidas con el fin de minimizar los daños que puedan ocasionar, es decir, sistemas actualizados de ciberseguridad.

De manera esquemática se puede afirmar que los objetivos de la ciberseguridad giran alrededor de:

- Promover la seguridad y libertad de las personas en el ciberespacio
- Potenciar la prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las amenazas en el ciberespacio
- Sensibilizar a los ciudadanos, profesionales y empresas de los riesgos derivados del ciberespacio
- Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas necesarias para garantizar la seguridad en el entorno digital
- Transformar la ciberseguridad en cultura: es un problema de todos
- Impulsar la seguridad de los sistemas de información y comunicación
- Evaluar la necesidad de contar con especialistas en seguridad
- Proporcionar recursos para combatir la desinformación y las fake news
- Fomentar la alfabetización mediática de la sociedad para conseguir una ciudadanía digital
- Proteger la privacidad e identidad digital de virus, fraudes y bulos

Principales amenazas de la ciberseguridad

La ciberseguridad está presente en todos lados. Son muchas las amenazas que giran en torno a una organización y todas sus redes, comprometiendo la información y los datos que están archivados en sus dispositivos. Los riesgos están por doquier: desde abrir el correo electrónico o un mensaje de WhatsApp, sacar dinero en un cajero automático hasta en los sistemas de climatización de una empresa.

El siguiente listado es una simple recopilación de las amenazas más comunes a las que tiene que hacer frente la ciberseguridad:

- **Amenazas móviles**
  Fallos en los sistemas operativos de smartphones y tablets, lo que ayuda la proliferación de ataques Man-in-the-Middle, puntos de acceso falsificados (a menudo desde redes abiertas de WiFi) y malware (especialmente el bancario).

- ***Ramsomware y malware***
  Es una fuente fácil de ingresos para los delincuentes que sirve como camuflaje para ocultar propósitos más destructivos en ataques como el conocido WannaCry.

- ***Phising***
  Se aprovechan de las debilidades humanas, ya que al fin y al cabo no existe industria, gobierno o sector privado inmune a la manipulación del comportamiento humano.

- **El *Cloud***
  Cada día son más las empresas que migran sus datos a la nube y también muchos particulares que usan servicios de este tipo. Aunque la seguridad es alta, los criminales saben que es un lugar en el que pueden obtener beneficios y por ello intentan acceder a la información alojada en la nube.

- **Ataques a cajeros automáticos**
  Una sofisticada tecnología de skimming conducirá al alza en ataques de cajeros automáticos, por lo que se espera que cada vez existan más incidentes dentro de esta línea.

- **Ataques contra asistentes virtuales**
  Para el próximo año veremos un aumento en ataques hacia dispositivos IoT y asistentes IA del hogar. El usuario promedio está al tanto de la posibilidad de un robo de datos, pero desafortunadamente carece de las habilidades para mitigar tales ataques.

- **Infraestructuras críticas**
  Infraestructuras críticas como redes eléctricas, sistemas de acueducto y comunicaciones también están en riesgo. La mayoría de las redes de estas infraestructuras se diseñaron y construyeron antes de que la ciberdelincuencia fuera un problema serio. Se sabe que un ataque de este tipo y escala puede ocurrir.

- **Inteligencia artificial**
  Las mismas técnicas en inteligencia artificial que crean resultados increíbles y de gran utilidad para usuarios y empresas, también son usadas para crear caos y dañar a los demás. A medida que los criminales obtienen más conocimientos del funcionamiento del machine learning, empiezan a modificar su software y técnicas de ataque.

- **Virus auto-propagados**
  Virus como TrickBot, la nueva sensación de los troyanos bancarios, Locky y otros, están causando un gran daño. Estos ataques funcionan muchas veces de manera automática y no dan aviso a los usuarios para que puedan detenerlo.

¿Dónde formarse en ciberseguridad?

Para evitar ser víctimas de ciberataques, es incuestionable la necesidad de formarse adecuadamente en ciberseguridad.

Esto aportará un amplio abanico de medidas aptas para que la información se conserve segura y, además, se eviten ciertas acciones que podrían poner en peligro la seguridad informática.

Es mucha la oferta académica que existe con el objetivo de adquirir competencias en ciberseguridad. El INCIBE (Instituto Nacional de Ciberseguridad) ofrece dos catálogos[2] que se actualizan de manera periódica (la última actualización es de junio de 2020) y que recogen todos los programas formativos que cumplen los requisitos.

El primer catálogo plasma los grados y másteres en ciberseguridad en España, con un total de 4 programas de grados y 72 programas de máster.[3]

El segundo catálogo enumera las instituciones que ofrecen formación en ciberseguridad, con el que reúne 132 centros donde se puede realizar algún estudio en ciberseguridad, en modalidad máster o en otro formato.[4]

2. https://www.incibe.es/catalogos-formacion-ciberseguridad
3. https://www.incibe.es/sites/default/files/paginas/talento/catalogos-formacion/catalogo-masteres_junio_2020.pdf
4. https://www.incibe.es/sites/default/files/paginas/talento/catalogos-formacion/catalogo_instituciones_junio_2020.pdf

Ciberseguridad 2014 - 2020

Ejes temáticos de la Ciberseguridad

- Transparencia, libertad, seguridad, privacidad
- Nuevos contextos: Nuevas guerras, ciberataques, ciberactivismo, ciberseguridad
- Terrorismo. ISIS
- Futuro periodismos y del Ecosistema mediático. Medios de comunicación. Propaganda y Fake news
- Entorno digital. Redes sociales
- Herramientas actualizadas: Realidad Virtual, periodismo de datos, drones. Big Data/Algoritmos
- Guerras virtuales
- La seguridad y los ciclos electorales
- Ciudades y seguridad global

La Facultad de Comunicación de la Universidad de Castilla-La Mancha (antes llamada de Periodismo) y el Centro de Estudios Europeos organizan desde 2014 un seminario sobre ciberseguridad y comunicación.

2014. Ciberseguridad, transparencia y periodismo: la seguridad nacional como servicio público

En su primera edición celebrada en Toledo, el tema fue «Ciberseguridad, transparencia y periodismo: la seguridad nacional como servicio público», en colaboración con el Instituto Español de Estudios Estratégicos del Ministerio de Defensa. La actividad buscaba pensar cómo se concilian los derechos fundamentales de los ciudadanos con la defensa en el ámbito digital para que los estudiantes de Derecho y Periodismo conocieran cuáles son los principales problemas y desafíos de uno de los servicios públicos esenciales, la seguridad nacional.

La conferencia de apertura corría a cargo del Teniente Coronel Ángel Gómez de Agreda, Mando Conjunto de Ciberdefensa, para dibujar el nuevo escenario estratégico. Seguidamente, Cristina Manzano, directora de EsGlobal, Pedro Baños, Coronel del Ejército de Tierra, y Carola García-Calvo, investigadora del Real Instituto Elcano, ofrecían una perspectiva global con particular interés en los asuntos de terrorismo yihadista.

En sesión de tarde, Emilio Guichot, profesor titular de Derecho Administrativo en la Universidad de Sevilla, diseccionaba los pormenores de la transparencia, el actual marco legal y los asuntos de la defensa. Juan Luis Manfredi, profesor de la Facultad de Comunicación y organizador de las jornadas, y David Ramírez, analista principal del Instituto de Estudios Estratégicos debatían sobre los límites de la libertad de expresión y la seguridad digital. Clausuraba Luis Ortega, que fue catedrático de Derecho Administrativo y Magistrado del Tribunal Constitucional hasta su fallecimiento en 2015, que defendía los cimientos de una cultura de la transparencia.

2015. Ciberseguridad, redes sociales y propaganda

La segunda edición de 2015 se trasladó a Cuenca. El objeto de análisis de las jornadas fue el papel que realizan las Fuerzas Armadas en relación con la ciberseguridad y la defensa, los retos informativos para el periodismo internacional y el uso de las redes sociales para la difusión de propaganda.

