DE LAS OBLIGACIONES VIRTUD

FRANCISCO LÁZARO ANGUÍS
CISO y DPD

El uso intensivo, inmersivo y omnipresente de las tecnologías conocidas como TIC (Tecnologías de la información y las comunicaciones), está generando de forma continua una mayor eficacia y eficiencia en los procesos productivos, transformando sus modelos, facilitando y ampliando las relaciones (tanto sociales, como profesionales), mejorando nuestra calidad de vida (por ejemplo, en el campo de la salud), permitiendo romper con las barreras de las distancias y las diferencias idiomáticas y culturales, entre otros muchos beneficios. Las sociedades modernas (incluyendo a sus ciudadanos, empresas y organismos públicos) se caracterizan por la dependencia de las TIC, de su variedad, complejidad e interdependencia de los sistemas sobre los que realizan la prestación de servicios, suministros y comunicaciones para sustentar su progreso y calidad de vida.

INTRODUCCIÓN: CONTEXTO Y NECESIDAD

Como cualquier Tecnología, paralelamente a estos beneficios el uso de las TIC, conlleva riesgos. Estos Riesgos, se ven incrementados de forma exponencial al requerir que la información fluya por lo que llamamos el ciberespacio o de una forma menos pretenciosa: por Internet. El Riesgo como concepto cuantificable se define de una forma «casi» matemática como Probabilidad x impacto. Es decir, hay mayor Riesgo cuando más probable es que un hecho negativo se materialice y sus consecuencias tengan mayor impacto.

Según el plano de relación en el que nos fijemos, el Ciberespacio, nos acerca a clientes y proveedores, a estudiantes y profesores, a ciudadanos y administraciones, a familiares, pero también a delincuentes, mafias, terroristas, o activistas antisociales, entre otros muchos agentes amenazantes.

Las amenazas en el ciberespacio, las ciberamenazas, junto con el uso intensivo e hiperconectado al que nos referíamos al principio, incrementan la probabilidad de la materialización de acciones negativas y a la vez, a que el impacto sea mayor; lo que nos expone a mayores riesgos. Hace años, sólo podíamos imaginar una vuelta a la edad de las cavernas, por una guerra nuclear entre las dos o tres primeras potencias; era imposible conjeturar que un grupo de personas tuvieran la capacidad de llevar a un país o al mundo entero a ese punto del pasado. Hoy en día, nuestro grado de exposición a las ciberamenazas, las sitúan como la principal amenaza de origen humano junto con la nuclear. La comparación entre ambas se hace más dramática, si cabe, cuando observamos que el factor «Probabilidad» es mayor en las cibera-

menazas pues, la posesión del arsenal destructor se ha extendido y ya no es cosa de dos.

Los Ciberatacantes responden a un abanico de intereses tan amplio que cubren tanto los individuales, como las de los estados y en sus manos está atacar a un objetivo individual (por ejemplo, a un marcapasos o un vehículo conectado de un individuo concreto), a un objetivo selectivo (como una empresa o un sector) o golpear de forma colectiva (por ejemplo, atacando una infraestructura crítica del sector nuclear o del agua). Sus motivaciones cubren también un muy amplio rango de causas que van desde el plano material al inmaterial; por ejemplo, cuestiones económicas, por sentimientos tales como el amor o la venganza a una persona, un ideal o un país. La consecuencia de todo ello es de nuevo el incremento de la Probabilidad y según sea el tamaño del objetivo y su capacidad de resiliencia: el impacto.

Para el año 2020 se espera que estén conectados a Internet entre 20 y 50 mil millones de dispositivos IoT (*Internet of things*), uniéndose a millones de servidores y servicios, tanto del entorno IT como del entorno Operacional o fabril (OT). Los expertos en seguridad de la información (en cualquiera de sus campos: IT, OT e IoT), vaticinan malos tiempos para la sociedad, sino hay un cambio cultural radical en la toma de conciencia de ese riesgo, la asunción de responsabilidades, el acompañamiento de inversiones y la aplicación de medidas (controles) de seguridad de la información, que nos lleven a un mayor control de la tecnología, de su uso y por tanto de sus consecuencias.

La tecnología TIC es cada día más «sexy», pero sus riesgos pueden ser mortales. La proximidad de la tecnología, su orientación a hacernos más cómodo cualquier actividad rutinaria y poco gratificante o a mejorar nuestra calidad o estilo de vida, la hace más y más atractiva. Pero todo ello, también conforma uno de los aspectos esenciales de la transformación del Riesgo TIC que se está produciendo: el salto del «*Security*» al «*Safety*», de la seguridad de los bienes a la seguridad de las personas. Ese salto se produce tanto a escala individual, cómo a nivel colectivo.

Pensemos primero a escala individual y para ello, lo ejemplarizaremos mediante elementos IoT. Estos elementos, en su mayoría de bajo coste hacen que las TIC abandonen las mesas y que por primera vez se pueden vestir, adherir, inyectar, tragar o implantar; es decir, la relación con el cuerpo es directa y en consecuencia también con la vida. Si algún lector del presente artículo juzga que esto es una exageración, no tendrá más que acercarse a las hemerotecas digitales para hallar múltiples referencias a la revisión en el 2017 de 465.000 marcapasos, que se tuvo que llevar a cabo al tenerse la certeza que podían ser atacados (hackeados) remotamente (Beamonte, 2017)

A escala colectiva, son ya varios los casos conocidos y documentados sobre ataques a servicios esenciales; por ejemplo, los ataques sufridos por Ucrania en el 2016 y 2017 afectando a centrales eléctricas, grandes empresas de banca, 'utilities', instituciones públicas y aeropuertos.

La mayoría de esos servicios esenciales se prestan por un conjunto de infraestructuras de gestión pública y privada, que son consideradas críticas porque la interrupción o perturbación severa de su funcionamiento, ocasionaría graves efectos sobre el normal desarrollo de las actividades básicas de la sociedad.

Los estados, desde 1996, pero sobre todo desde el 2004 han ido estableciendo regulaciones y leyes que obliguen a los diferentes actores productivos a considerar la Ciberseguridad como parte esencial de sus servicios. Así, por ejemplo, la Unión Europea materializó su preocupación y su estrategia, primero, en el Programa Europeo de Protección de Infraestructuras Críticas (PEPIC) publicado en el año 2004.

Tanto el legislador europeo como el nacional han convenido establecer Directivas, leyes y regulaciones relacionadas con la Ciberseguridad. No sólo estableciendo la obligación de proteger los activos de información objeto de estas, sino estableciendo expresamente la obligación de notificar las brechas de seguridad, y consecuentemente, la de investigar los incidentes de seguridad.

Todas ellas, en mayor o menor medida coinciden en aspectos tales como: Establecer la autoridad de control, obligación de notificar las brechas de seguridad, tomar las medidas de seguridad apropiadas, el punto de contacto de notificación, rol responsable de aplicar las medidas, etc.

Es cierto, que el grado de coincidencia con estos puntos no es del 100% o que las denominaciones pueden no ser las correctas e incluso que falten conceptos de «primero de ciberseguridad, pero el espíritu común de prevención y reacción está en todas ellas y en lo que la tendencia marca: la ciberseguridad estará presente en todas las grandes regulaciones sectoriales (medicina, transporte, financiera, energéticas, etc..).

Muchas empresas están en el alcance subjetivo de más de una ley, con el mismo o diferente alcance objetivo, por lo que debe afrontar el reto de hacer convivir su aplicación con el mayor grado de eficacia en el cumplimiento y de eficiencia operacional, para que además de responder adecuadamente a la ley, le represente, no ya un hándicap competitivo, sino una garantía de las operaciones de las áreas de Negocio y de las oportunidades de negocio. Estas organizaciones deben ponerse como un objetivo parejo al cumplimiento, hacer de esta obligación un mecanismo de garantía y crecimiento. Este, «hacer virtud de la necesidad», será nuestro objetivo.