Abría la jornada de nuevo el Teniente Coronel Gómez de Ágreda, quien explicaba cuál es el estado actual de la ciberseguridad y detallaba los hitos en el desarrollo de la geoestrategia digital. Su visión aunaba las relaciones internacionales, los estudios estratégicos y la seguridad. A continuación, Miguel Ángel Benedicto, periodista con

una sólida trayectoria europea y profesor de relaciones internacionales en la Universidad Europa de Madrid, conversaba con Carola García-Calvo y José Manuel Corrales sobre los nuevos usos de la propaganda internacional. El terrorismo internacional, en especial Daesh, parece haber ocupado las redes sociales mediante la creación de campañas de vídeos y contenidos virales. El reto es saber prevenir, atajar y contrarrestar estas acciones. El tercer acto consistía en un análisis extenso sobre cómo ha evolucionado la libertad de expresión en el mundo, cuando la propaganda, la seguridad, la geoestrategia digital y la información se funden en un plano único.

Por la tarde, el periodista Luis Mauricio Calvo dirigía un taller sobre el activismo digital creado para facilitar la comprensión y la práctica de las campañas de propaganda en la red. José María Herranz de la Casa, profesor de Periodismo, actuaba de facilitador de las dinámicas digitales. Cerraban el curso Isaac Martín Delgado y Juan Luis Manfredi, codirectores de la actividad.

2016. Big data, drones y guerras de futuro

La jornada de 2016 volvió a repetir en Cuenca. El encuentro se presentaba en su tercera edición con el título de «"Big data", drones y las guerras del futuro» e incidía en el conflicto entre libertad y seguridad en un mundo cada vez más amenazado y controlado por los sistemas de información digitales.

Una iniciativa que pretendía promover el debate en torno a los nuevos retos que se ciernen sobre los derechos a la información y a la intimidad, la seguridad o la transparencia en un contexto digitalizado hasta en lo más cotidiano.

En un nuevo contexto en el que elementos como la inteligencia de datos ('big data'), los drones o el internet de las cosas van a provocar un cambio sustancial en las dinámicas de seguridad internacional, los cambios se manifestarán tanto en el campo del periodismo como en el del derecho.

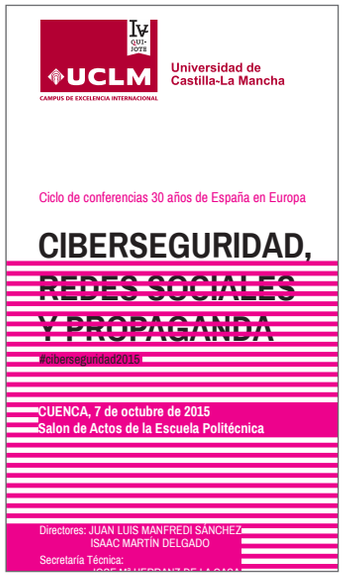
La jornada la abría el teniente coronel del Batallón de Helicópteros de Ataque (BHELA I), Santiago Juan Fernández Ortiz-Repiso, que repasaría el actual panorama estratégico de España. A continuación, Ana Mangas, de la revista Esglobal.com, y el profesor de Derecho Internacional de la UCLM Juan Miguel Ortega Terol, explicaban los efectos de la gestión masiva de información y datos en las relaciones internacionales, profundizando en la seguridad de un mundo post-Snowden. Cerraban la mañana la profesora de la UCLM Ángeles Gutiérrez Zarza, y la autora de Ciberguerra, Yolanda Quintana, en el que señala que el ciberespacio se ha convertido en un campo de batalla para actores estatales y no estatales, un espacio para la propaganda y también para el activismo.

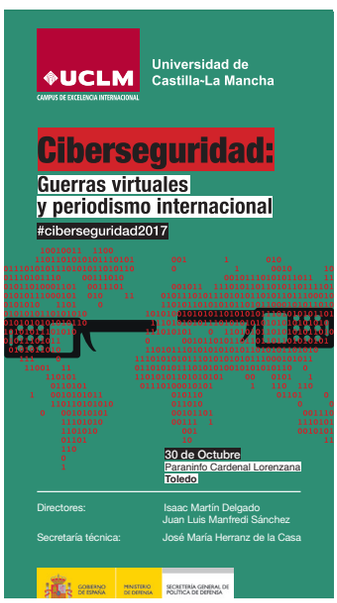
Por la tarde, Javier Talavera, director de la empresa VistaDron, organizaba un taller práctico de utilización de los drones con fines informativos y periodísticos. Cerraba la jornada el profesor Manfredi con una ponencia sobre los efectos en la seguridad internacional de la generalización de lo digital.

2017. Guerras virtuales y periodismo internacional

En 2017, El seminario volvía al Campus de Toledo. La cuarta edición se orientó hacia al auge de la realidad virtual como elemento estructurador de los mensajes periodísticos, la formación, la estrategia y la seguridad internacional.

En perspectiva teórica, existe un intenso debate sobre el carácter bélico o no de las acciones digitales. ¿Son guerras como tales las actividades del entorno digital? ¿Hay víctimas? ¿Qué tipo de derecho rige en el desarrollo de la contienda?





Carteles de las distintas ediciones del seminario de Ciberseguridad y Comunicación

En este contexto estratégico, la organización del seminario perseguía estudiar cuáles son los retos informativos, cuáles son los procesos de transformación de la defensa y cómo afectará el mundo virtual al derecho, el periodismo y la seguridad.

La conferencia inaugural fue dada como en las primeras ediciones por el Teniente Coronel Ángel Gómez de Ágreda, analista del Ministerio de Defensa (especialista en Afganistán y Oriente Medio) quien aportaba una amplia visión sobre la gobernanza global y la ciberseguridad.

A continuación, tendría lugar una mesa redonda que versaba sobre la forma de contar la realidad internacional. Cristina Manzano, de la revista Esglobal.com y Cristina Casabón, especialista en contenidos digitales del World Economic Forum, explicaban la situación del periodismo internacional adaptada al entorno global y digital, las narrativas y las perspectivas de futuro.

Cerraban la mañana Miguel Ángel Benedicto, profesor de relaciones internacionales en la Universidad Europea de Madrid y Juan Miguel Ortega, profesor de derecho internacional público y relaciones internacionales en la Universidad de Castilla-La Mancha. Una mesa redonda sobre las guerras virtuales, sus riesgos y oportunidades en la coyuntura internacional.

Por la tarde, la jornada se articulaba en torno a dos talleres: uno sobre seguridad para periodistas, impartido por Antonio Delgado, profesor en el módulo de datos en el Master de Periodismo de Investigación, Datos y Visualización de Unidad Editorial; y otro sobre realidad virtual e innovación, a cargo de Pavel Sidorenko, doctor en periodismo e investigador en nuevos formatos.

La conferencia de clausura corrió a cargo del organizador de las jornadas y profesor de periodismo en la UCLM, Juan Luis Manfredi, que aportaba las claves a tener en cuenta en el ámbito de la ciberseguridad y el periodismo internacional para 2018.

2019. La seguridad y los ciclos electorales

Tras hacer un parón en 2018, el seminario regresó con su quinta edición: «Ciberseguridad 2019: La seguridad y los ciclos electorales».

Esta Jornada tuvo como objetivos principales conocer el impacto de la ciberseguridad en los procesos electorales y la desinformación que existe en época electoral, enseñando cómo se deben realizar las coberturas periodísticas para evitarla. Las sospechas fundadas de injerencia, el deseo de manipulación o la propia creación de iniciativas digitales internacionales nacidas con el ánimo de influir fuera de las fronteras abren nuevas avenidas de investigación a la ciberseguridad. No se trata, pues, de una cuestión de dispositivos o soportes tecnológicos, sino un asunto que afecta a la seguridad nacional en su dimensión electoral.