REGULACIÓN

Los principales Reglamentos, Directivas y Leyes Europeas y Españolas, que actualmente están vigentes y que

abordan la Ciberseguridad (Ciberseguridad, Seguridad de la información, protección de la información) son:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Vigencia desde el 7 de diciembre de 2018. Deroga la Ley Orgánica a 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Publicada en el BOE num. 298 de 14 de diciembre de 1999.
- 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. Conocido como Reglamento General de Protección de Datos de Carácter personal (en adelante RGPD).
- Real Decreto 3/2010, de 8 de enero, Esquema Nacional de Seguridad en el ámbito de la Administración electrónica (en adelante ENS)
- Ley de Protección de infraestructuras Críticas; Ley 8/2011, de 28 de abril (en adelante LPIC)
- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 de servicios esenciales y Digitales; incorporada al ordenamiento jurídico español a través del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. (en adelante NIS, por sus siglas en inglés *Network and informations Systems*).
- Reglamento (UE) Nº 910/2014 sobre identificación electrónica y servicios de confianza (eIDAS).
- Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE. Conocida como PSD2.

En este listado, el alcance subjetivo (sujetos obligados) y alcance objetivo (materias sobre las que regula; servicios, sistemas o tipo de información a la que aplica), son diferentes, pero como ya hemos dicho una misma empresa puede estar afectada por una o más de una de ellas. En el presente articulo nos centraremos en: RGPD, ENS, LPIC, NIS; es decir, en protección de datos de carácter personal, servicios de la administración y empresas públicas, así como en servicios estratégicos y esenciales. Todas ellas, están en vigor y son plenamente aplicables.

El objetivo (cumplir y mejorar) y las ideas que para ello desarrollaremos en este artículo, pueden ser de aplicación sea cual sea el tamaño de la empresa, siempre que deba hacer convivir las obligaciones de al menos dos de estas regulaciones, con independencia que la empresa debe cumplir con dos, tres o más de estas leyes, reglamentos o Directivas.

Para entender y lograr el objetivo debemos previamente conocer el objeto y alcances de nuestras obligaciones, por eso trataremos de resumirlas, identificándolas en los textos legales, señalando una serie de elementos comunes que permitirán no sólo «sobrellevar la carga» sino «aprovechar el viaje» para mejorar.

Dos aclaraciones, la primera es que, al intentar resumir estas leyes, omitiremos artículos o contenidos que en una extensión mayor deberíamos haber incluido. La segunda es que antes de entrar en materia de alcances, autoridades, exigencias y puntos de encuentro, será desterrar la idea de que este tipo de leyes sólo afecta a organizaciones «grandes»; pues, siendo verdad que el grueso se sitúa en esa dimensión de empresa, hay pequeñas y medianas empresas en número de empleados, o sedes, que sin embargo tratan millones de datos de carácter personal, de la misma forma hay operadores de infraestructura crítica con apenas unas decenas de empleados.

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD)

Leyes y antecedentes

Hasta la llegada del 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 (Reglamento general de protección de datos o RGPD en lo sucesivo) y por el que se deroga la Directiva 95/46/CE, la norma que regulaba esta materia en el ámbito europeo era la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, Directiva de protección de datos). Así, la llegada del RGPD obedece a una razón principal para su aparición, que no es otra que la de armonizar los criterios en cuanto al cumplimiento de protección de datos en todo el entorno de la UE; por este motivo, la norma se traspone como un Reglamento (trasposición directa en la normativa local de cada Estado miembro) frente a la anterior Directiva a la que deroga, que propiciaba un escenario menos homogeneizada al permitir que cada Estado desarrollara su propia normativa nacional en materia de protección de datos, lo que ha dado lugar a aplicaciones dispares en aspectos esenciales entre los distintos países, como es la obtención del consentimientos, los deberes de información o la categorización de las distintas tipologías de datos, por ejemplo.

El RGPD tiene plena y efectiva aplicación desde el 25 de mayo de 2018. Desde dicha fecha y la normativa interna y local de los Estados, derivada de la Directiva de protección de datos, queda derogada y a la espera de nuevas leyes que se adapten al RGPD.

En el caso de España, hasta el 25 de mayo de 2018, eran de aplicación dos normas esenciales en el ámbito de la protección de datos de carácter personal:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD): Esta ley ha venido siendo norma central en España para todo responsable de datos y establecía los criterios básicos y esenciales en cuanto a las obligaciones y principios que debían regir en todo tratamiento de datos.

- 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 (RLOPD): El Reglamento de desarrollo de la LOPD vino a especificar aspectos concretos sobre el cumplimiento a la hora de tratar datos de carácter personal, especificando y detallando elementos concretos como la tramitación de derechos de los titulares y datos y, especialmente, en materia de seguridad, incluyendo la clasificación de 3 niveles de seguridad para los ficheros de datos conforme a una serie de criterios (como la tipología de los datos tratados) y las medidas de seguridad aplicables a cada uno de esos niveles.

Con la irrupción del RGPD, estas normas dejan de tener eficacia y se precisará de una nueva normativa que armonice su contenido a las disposiciones del Reglamento. Actualmente, la nueva LOPD se encuentra en fase de enmienda previa a su futura publicación, previsiblemente para finales de año o principios de 2019. Provisionalmente, el gobierno publicó en fecha de 27 de julio de 2018 el Real Decreto-ley 5/2018, de medidas urgentes de protección de datos, que vino a tratar de paliar la falta de normativa interna en España. Este Real Decreto-ley vino a cubrir ciertos aspectos prioritarios para permitir la aplicación de ciertos aspectos esenciales del RGPD con un mínimo grado de certeza y seguridad, tanto para los Responsables del tratamiento a la hora de cumplir con sus obligaciones, como para la AEPD, como Autoridad de Control, para el ejercicio de sus funciones, como es la actividad sancionadora. Si bien esta norma ostenta una carácter transitorio y no sustitutivo ante la necesidad de una efectiva normativa interna que concrete todos los aspectos necesarios en materia de protección de datos en España.

Alcances: Subjetivo y Objetivo

Seguidamente, se reflejan algunos artículos esenciales del RGPD en cuanto al alcance de la norma:

- Alcance subjetivo del RGPD (art. 3) -referido al ámbito territorial, pero haciendo una expresa mención a los sujetos afectados por el mismo-: El RGPD afecta a toda entidad que trate datos de carácter personal en el ámbito de la UE, independientemente de que el tratamiento se realice o no dentro de la UE. Esto incluye: Responsables o Encargados del tratamiento ubicados en la UE; Responsables o Encargados fuera de la UE que traten datos de carácter personal de ciudadanos de la UE; Responsables o Encargados que, aun estando fuera de la UE, les sea de aplicación la normativa de la UE en virtud del Derecho Internacional Público.

- Alcance objetivo del RGPD (art. 2.1): El RGPD afecta a todo tratamiento de datos de carácter personal, automatizado o no automatizado, contenido o destinado a ser incluido en un fichero (conjunto organizado de datos).

Aspectos de relevancia en materia de seguridad en el articulado

Seguidamente, se reflejan algunos artículos esenciales del RGPD en cuanto al alcance de la norma y las regulaciones específicas que éste establece en materia de seguridad:

- El Responsable del tratamiento (art. 4.7): El RGPD define al Responsable del tratamiento como «la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros determine los fines del tratamiento». Si bien, a nivel conceptual, el RGPD no establece grandes diferencias identificativas para la figura del Responsable del tratamiento respecto a la anterior normativa. No obstante, la aplicación del RGPD someterá al Responsable del tratamiento a un mayor catálogo de deberes de cumplimiento, entre ellos tiene el de la aplicación de los principios de privacidad desde el diseño y por defecto en las actividades del tratamiento que se lleven a cabo en su entidad.