En esta ocasión, la celebración fue conjunta en Toledo y Cuenca, haciendo una parte en cada una de las dos ciudades castellanomanchegas. El Congreso contó como habitualmente con la participación de expertos en el mundo de la comunicación y la ciberseguridad, en esta ocasión con dos talleres que enseñaron a los participantes la mejor manera de evitar la desinformación y crear coberturas periodísticas que aporten valor a los ciudadanos.

La Conferencia de apertura: «Desinformación. Un Cambio de paradigma», de la mano de Raúl Magallón –Universidad Carlos III de Madrid-. Tras esta, se realizaba el Taller «Coberturas periodísticas y ciberseguridad en tiempo electoral», impartido por Yolanda Quintana, secretaria general y coordinadora de la Plataforma en Defensa de la Libertad de Información (PDLI). La Jornada terminó con el Taller «Periodismo contra la desinformación electoral», impartido por Juan Luis Manfredi y Juan Ignacio Cantero, ambos de la Universidad de Castilla-La Mancha.

2020. Las ciudades y la seguridad global

El Seminario volvió a celebrarse de formar conjunta y coordinada en Toledo y Cuenca, con cuatro jornadas repartidas en dos y dos entre ambas capitales. Una vez más participaron expertos del mundo de la comunicación y la ciberseguridad, enfocándose las jornadas toledanas a las conferencias y ponencias magistrales y las de Cuenca, a la realización de talleres prácticos y participativos.

El objetivo de esta edición fue el de conocer los cambios profundos que han experimentado las ciudades como territorios estratégicos para poder impulsar transformaciones positivas. La consecución de los principales retos actuales, establecidos en los Objetivos de Desarrollo Sostenible y la Agenda 2030, se concentran en las ciudades.

La internacionalización de las grandes ciudades es la actividad de seguridad y comunicación política que más ha crecido en la última década, como consecuencia de la nueva estructura demográfica, la transformación del poder político y económico, el impacto del cambio climático y el empoderamiento ciudadano. Las ciudades influyen en los asuntos globales tales como las infraestructuras y tecnologías de la información, el turismo, la salud pública y la lucha contra el cambio climático. La ciberseguridad aparece aquí como una cuestión estructural en la gestión urbana.

Muchos son los temas relacionados con la tecnología y la ciudad. La vinculación entre gobernanza de la ciudad, plataformas y tecnologías digitales conduce a la privatización de decisiones basadas en datos (polución, aire limpio, calles seguras, transporte y movilidad), sin considerar otros elementos propios de la política y los valores (apoyo a las minorías, igualdad de oportunidades, igualdad de acceso).

En último término, urge pensar qué rol desempeña la ciudad en la protección de la privacidad. Es en el espacio urbano en que se produce la mayor parte del control de videovigilancia: ¿podrían las ciudades ofrecer un valor añadido a la ciudadanía local mediante la protección superior de sus datos?, ¿habrá ciudades refugio o santuario al margen de las cadenas de vigilancia en red?

La cuestión de la videovigilancia, la creación de industrias de bienes y servicios digitales, el control (improbable) de las fronteras digitales, el impacto de los datos en la vida urbana o la aparición de conflictos en territorio urbano coordinados mediante actividad digital plantean escenarios nuevos para la investigación aplicada en materia de estudios internacionales, seguridad, derecho y periodismo.

La Conferencia de apertura que tuvo lugar en Cuenca el martes 6 de octubre: «Protección de las ciudades Patrimonio de la Humanidad», de la mano de Pablo Muñoz del Olmo, Jefe del servicio de Bomberos y protección civil del Ayuntamiento de Cuenca y Presidente de la Fundación Fuego. Tras esta, se realizaba el Taller «Coberturas periodísticas. La ciberseguridad en el medio radiofónico», impartido por Mariela Rubio, periodista de Cadena Ser y José María Herranz, profesor titular de Periodismo en la UCLM y secretario de las jornadas. Este taller tendría su continuación en el celebrado una semana más tarde, el 13 de octubre, de nuevo en Cuenca. «La ciudad, territorio periodístico. Dinamización de las coberturas periodísticas en asuntos de seguridad y defensa» impartido por Luis Mauricio Calvo y Juan Ignacio Cantero, ambos de la UCLM.

En el paso a Toledo dos días después, el 15 de octubre, abrirían Raquel Jorge (Fulbright Fellow, Elliott School of International Affairs The George Washington University) y Miguel Ángel Benedicto (Universidad Complutense de Madrid) con una charla sobre «Gobernanza de la ciudad digital: agenda y colaboración pública y privada, videovigilancia» para después cerrar con otra sobre «¿Ciudades seguras? El impacto de la tecnología en la seguridad urbana» a cargo de Ana Alonso, periodista de El Independiente y Juan Luis Manfredi, profesor de la UCLM y director de las jornadas.

El último de los ciclos tuvo lugar el 19 de octubre de nuevo en Toledo con la presentación general del panorama estratégico por parte del General Francisco José Dacoba (Director general del Instituto Español de Estudios Estratégicos, IEEE) e Isaac Martín Delgado (UCLM), director de las jornadas y del Centro de Estudios Europeos Luis Ortega Álvarez.

Los expertos de las jornadas

01. **Emilio Guichot Reina**. Doctor en Der. público y profesor de Der. administrativo, U. de Sevilla. Foto: congresotransparencia.com
02. **Luis Ortega Álvarez**. Fue magistrado del Tribunal Constitucional y profesor de la UCLM. Foto: blog.uclm.es
03. **Isaac Martín Delgado**. Director del CEE Luis Ortega Álvarez. Profesor de Der. Administrativo, UCLM. Foto: congresonovagob.com
04. **Juan Luis Manfredi Sánchez**. Profesor de Periodismo, UCLM. Foto: agendapublica.elpais.com
05. **Cristina Manzano**. Directora de la revista Esglobal.com. Foto: esglobal.org
06. **Juan Miguel Ortega Terol**. Profesor de Der. Internacional, UCLM. Foto: m.europapress.es
07. **Yolanda Quintana**. Periodista y autora del libro Ciberguerra. Foto: libertadinformacion.cc
08. **Miguel Ángel Benedicto**. Profesor de Relaciones Internacionales, U. Complutense y U. Europea de Madrid. Foto: navarroreverter.com
09. **Ángel Gómez de Ágreda**. Teniente Coronel del Ejército del Aire. Jefe de Relaciones y Cooperación del Mando Conjunto de Ciberdefensa. Foto: sedianday.es
10. **David Ramírez Morán**. Analista principal del Instituto de Estudios Estratégicos (IEEE). Foto: freelance.tecnoempleo.com
11. **Carola García-Calvo**. Investigadora del Real Instituto Elcano. Foto: laregion.es
12. **Lidia Yanel**. Presidenta de la Federación de Asociaciones de Periodistas de Castilla-La Mancha. Foto: eldigitalcastillalamancha.es
13. **Cristina Casabón**. Especialista en contenidos digitales del *World Economic Forum*. Foto: theobjetive.com
14. **Luis Mauricio Calvo Rubio**. Profesor de Periodismo, UCLM. Foto: uclm.es
15. **Ana Mangas**. Periodista de la revista Esglobal.com. Foto: esglobal.org
16. **Javier Talavera Eslava**. Director de la empresa VistaDron. Foto: observador.uclm.es
17. **Pavel Sidorenko Bautista**. Profesor e investigador en nuevos formatos, U. Francisco de Vitoria. Foto: loft360.wordpress.es
18. **Raúl Magallón Rosa**. Profesor de Periodismo y Comunicación Audiovisual, U. Carlos III de Madrid. Foto: uc3m.academia.edu
19. **Pedro Baños Bajo**. Coronel del Ejército de Tierra especialista en defensa, geoestrategia, seguridad, inteligencia (entre otros). Foto: clubceo.es
20. **José Manuel Corrales Aznar**. Periodista. Foto: observador.uclm.es
21. **José María Herranz de la Casa**. Profesor de Periodismo, UCLM. Foto: twitter.com
22. **Santiago J. Fdez. Ortiz-Repiso**. Teniente Coronel del Batallón de Helicópteros de Ataque (BHELA I) | Foto: observador.uclm.es
23. **Ángeles Gutiérrez Zarza**. Profesora de Der. Procesal, UCLM | Foto: blog.uclm.es
24. **Antonio Delgado**. Periodista de Datadista | Foto: observador.uclm.es
25. **Juan Igancio Cantero de Julián**. Periodista e investigador, UCLM | Foto: twitter.com
26. **Raquel E. Jorge Ricart**. *Fulbright Fellow, Elliott School of International Affairs The George Washington University* | Foto: esiagrad.wordpress.com
27. **Ana Alonso**. Periodista de El independiente | Foto: casamerica.es
28. **Francisco José Dacoba Cerviño**. Director General del Instituto Español de Estudios Estratégicos (IEEE) | Foto: defensa.gob.es
29. **Pablo Muñoz del Olmo**. Jefe de Bomberos y Proteccion Civil en Ayto. Cuenca. Presidente Fundación Fuego | Foto: informacionguadalajara.com
30. **Mariela Rubio**. Periodista de Cadena Ser | Foto: 20minutos.es