- La AEPD como Autoridad de control (art. 51): Cada Estado designará una o varias autoridades públicas independientes para supervisar el cumplimiento del RGPD. Adicionalmente, el RGPD regula ciertos aspectos específicos relativos a las autoridades de control (artículos 52 hasta 84), entre las que se encuentran; Poderes de investigación y auditoría para investigar y poder cumplir las obligaciones indicadas (art. 58); Gestionar los oportunos procedimientos sancionadores en aplicación a los criterios del RGPD o su normativa de desarrollo (art. 83).

- Nueva metodología de seguridad: Análisis de riesgos (art. 32.2): Entre las novedades del RGPD está la desaparición del deber de notificación a la autoridad de control sobre los ficheros tratados por el Responsable del tratamiento, para ahora pasar a un sistema de tratamiento basado en la responsabilidad proactiva (accountability). Así, será el propio Responsable del tratamiento quien deberá llevar a cabo un registro actualizado de las actividades de tratamiento de su entidad para que, una vez pueda determinar los elemen-

tos inherentes al mismo, lleve a cabo el análisis de los posibles riesgos y, en su caso, las Evaluaciones de Impacto de Protección de Datos cuando este tratamiento implique un alto riesgo para los derechos y libertades de los interesados y aplicar así las oportunas medidas de seguridad que mitiguen estos riesgos. Dichas medidas de seguridad pasan de estar contempladas en un listado «númerus clausus» en el Reglamento de Desarrollo de la LOPD, a tener que aplicar cualquier medida que sea apropiada para garantizar un nivel de seguridad adecuado en función de los riesgos detectados en el análisis previo, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento.

- El deber de notificación de brechas de seguridad y su vía de notificación (Arts. 33 y 34): Otra de las novedades del RGPD en materia de seguridad es la de asumir, por parte del Responsable del tratamiento, el deber de comunicar a la Autoridad de control la producción de cualquier evento (o incidente) respecto al tratamiento de datos personales que ponga en riesgo la seguridad de los datos personales. Este deber de comunicación contemplas una serie de obligaciones como; Recopilar toda la información posible sobre el incidente (alcance, directorios, colectivos de titulares de datos o categorías de datos afectados, por ejemplo); Aplicar las oportunas medidas correctoras o mitigadoras conforme a los oportunos protocolos en materia de seguridad; Informar sobre el mismo a la Autoridad de control en un plazo no superior a 72 horas, Si el incidente entraña riesgos para los derechos y libertades de las personas físicas, deberá comunicar en los mismos términos la producción de la violación de seguridad a los afectados. La AEPD ha establecido un canal electrónico para la notificación de brechas de seguridad.

- El interlocutor/garante del cumplimiento, el Delegado de Protección de Datos (arts. 37 a 39): El RGPD trae consigo una figura relevante a nivel de cumplimiento por parte de los Responsables del tratamiento, a través de la figura del Delegado del Protección de Datos (DPD o DPO).

    - La designación del DPD (art. 37.1) será preceptiva en una serie de supuestos; Cuando el tratamiento sea llevado a cabo por una autoridad u organismo público (salvo Tribunales); Cuando las actividades del tratamiento del responsable entrañen una observación sistemática de interesados a gran escala (como cámaras de videovigilancia); Cuando las actividades del responsable impliquen el tratamiento de categorías especiales de datos a gran escala.