25 ideas de ciberseguridad

Transparencia, Libertad, Seguridad y Privacidad

«La desconfianza ha hecho que haya ley de transparencia»

La ley de transparencia se propuso en varios programas electorales de los diferentes partidos, en las elecciones de 2004 y 2008, en 2010 estuvo a punto de aprobarse, sin embargo, en el último momento, el día de antes se retiró del orden del día de Consejo de Ministros. No se consideró tan prioritario, se consideró que no estaba avanzado. No obstante, se aceleró en 2011 con el movimiento del 15M, una de cuyas reivindicaciones fue una ley de transparencia política. El 23 de marzo de 2012 se aprobó el anteproyecto de ley de transparencia pero no solo eso, sino que la presión popular hizo que ese anteproyecto de ley se mejorara y se ampliara. Es decir, que ha sido precisamente la presión social la que ha hecho que haya ley de transparencia y la que ha mejorado la que había elaborado el gobierno.

Emilio Guichot [2014] *https://cutt.ly/SfGTh3Q*

«Instrumentos han existido muchos, el problema es el seguimiento de todos ellos»

Hay muchos mecanismos de transparencia y habría que ver cómo se recogen, porque no solamente a través de la ley de transparencia se obtiene información. También habría que analizar todos los temas, y más en el ámbito de la política, como las comisiones de investigación, el derecho de los parlamentarios a acceder a cierta información e instituciones miles, pero depende de cómo funcionen. El defensor del pueblo tiene derecho a acceder a información de entes locales en función de comportamientos relativos a derechos fundamentales y del funcionamiento de instituciones públicas.

Luis Ortega [2014] *https://cutt.ly/SfGTh3Q*

«Sin transparencia no hay información, y sin información no hay democracia»

La relación entre transparencia y democracia no solo nos permite votar cada cierto tiempo, sino también participar en el proceso de adopción de decisiones. Si quienes gobiernan hacen decisiones desde la opacidad, no sabremos el contenido de las mismas, por lo tanto, no podremos participar en su proceso de adopción.

Isaac Martín [2014] *https://cutt.ly/SfGTh3Q*

«Por la seguridad debemos pagar un precio en libertad individual»

Por defecto, prima la libertad individual y la libertad del ciudadano. Lo que sucede es, que en un entorno como en el que vivimos actualmente, hay numerosos riesgos y amenazas muy claras a la democracia y a la seguridad nacional, y para mantenerlas tenemos que pagar un precio, por ejemplo, la incomodidad en un aeropuerto al tener que quedarnos casi desnudos para pasar un control. Y, aunque es una cosa menor, habría que ver a lo que estamos dispuestos a renunciar. No es un lastre tener que realizar acciones como la anterior, siempre y cuando esa seguridad esté instrumentalizada y rinda cuentas. Sin embargo, no es lo apropiado que el gobierno decida libremente si va a espiar mi teléfono móvil o si luego mis conversaciones van a ir al CNI. Esas explicaciones tendrán que ir a las comisiones de secretos oficiales y que sigan los cauces de la democracia normal y corriente.

Juan Luis Manfredi [2014] *https://cutt.ly/SfGTh3Q*

Nuevos contextos: Nuevas guerras, ciberataques, ciberactivismo y ciberseguridad

«La ciberguerra ha cambiado el campo de batalla»

Los enfrentamientos ahora tienen lugar en el ciberespacio, pero el problema es que el ciberespacio ya no es una esfera aislada, no es una burbuja. Buena parte de los servicios y los productos que utilizamos tienen que ver con el buen funcionamiento del entorno digital, de que tengamos luz eléctrica, o de que funcionen nuestros sistemas de comunicaciones. Lo crítico es que todo está ciberconectado y que el mundo real ya no es una esfera distinta del mundo virtual. La segunda diferencia es que han cambiado los agentes. Los que intervenían hasta ahora eran los ejércitos convencionales, un ejército regular armado. En la ciberguerra hay muchos actores diferentes. Desde luego están los estados con ciberunidades de sus ciberejércitos. También están los ciberterroristas, pero también deben preocuparnos los cibermercenarios, personas con una gran formación técnica y que están al servicio del mejor postor. También los grupos de ciberactivistas que en ocasiones tienen acciones de menor intensidad, pero que también tienen incidencia en el buen funcionamiento del ciberespacio. Y también han cambiado las armas. Ahora mismo para destruir una central nuclear, o para destruir una central eléctrica no hacen falta grandes bombardeos ni una gran explosión. Con vulnerar y atacar sus sistemas informáticos es suficiente.

Yolanda Quintana [2016] *https://cutt.ly/Vf8fmP4*

«El término nuevas guerras hace referencia, más que a los nuevos tipos de conflicto, a las nuevas formas de operar de los actores en conflicto»

Tiene que ver con la propaganda y su visibilidad en un ámbito donde la red está presente en todos los lugares. Se refiere a un fenómeno que ya conocíamos: el de los conflictos olvidados y las nuevas líneas de frente, que tienen que ver con la seguridad cibernética. También tiene que ver con los distintos tráficos que se producen a escala global: tráficos ilegales, muchos de ellos, no solo relacionados con los estupefacientes, también con las armas, con el tráfico de personas o con el de bienes en situación de conflicto. Llamar poderosamente la atención que alguno de estos conflictos se producen en lugares donde hay recursos naturales muy importantes. Y estos recursos naturales no dejan desabastecido el mercado. Ha pasado con el coltán en el Congo, está pasando con el petróleo, los diamantes, el oro y con otro tipo de bienes. Incluso la comida se convierte en un artículo de primera necesidad en la zona de conflicto que se convierte en objeto de tráfico.

Juan Miguel Ortega [2015] *https://cutt.ly/lf8fkaE*

«Estamos posiblemente perdiendo la batalla con el terrorismo por el impacto que está teniendo, y lo que hay detrás puede que no sea tan grande como podría parecer»

Desde el punto de vista de la propaganda, el terrorismo nos está ganando la batalla en dos frentes: en el de transmitir y difundir el terror, tanto por las escenas atroces que ellos difunden desde sus territorios como en lo que sucede aquí, así como en la captación. Las capacidades que hay detrás de todo esto son limitadas; entre otras cosas porque en las sociedades occidentales con nuestra defensa de la libertad de expresión deja-

mos que todo el mundo comunique y transmita como debe ser, y la forma de luchar técnicamente contra todo ese tipo de cuestiones es muy difícil. Primero porque al ser redes transnacionales, es muy difícil combatirlos en un propio territorio y segundo, porque las ramificaciones que tiene son muy complicadas.

Cristina Manzano [2015] *https://cutt.ly/Qf8ffUX*

«Las guerras del futuro son ya guerras del presente»

Las guerras ya no se libran solo en los campos de batalla, ahora mismo hay un tipo de guerras que son más económicas y comerciales e incluso estamos viendo guerras en el ciberespacio a través de las redes sociales y la propaganda. Es lo que se llama la guerra híbrida, esa mezcla de nuevos instrumentos y herramientas para la propaganda.

A las ciberguerras obviamente no les veo ninguna oportunidad, lo único que veo es la posibilidad de poder prevenir desde ya. Todas las empresas, no solo las multinacionales sino cualquier pequeña empresa, puede tener un problema muy grave con un malware o un virus de este tipo. Esta es una amenaza que está a la orden del día. Todos conocemos alguna PYME que ha sufrido un ataque de este estilo y se ha quedado sin información que era muy importante y recobrarla o ha sido imposible y la ha perdido con lo cual el coste es tremendo, o ha tenido que pagar un rescate.

Miguel Ángel Benedicto [2017] *https://cutt.ly/cf8fYNS*

«Nadie está preparado para un ciberataque porque cada día son distintos»

Hay mucha innovación en este campo, entonces nadie está preparado al 100% para un ciberataque. De lo que sí que tenemos que ser capaces es no de resistir esos ataques, sino de ser resilientes, el ser capaces de seguir operando una vez que te han atacado, de recuperarte cuanto antes y recuperar la operatividad cuanto antes. Como hemos visto, depende mucho de las empresas concretas. En general España, por lo menos parte de la administración, está bastante preparada.

Ángel Gómez de Ágreda [2017] *https://cutt.ly/Ef8fCg6*

«El problema de la ciberseguridad es que nunca estamos perfectamente protegidos»

Nuevos sistemas, nuevos software, nuevas aplicaciones, nuevas utilizaciones de los sistemas... El escenario es tan cambiante que tomas todas las medidas preventivas que están en tu mano, pero siempre queda la oportunidad de que alguien se las salte.

David Ramírez [2014] *https://cutt.ly/SfGTh3Q*

Futuro periodismo y del ecosistema mediático. Medios de comunicación. Propaganda y Fake News

«Información que sea clave, de información bien estructurada y de fácil acceso»

Cuando hablamos de libertad de información y hablamos de transparencia y de derechos de acceso, no sólo tenemos que pensar en periodistas cualificados que se dedican profesionalmente a investigar para publicar noticias, tenemos que pensar también en los ciudadanos. Por tanto, ofrecer mucha información puede ser opacidad perfectamente: mucha información irrelevante es anti-transparencia total.

Isaac Martín [2017] *https://cutt.ly/ff5XRCy*

«Ante el exceso de información, periodismo»

El problema que tiene el mundo digital y las redes sociales, que hay un exceso de información y quizás faltan gatekeepers, faltan filtradores de información que hasta ahora siempre han sido los medios tradicionales de los cuales nos fiábamos de su objetividad y veracidad. Tendremos que volver a fiarnos de una serie de empresas informativas que nos pueden ayudar a interpretar ese marasmo de informaciones que tenemos en las redes sociales y que nos sirvan de filtro para discernir entre lo que es veraz y lo que es radicalmente falso.

Miguel Ángel Benedicto [2017] *https://cutt.ly/cf8fYNS*

«Las fake news son lo mejor y lo peor que le ha podido pasar al periodismo»

Es cierto que está afectando a la confianza del público en los medios de comunicación, al discurso democrático, al consumo de información etc., pero por otra parte si los grupos mediáticos saben salir de esta crisis y apostar por un periodismo basado en contenidos de calidad tomándose más en serio las cuestiones de responsabilidad y de regulación de todo el ecosistema de las redes sociales, entonces, bienvenida sea esta crisis.

Cristina Casabón [2017] *https://cutt.ly/df5XKw4*

«La ciberseguridad pretende proteger la información y el periodismo pretende difundir esa información»

En los dos estamos hablando de información, del equilibrio que tiene que haber entre la protección de la información y la difusión de la misma. Yo soy partidario de que la información sea lo más abierta posible, respetando unos ciertos límites, evidentemente, para que tengamos la capacidad para decidir qué parte podemos aprovechar de esa información. Al final, de lo que se trata es que seamos capaces de controlar hasta donde difundimos la información y el Periodismo tiene que ser capaz de hacerlo dentro de los límites que nosotros decidamos, aplicando los criterios de la ciberseguridad; son cosas complementarias.

Ángel Gómez de Ágreda [2014] *https://cutt.ly/SfGTh3Q*

«Interpretar los datos no es manipularlos»

Hay un periodismo de datos que consiste en cotejar muchísimos datos que ahora mismo existen en la sociedad en muchos niveles, pero tú no los puedes ofrecer, los tienes que interpretar. Eso no es una manipulación, eso es lo que ha hecho el periodista desde que el periodismo existe, es decir, yo observo lo que hay en la sociedad, recurro a las fuentes y lo explico. Tú no puedes dar unas cifras estadísticas sin interpretarlas ¿Es una manipulación? No, es una interpretación, pero ahí está la formación que tiene el periodista; si no tiene información suficiente acude al experto que le ayude a interpretar esos datos o esa cantidad de información; eso es trabajo periodístico. El periodista debe dar toda la información y acudir a las fuentes para ofrecer no solamente los datos, sino también contextualizarlos, hacer un background, explicar las consecuencias que puede haber, las causas de dónde proceden, es decir, todo el panorama completo, no solamente darlos.

Lidia Yanel [2014] *https://cutt.ly/SfGTh3Q*

Terrorismo

«La objeción al terrorismo tiene que ser multifacética»

No nos podemos centrar en una sola dimensión y esto quiere decir que no solo es la respuesta policial, o de fuerzas armadas, sino que también tiene que haber respuestas sociales y desde luego, trabajando en la prevención.

Carola García-Calvo [2014] *https://cutt.ly/SfGTh3Q*

«Hay que buscar siempre el equilibrio entre informar y dar propaganda al terrorismo»

Si tú te dejas atrapar en esa red les estás haciendo el juego, pero no puedes dejar de informar. La solución para ello es ir buscando en el día a día el equilibrio permanente. Lo que siempre hay que buscar es una multiplicidad de fuentes y ahí muchas veces fallamos, por la facilidad y rapidez de acceso a las fuentes y por la inmediatez. Esto es uno de los retos que tienen los medios y una de las bases del periodismo: tratar de ofrecer el mayor número de puntos de vista para que así el público pueda tomar sus propias decisiones.

Cristina Manzano [2014] *https://cutt.ly/SfGTh3Q*

Entorno digital. Redes Sociales

«Minusvaloramos la seguridad, firmamos cualquier cosa»

Todos nos damos de alta alegremente en redes sociales, todos firmamos las cláusulas legales del contrato y sin leerlas. Vendemos nuestra vida cuando firmamos un contrato de alta en redes sociales y no nos preocupamos de esto. Pero al revés, cuando queremos regularlo y plasmarlo en una norma tendemos a establecer criterios, límites. Por tanto, regularlo restringiendo la libertad es una paradoja que está ahí.

Isaac Martín [2017] https://cutt.ly/ff5XRCy

«La globalización ha roto totalmente las fronteras con la irrupción de la información al momento y las redes sociales»

Esa ruptura de fronteras y de poder llegar a cualquier sitio del mundo en un segundo puede ser muy buena pero también puede ser una amenaza. Lo que hay que hacer es desarrollar herramientas que permitan afrontar ese problema que se nos viene encima. Para ello hay que tener muy en cuenta en este momento a todas las empresas tecnológicas como Facebook, Twitter, Instagram o Google. Estas empresas multinacionales de la tecnología tienen que ayudar a los estados a luchar contra amenazas como intervenir o falsear elecciones hasta otro tipo de amenazas mucho más graves como la captación del terrorismo yihadista.