    - La posición del DPD dentro del organización (art. 38) conlleva los siguientes requisitos; El DPD deberá contar con el apoyo y oportuno respaldo de los responsables de la organización y que participe de forma activa en todas las cuestiones relativas a la protección de datos personales; Se garantizará que pueda desempeñar sus funciones con independencia y sin conflicto de intereses; Dispondrá de los oportunos medios por parte del Responsable para llevar a cabo sus funciones.

    - En cuanto a sus funciones (art. 39), el DPO; Deberá informar al Responsable o Encargado sobre sus obligaciones de cumplimiento de la normativa aplicable en materia de protección de datos de carácter personal; Supervisará específicamente el cumplimiento del RGPD y la adecuación a éste de las políticas internas de la compañía.Asesorará en las evaluaciones de impacto, si fuera necesario; Será un interlocutor entre el Responsable y la Autoridad de contro y los interesados titulares de datos personales.

ESQUEMA NACIONAL DE SEGURIDAD

Leyes y antecedentes

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos estableció el Esquema Nacional de Seguridad (en adelante ENS) que, aprobado mediante Real Decreto 3/2010, de 8 de enero, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

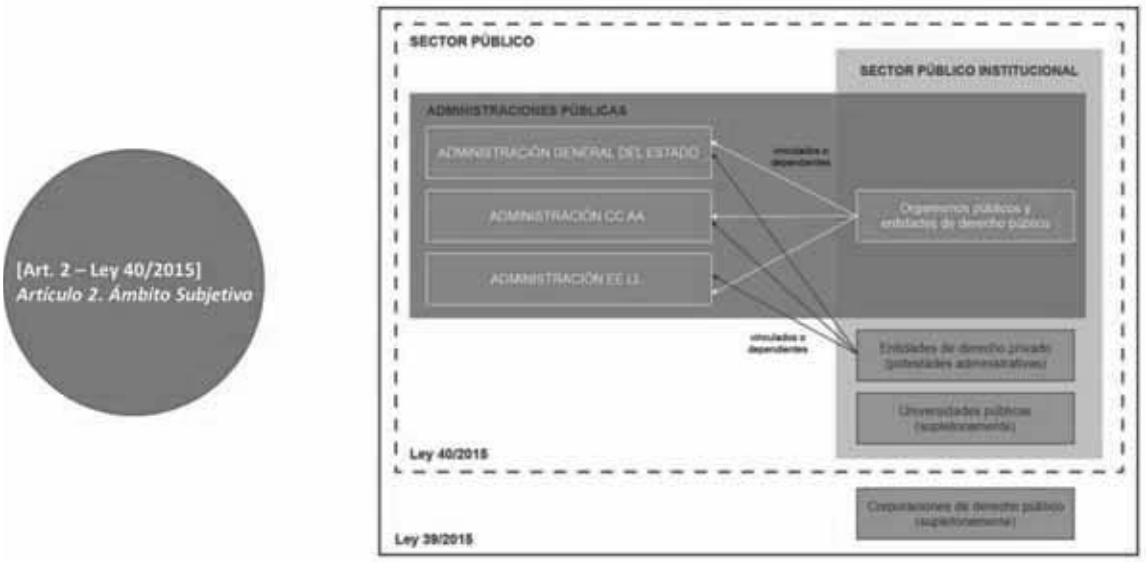
En 2015 se publicó la modificación del Esquema Nacional de Seguridad a través del Real Decreto 951/2015, de 23 de octubre. Esta actualización fue en respuesta a la evolución del entorno regulatorio, en especial de la Unión Europea, así como de las tecnologías de la información, la necesidad en algún caso de aclarar responsabilidades entre organismos (aunque fuera de forma indirecta) y de la experiencia en la implantación del Esquema.

Alcances: Subjetivo y Objetivo

El CCN ha publicado numerosas guías de Seguridad TIC (STIC). La Guía CCN-STIC 830 Ámbito de aplicación del Esquema Nacional de Seguridad en la que se precisa en qué organizaciones y sobre qué materias es preciso aplicar el Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS.

El documento diferencia entre el ámbito subjetivo de aplicación (organismos del sector público a los que aplica) y el ámbito objetivo o material (siste-

FIGURA 1
ÁMBITO DE APLICACIÓN SUBJETIVO DEL RD 3/2010 (ENS)



Fuente: Figura de la propia Guía

mas de información y comunicaciones a los que les es de aplicación).

La primera y más amplia referencia al ámbito de aplicación objetivo o material del RD 3/2010 (sistemas de información y comunicaciones a los que les es de aplicación) se encuentra en el número dos de su artículo 1, cuando señala: «2. El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones Públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.» (CCN-STIC-830, Septiembre 2016)

Es esencial indicar que frente al alcance original del ENS (básicamente para las sedes electrónicas, el servicio «más exterior» de las administraciones y más cercano en aquel momento al ciudadano), las Leyes 39/2015 y 40/2015 permiten establecer un alcance más amplio: «(..) bastará que el sistema de información en cuestión (cuando esté sustentado en medios electrónicos) se dirija a gestionar las competencias de la entidad pública correspondiente (que deberá estar incluida en su ámbito subjetivo de aplicación), para que le sea de aplicación el ENS.» (CCN-STIC-830, Septiembre 2016)

Es decir, prácticamente todos los sistemas de la administración pública (con las excepciones que el propio ENS establece).

Aspectos de relevancia en materia de seguridad en el articulado

El Centro Criptológico Nacional (en adelante CCN), dependiente del Centro nacional de Inteligencia (CNI), es a todos los efectos la autoridad de control o de referencia para el ENS, si bien no se define de esa forma en el RD, en el mismo se le asigna entre otras responsabilidades: elaborar y difundir las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones, tomar la iniciativa para la aprobación de las instrucciones técnicas de seguridad de obligado cumplimiento y ser el receptor de los incidentes de seguridad para el alcance del ENS.

En el Artículo 10 del RD_3/2010, define roles y funciones. En concreto el título enuncia La Responsabilidad de la Seguridad como función diferenciada; pues, la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios, lo cuales dependen en su grado máximo del responsable de la información, así como del diseño y ejecución de responsable del servicio. «El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.» (RD_3/2010, 8 de enero 2010)

Los elementos principales del ENS son los siguientes:

- Los principios básicos a considerar en las decisiones en materia de seguridad; Seguridad integral; Gestión de riesgos; Función diferenciada, entre otros.

- Los requisitos mínimos que permitan una protección adecuada de la información.; Organización e implantación del proceso de seguridad; Análisis y gestión de los riesgos; Seguridad por defecto; Incidentes de seguridad, entre otros.
- El mecanismo para lograr el cumplimiento de los principios básicos y de los requisitos mínimos mediante la adopción de medidas de seguridad proporcionadas a la naturaleza de la información y los servicios a proteger.
- La respuesta ante incidentes de seguridad.
- La auditoría de la seguridad.
- Las comunicaciones electrónicas.
- La certificación de la seguridad.
- La conformidad.

La actualización del 2015 del RD de desarrollo del ENS incorporó entre otras cuestiones:

- En el artículo 24, el despliegue de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información.
- En el artículo 36, la notificación al Centro Criptológico Nacional de aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados.
- En el artículo 37, las evidencias necesarias para la investigación de incidentes de seguridad por parte del Centro Criptológico Nacional.

Precisamente para poder encauzar los incidentes y sus notificaciones se crea el CCN-CERT. El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la información del Centro Criptológico Nacional (CCN). Este servicio se creó en el año 2006 como CERT Gubernamental/Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS). modificado por el RD 951/2015 de 23 de octubre.

De acuerdo con todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de las Administraciones Públicas y de empresas y organizaciones de interés estratégico para el país.