Miguel Ángel Benedicto [2017] https://cutt.ly/cf8fYNS

«Monitoreo en tiempo real: la gran virtud del entorno digital»

Poder escuchar y poder monitorizar casi en tiempo real qué se está diciendo de tu marca, qué influencia están teniendo todas tus acciones de comunicación e ir reconfigurando esas estrategias que te has marcado en base a los resultados que vayas obteniendo de medir, esta es una de las grandes virtudes que tiene todo lo digital.

Luis Mauricio Calvo [2015] https://cutt.ly/ngqyVAP

«El mejor antivirus que podemos utilizar es ser conscientes de que cualquier aparato que esté conectado a internet, es una puerta abierta al mundo»

El punto más vulnerable siempre es el usuario porque no estamos concienciados, porque es muy fácil estar en tu cama, en el salón de tu casa tranquilamente con tu portátil o con tu móvil, en cualquier sitio y sentirte invulnerable. Lo que hagamos con las puertas y las ventanas abiertas de nuestra casa es una decisión que tenemos que tomar nosotros, pero la conciencia de que estamos en esa situación, que no estamos en el salón de nuestra casa sino de que estamos en una plaza pública, eso es lo que tenemos que tener a la hora de utilizar los medios tecnológicos.

Ángel Gómez de Ágreda [2015] https://cutt.ly/Ngqy9OY

Herramientas actualizadas: Realidad virtual, periodismo de datos, drones. Big Data/Algoritmos

«Los drones han venido para quedarse»

Llegará el día a día y poco a poco se irá implantando dentro la sociedad el uso de drones con unas medidas de seguridad con unos dispositivos de ayuda para poder utilizar. Es una herramienta que en próximos años será fundamental y va a tener presencia en todos los sectores. El código ético tiene que ser el mismo para una cámara que se cuelga en una grúa, en una cámara al hombre o en un dron.

Javier Talavera [2016] *https://cutt.ly/8fGEaP5*

«El peligro de la esclavitud de los datos»

Hay un peligro de que se «datifique» la realidad y que haya decisiones políticas o de gobernanza que al final terminen estando basadas excesivamente en los datos o en las conclusiones que sacan determinados algoritmos, al final que seamos un poco esclavos de los datos. Que haya un determinismo de datos que se nos quede un poco de lado el criterio humano porque yo creo que con todas las oportunidades que supone se va a necesitar para afrontar esos riesgos que haya un pensamiento humano crítico.

Ana Mangas [2016] *https://cutt.ly/tgqutGR*

«La realidad virtual va a jugar un papel bastante importante»

Vemos como se está librando una batalla digital en la red. Todos los días hay ataques. Ataques de gobiernos contra gobiernos, de empresas contra gobiernos, de empresas contra empresas... hay constantemente una intención de tumbar servidores, de buscar información, robar información, penetrar en los bancos de datos... La realidad virtual lamentablemente plantea un escenario adicional para esta realidad, valga la redundancia, en que nos encontramos donde confluyen estos enfrentamientos.

Pavel Sidorenko [2017] *https://cutt.ly/DfGEfKC*

Seguridad y ciclos electorales

«Se reproducen encuestas falsas y hay muchos actores implicados en generar incertidumbre»

Uno de los problemas que tenemos es que no contamos con una legislación adaptada al contexto digital. Esto significa que en principio no se pueden publicar encuestas electorales durante los últimos cinco días de campaña. Pero si hay algo que sabemos es que esas encuestas están ahí, que se realizan y que los partidos las manejan. Esa información debería ser pública para que todos pudiéramos votar con conocimiento de la situación. Las encuestas pueden hacer que votemos o dejemos votar a determinado partido político.

Raúl Magallón [2019] *https://cutt.ly/dfGEP5w*

Recursos y enlaces para mejorar la seguridad y la privacidad

Libros recomendados

- **Periodismo y ciberseguridad en tiempos de incertidumbre (2020)**.
  Juan Luis Manfredi, María José Ufarte y José María Herranz

  Fruto de los estudios y análisis que se han producido en el seno del Seminario permanente sobre Ciberseguridad en el que confluyen expertos del mundo del derecho, las relaciones internacionales, la comunicación, las fuerzas armadas y la ciencia política en torno a los retos que plantean a la sociedad la «Cultura de la Ciberseguridad». Aspira a sentar las bases de una disciplina de investigación que demandará nuevos modelos de producción social del conocimiento, de interrelaciones sociales y de estudio de las cuestiones internacionales en el nuevo orden post-liberal que se avecina.

- **El pequeño libro rojo del activista en La Red (2015).**
  Marta Peirano

  Tres ciudadanos que decidieron cumplir con su deber civil y acabaron siendo víctimas de una campaña internacional de descrédito personal cuya intención es convencer a los espectadores de que lo importante son las apariencias y no los hechos.

- **El enemigo conoce el sistema (2019).**
  Marta Peirano

  En la era actual de la información, las estructuras del poder se han vuelto invisibles: el poder geopolítico que antes ostentaba el estado se concentra ahora en manos de las redes de comunicación. Google y Facebook ya saben más de ti que la policía. Se discurre sobre este y otros temas como el control y destrucción de los procesos democráticos, el poder de los algoritmos o la militarización del espacio público.

- **Resistencia digital. Manual de seguridad para Smartphones (2019).**
  Críptica

  El Smartphone se está convirtiendo en la herramienta principal con la que nos conectamos con la sociedad. Casi todas las actividades del ser humano se realizan, a día de hoy, a través de una aplicación.
  Deep Web, TOR, FreeNET, I2P, Privacidad y Anonimato, Daniel Echeverry.
  Se exponen el funcionamiento de las principales herramientas para proteger la propia privacidad y consolidar el anonimato en entornos como Internet.

- **Manual del Ciberactivista (2015).**
  Javier De La Cueva

  El lector encontrará en este manual la motivación y el conocimiento necesario para la puesta en práctica y el uso de la web como herramienta para un ejercicio público de sus derechos.

- **Ciberactivismo: Las nuevas revoluciones de las multitudes (2012).**
  Mario Tascón y Yolanda Quintana

  Con la popularización de las redes sociales la gente tiene a su alcance poderosas herramientas para protestar contra los gobiernos, los políticos o las grandes empresas. Cualquiera puede ser un cabecilla o puede apoyar con facilidad un movimiento, la difusión de una idea que comparta o con la que no esté de acuerdo.

- **Datanomics (2019).**
  Paloma Llaneza

  Muestra una radiografía sobre cómo se recaba y se usa nuestra información personal, y de cuáles han sido las consecuencias indeseadas de estos usos.

- **Vigilancia permanente (2019).**
  Edward Snowden

  En 2013, Edward Snowden fue el responsable de la mayor filtración de inteligencia de la historia: reveló que el gobierno estadounidense podía leer cada correo electrónico, escuchar cada llamada y entrometerse en los rincones de la vida privada de todos y cada uno de los ciudadanos del mundo.
  En este libro el autor desgrana por primera vez por qué lo hizo, cómo ayudó a construir un sistema de vigilancia masivo y la crisis de conciencia que le llevó a destaparlo todo y poner en jaque al sistema. Como resultado de aquello, se inició una caza y captura internacional que a día de hoy sigue abierta.

- **#FakeYou (2019).**
  XNet & Simona Levi
  Expone investigaciones que desmontan los mitos en los que se respalda la ola de legislaciones liberticidas que sufrimos en la actualidad. Este libro se plantea como una herramienta de defensa contra los recortes de las libertades fundamentales y un arma contra las nuevas formas de manipulación, mentira y falsificación.

Enlaces web

- **'Fake news' challenges audiences to tell fact from fiction**
  UN News
  https://cutt.ly/LfHejAS

- **Fake news: an insidious tren that's fast becoming a global problema**
  The Guardian
  https://cutt.ly/ofHezfk

- **Disinformation and 'fake news': Interim Report, The Digital, Culture, Media and Sport Committee**
  https://cutt.ly/gfHebde

- **Ciberseguridad, transparencia y periodismo: La Seguridad Nacional como servicio público**
  El Observador de Castilla – La Mancha
  https://cutt.ly/SfGTh3Q

Tutoriales y ayudas para identificar bulos

- **Aprende a reconocer las fake news**
  Internet Segura for Kids (IS4K)
  https://cutt.ly/yfHrPvT

- **¡¡Stop bulos, no alimentes las leyendas urbanas!!**
  Oficina de Seguridad Informática (OSI)
  https://cutt.ly/qfHrGJ7

- **Ponle freno a los fraudes y bulos con buenas prácticas**
  Oficina de Seguridad Informática (OSI)
  https://cutt.ly/afHrVwO

  Consejos para prevenir la propagación de rumores y noticias falsas, WhatsApp https://cutt.ly/zfHr1G3
  Guía para evitar ser manipulados por las fake news, Policía Nacional https://cutt.ly/8fHtqMw

Informes y artículos sobre los bulos del coronavirus

ESCUELA ANDALUZA DE SALUD PÚBLICA (EASP)

- **Fake news y bulos contra la seguridad y la salud durante la crisis del coronavirus**
  Amelia Martín, Manuela López, Nuria Luque y Joan Carles March
  https://cutt.ly/8fCpyuF

EL PROFESIONAL DE LA INFORMACIÓN (EPI)

- **Especial Covid-19 (v. 29, n. 2)**
  https://cutt.ly/9fCpdP3

REVISTA NATURE

- **The epic battle against coronavirus misinformation and conspiracy theories**
  Philip Ball & Amy Maxmen
  https://cutt.ly/0fCpnaV

- **Coronavirus misinformation needs researchers to respond**
  Editorial
  https://cutt.ly/cfCpIyk

Recursos para contrastar los bulos del coronavirus

- **Organización Mundial de la Salud (OMS)**

  Debido a la proliferación de los bulos sobre el Coronavirus la OMS se ha visto obligada a crear una sección en su Web con Consejos para frenar su difusión y aclarar cómo prevenirse ante el virus.
  https://cutt.ly/CfHrqVH

- **Unión Europea (UE)**

  La Comisión Europea con el objetivo de combatir la desinformación promociona un espacio con en el que recomienda al ciudadano que utilice únicamente fuentes autorizadas para obtener información sobre la Covid-19
  https://cutt.ly/vfHrgKn

- **Organización de Consumidores y Usuarios (OCU)**

  La página Web dedica unos consejos para combatir los bulos sobre el virus
  https://cutt.ly/VfHrWF0

Herramientas para evitar que te espíen en internet

- **Tor Project**
  Software gratuito que oculta la dirección de IP de los dispositivos utilizados.
  Permite navegar sin ser detectado ni dejar rastro de sitios visitados o la ubicación geográfica del usuario
  https://www.torproject.org/

- **Cryptocat**
  Servicio de mensajería instantánea privada en la web que puede ser usado desde cualquier navegador y en dispositivos móviles
  https://crypto.cat/

- **Mozilla Thunderbird**
  Programa de correo libre y de código seguro para recibir, enviar y almacenar mensajes electrónicos. Se puede gestionar varias cuentas de correo con un solo programa
  https://www.mozilla.org/en-US/thunderbird/

- **Enigmail**
  Complemento del Thunderbird que permite enviar correos protegidos con claves cifradas. El usuario mantiene su clave. Para usar Enigmail, se debe instalar también GNU Privacy Guard (GnuPG)
  www.enigmail.net

Otros recursos

- **Softwares de almacenamiento de las contraseñas**
  http://keepass.info

- **Servidor de seguridad**
  http://mega.co.nz

- **Encriptación del correo con Firefox o Chrome**
  https://www.mailvelope.com/

- **Electronic Frontier Foundation (EFF)**
  Organización sin ánimo de lucro con el objetivo de conservar los derechos de libertad de expresión y educar a la prensa, legisladores y al público en la actual era digital.
  https://www.eff.org

- **Protección de las comunicaciones en el móvil**
  https://whispersystems.org/

Decálogo de Ciberseguridad

1. **Incrementar** la vigilancia en las redes y los sistemas
2. **Establecer** herramientas que faciliten la monitorización y correlación de eventos (tráfico de red, contraseñas, usuarios remotos)
3. **Adecuar** los permisos de los usuarios a través de una Política de Seguridad Corporativa restrictiva
4. **Consolidar** la configuración de seguridad de todos los componentes de la red corporativa
5. **Incentivar** el uso de redes y sistemas confiables y certificados: acreditados para información sensible o clasificada
6. **Impulsar** la reciprocidad entre organizaciones para intercambiar información de incidentes de seguridad
7. **Promover** la aceptación de la existencia de riesgos en el entorno digital por parte de la Dirección de cualquier organización o institución
8. **Concienciar** a todos los usuarios sobre los riesgos en la red y la necesidad de actuar en consecuencia
9. **Fomentar** las buenas prácticas en el entorno digital ateniéndose a la legislación vigente
10. **Proteger** los activos fundamentales y trabajar como si se estuviese comprometido o amenazado en el entorno virtual

Conceptos útiles en Ciberseguridad

APT (amenaza persistente avanzada). Se refiere a un periodo de ataque donde un intruso (o varios) se implanta de manera ilícita y a largo plazo en una red con el objetivo de conseguir datos muy confidenciales.

Ataques Man-in-the-Middle (MitM). También conocido como ataque de intermediario. Es el proceso mediante el cual un hacker interviene en el intercambio de datos de una comunicación haciendo creer a los usuarios que se están comunicando entre ellos, pero realmente el hacker es el que recibe la información.

Backdoor (puerta trasera). Punto débil de un sistema o programa por donde alguien no autorizado puede acceder al mismo.

Big Data (grandes volúmenes de datos). Se trata de una gran cantidad de datos que son procesados para detectar patrones o hacer predicciones válidas para culminar una toma de decisiones. Se usa para crear modelos predictivos en sectores como la publicidad, análisis de negocio, medicina, lucha contra el crimen o meteorología.

Bitcoin (moneda digital o criptomoneda). Es una moneda que no está controlada ni por el Estado ni por la banca. No se puede falsificar ni tiene intermediarios. Los movimientos son irreversibles (no se pueden anular), pero sí permiten el cambio a otras monedas.

Bot (contracción de robot). Programa que permite el control de un sistema de forma remota sin que el usuario lo conozca o consienta.

Bulo. Noticias falsas reenviadas de forma masiva a través de redes sociales, mensajería instantánea o correo electrónico para extender entre los usuarios la creencia de algo falso.

Chatbot. Hace referencia a una tecnología que permite a un usuario mantener una conversación con un programa informático dentro de una aplicación de mensajería.

Ciberataque. Cualquier acto donde se cometa algún agravio o daño a través de internet comprometiendo la seguridad de la información de una organización.

Ciberentorno. Incluye a los usuarios, dispositivos, redes, procesos e información almacenada que circula directa o indirectamente a través de las redes.

Ciberespionaje. Actividad secreta encaminada a obtener información en el ciberespacio o usándolo como medio.

Ciberdelincuencia. Cualquier actividad donde se emplee internet, una red (privada o pública) o un sistema informático doméstico con la finalidad de destruir o dañar medios electrónicos y redes de internet, es decir, mediante el empleo del ciberespacio.

Ciberseguridad. Engloba los conceptos, políticas, herramientas, métodos, acciones y tecnologías que se pueden emplear para salvaguardar de los riesgos de seguridad a los usuarios del ciberentorno y los activos de una organización.

Ciberterrorismo. Se refiere al uso de distintos medios tecnológicos con el objetivo de crear terror o miedo generalizado en una población, clase dirigente o gobierno, quebrantando así la libre voluntad de las personas.

Cloud (cloud computing, nube de computación o la información en la nube). Es un sistema que permite administrar el contenido de las aplicaciones fácilmente. Permite interactuar con otros usuarios y compartir el contenido que deseemos.

Control parental. Herramientas utilizadas para evitar que los menores de edad realicen un uso indebido de las tecnologías o se expongan a riesgos en la red.

Cookie. Almacenamiento de datos de comportamiento en un sitio web que se registran en el equipo del usuario. Con ellas el sitio web puede consultar la actividad previa del usuario.

DDOS (denial of service, denegación de servicio). Es una forma de ciberataque que afecta a una red corporativa y provoca la pérdida de conectividad para todos los usuarios del sistema. Los ataques DDOS sobrecargan hasta colapsar los recursos de la red de la empresa, provocando la parada y la perdida de conexión con el servicio.

Deep learning (aprendizaje profundo). Técnica para implementar *machine learning* mediante algoritmos. Se trata de máquinas basadas en la actividad del cerebro humano (con neuronas interconectadas), pero son redes neuronales artificiales con capas, conexiones e indicaciones de propagación de datos.

Deep web. Parte de la red de internet con contenido, información y páginas web no indexadas en alguno de los buscadores conocidos.

Hacker. También conocido como pirata informático. Es una persona con grandes conocimientos de informática que se dedica a detectar fallos de seguridad en sistemas informáticos.

Hacktivismo. Es el activismo digital antisocial. Aquellos que lo practican pretenden controlar distintos dispositivos tecnológicos o sitios web para promover su causa o persiguen el control de ordenadores o sitios web para promover su causa, defender su posicionamiento político u obstruir servicios dificultando su uso legítimo.

Huella digital. Rastro de información que el usuario deja en su navegación por la red.

IA (Inteligencia Artificial). Máquinas que han sido creadas exclusivamente para realizar tareas que requieren inteligencia humana.

Infraestructura crítica de información. Instalaciones, redes, servicios y equipos informáticos que, de ser afectados, degradados, obstruidos, interrumpidos o destruidos pueden tener una repercusión crucial en la salud, seguridad, economía o bienestar en los ciudadanos o gobiernos de los Estados.

IoT (Internet of Thinks, el Internet de las Cosas o de las Cosas Conectadas a Internet). Significa que cualquier elemento puede conectarse a internet y aprovecharse de las ventajas que la red ofrece. Se aplica a cualquier elemento al que se le puede incorporar la tecnología y que no es propiamente un dispositivo tecnológico nativo (una nevera, un patinete, una lámpara, el calentador o la cerradura de la puerta).

IP (Internet Protocol). Dirección cifrada en un número único e irrepetible con el que se identifica a un sistema conectado a una red.

Machine learning (aprendizaje automático). Es una rama de la inteligencia artificial que permite que las máquinas aprendan sin ser expresamente programadas para ello.

Malware. Término genérico en el que se incluye cualquier tipo de "malicious software" (software malicioso) que ha sido creado para infiltrarse en dispositivos sin conocimiento del usuario y trabajar en contra de sus intereses.

Metadatos. Conjunto de información relacionada con un documento que enriquece al propio documento al que están asociados.

Phishing. Estafa que tiene como objetivo conseguir datos privados de los usuarios, casi siempre para acceder a sus cuentas o datos bancarios.

Ransomware. Un tipo de malware que infecta mostrando mensajes que exigen el pago de dinero para que se pueda restablecer el funcionamiento del sistema. Puede llegar a bloquear la pantalla o cifrar archivos.

Scraping. Proceso de bajar información de manera automatizada.

Script. Programa simple para bajar información de manera automatizada.

Skimming. Técnica utilizada por ciberdelincuentes para obtener información bancaria y personal de compras online legales.

Spoofing. Suplantación de identidad en la red que se produce o bien a través de un proceso de investigación o bien con el uso de un malware.

Spyware. Tipo de malware que recopila información de un dispositivo y después la envía a otra unidad remota sin que el propietario lo conozca o consienta.

VPN (Virtual Private Network, Red Privada Virtual). Tecnología de red que permite una navegación segura en internet en cuanto a la seguridad de los datos y la protección de la confidencialidad.

Los autores

Juan Ignacio Cantero de Julián

Graduado en Periodismo por la Universidad de Castilla-La Mancha con Máster Oficial en Profesorado de Educación Secundaria Obligatoria, Bachillerato, Formación Profesional y Enseñanza de idiomas también en la Universidad de Castilla-La Mancha.

Actualmente trabaja como periodista en el diario digital El Deporte Conquense, siendo uno de los fundadores y financiadores de este proyecto. Hoy en día imparte clases en el Grado de Periodismo de la Universidad de Castilla-La Mancha, investiga sobre realidad virtual y vídeo 360° y está a punto de defender su tesis doctoral sobre periodismo ambiental.

También ha coordinado el medio digital de la Facultad de Periodismo de Castilla-La Mancha, El Observador y colabora asiduamente en Castilla La Mancha Hoy de CMM.

José María Herranz de la Casa

Decano y profesor titular de la Universidad de Castilla-La Mancha en la Facultad de Comunicación del Campus Cuenca. Imparte las asignaturas de Periodismo Especializado, Deportivo, Político, Teoría del Periodismo y Comunicación Institucional y Corporativa.

Sus trabajos y artículos publicados giran en torno a la comunicación y transparencia en las organizaciones sociales y ONG; la comunicación empresarial y organizacional; la responsabilidad social y los ODS; la innovación, el periodismo especializado y el periodismo inmersivo / realidad virtual.

Además, ha sido periodista en el diario deportivo MARCA, y también ha sido profesor y responsable de comunicación en la Universidad Católica de Ávila (UCAV) y en la Universidad Europea Miguel de Cervantes (UEMC).

Juan Luis Manfredi Sánchez

Profesor titular de Periodismo de la Universidad de Castilla-La Mancha. Doctor en Comunicación por la Universidad de Sevilla. Su tesis recibió una Distinción Especial en el Premio Blas Infante (mejor trabajo para la Administración Pública, 2002), el Primer Premio en los Premios Fundación Autor - SGAE (mejor trabajo en Estudios de Comunicación, 2006) y el Primer Premio RTVA (mejor trabajo en Estudios de Comunicación, 2006).

Es el investigador principal de «La diplomacia pública de las mega-ciudades iberoamericanas: estrategias de comunicación y poder blando para influir en la legislación ambiental global». El proyecto analiza cómo las grandes ciudades participan en la arena internacional mediante herramientas y técnicas de diplomacia pública.

El autor ha publicado más de 30 trabajos académicos sobre innovación, diplomacia y comunicación política internacional. Es titular de la Cátedra Príncipe de Asturias en la Universidad de Georgetown 2021-2022.

Isaac Martín Delgado

Profesor Titular de Derecho Administrativo en la Facultad de Ciencias Jurídicas y Sociales de Toledo (UCLM) y Director del Centro de Estudios Europeos «Luis Ortega Álvarez». Doctor Europeo en Derecho por la Universidad de Bolonia (Italia) y ha realizado estancias de investigación en Cambridge (Reino Unido) y en Bolonia.

Actualmente, sus tres principales líneas de investigación son Administración electrónica, transparencia y Derecho Público Europeo.

Ha dirigido dos proyectos de investigación sobre Administración Pública y Nuevas Tecnologías y, como investigador principal, un relevante Proyecto de Investigación financiado por el Instituto Nacional de Administración Pública sobre «La reforma de la Administración electrónica: una oportunidad para la innovación desde el Derecho», cuyos resultados han sido publicados en un volumen colectivo por parte del INAP.

Universidad de Castilla-La Mancha
Facultad de Ciencias Jurídicas y Sociales de Toledo
Ediciones de la Universidad de Castilla-La Mancha
Facultad de Comunicación Universidad de Castilla-La Mancha
Centro de Estudios Europeos Luis Ortega Álvarez 25 años
Gobierno de España · Ministerio de Defensa · Secretaría General de Política de Defensa