INFRAESTRUCTURAS CRÍTICAS

Leyes y antecedentes

El nivel de desarrollo y calidad de vida de Europa, encuentran en las tecnologías de la información y las telecomunicaciones (por sus siglas TIC) uno de sus principales sustentos. La complejidad e interdependencia de los sistemas de prestación de servicios, suministros y comunicaciones las hacen vulnerables y por tanto objetivo de protección.

La Unión Europea materializó su preocupación y su estrategia, primero, en el Programa Europeo de Protección de Infraestructuras Críticas (PEPIC) publicado en el año 2004, y más tarde, en la Directiva 2008/114 del Consejo de la Unión Europea, de 8 de diciembre.

En España la Ley 8/2011, de 28 de abril, estableció por primera vez las medidas para la protección de las infraestructuras críticas (más conocida ya como Ley PIC o simplemente LPIC) junto con el reglamento que la desarrolla (Real Decreto 704/2011, de 20 de mayo), respondiendo precisamente a esas necesidades de protección de infraestructuras críticas.

Alcances: Subjetivo y Objetivo

En el Articulo 1, define el objeto: «1. Esta Ley tiene por objeto establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, para mejorar la prevención, preparación y respuesta de nuestro Estado frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas. Para ello se impulsará, además, la colaboración e implicación de los organismos gestores y propietarios de dichas infraestructuras, a fin de optimizar el grado de protección de éstas contra ataques deliberados de todo tipo, con el fin de contribuir a la protección de la población. 2. Asimismo, la presente Ley regula las especiales obligaciones que deben asumir tanto las Administraciones Públicas como los operadores de aquellas infraestructuras que se determinen como infraestructuras críticas, según lo dispuesto en los párrafos e) y f) del artículo 2 de la misma.» (Ley_8/2011, 28 de Abril 2011)

En el Artículo 11. de la LPIC se crea la Comisión Nacional para la Protección de las Infraestructuras Críticas (en adelante, la Comisión) como órgano colegiado adscrito a la Secretaría de Estado de Seguridad. La Comisión es la competente para aprobar los diferentes Planes Estratégicos Sectoriales, así como para designar a los operadores críticos. La LPIC identifica como sectores críticos los siguientes 12 sectores: Administración, Agua, Alimentación, Energía, Espacio, Industria Química, Industria Nuclear, Instalaciones de Investigación, Salud, Sistema Financiero y Tributario, Tecnologías de la Información y las Comunicaciones (TIC) y Transporte.

Estos sectores definen el actual alcance subjetivo, mientras que el objetivo viene dado por el Articulo 2 y que de forma sucinta podríamos decir: «las instalaciones, redes, sistemas y equipos físicos y de tecnología

de la información sobre las que descansa el funcionamiento de los servicios esenciales»

Pues de las definiciones de la Ley, definimos las Infraestructuras críticas, como las infraestructuras estratégicas (*las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales*) cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales (aquellos servicios necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas).

Hasta el momento, la Comisión ha designado en torno a 150 Operadores Críticos con más de 500 infraestructuras críticas a su cargo.

Aspectos de relevancia en materia de seguridad en el articulado

En el Artículo 7, se define la Autoridad de Control para la LPIC: El Centro Nacional para la Protección de las Infraestructuras Críticas (en adelante CNPIC):

«El órgano ministerial encargado del impulso, la coordinación y supervisión de todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad (en adelante SES) del Ministerio del Interior en relación con la Protección de Infraestructuras Críticas en el territorio nacional.» (Ley_8/2011, 28 de Abril 2011)

Esta Autoridad, mantiene en la actualidad las siglas, pero no su denominación, pues la actual es Centro Nacional para las infraestructuras y la Ciberseguridad.

En el RD, en el CAPÍTULO III, Los Planes de Seguridad del Operador, Artículo 22. Finalidad, elaboración y contenido. Se define el Plan de Seguridad del Operador (PSO) como los documentos estratégicos definidores de las políticas generales de los operadores críticos para garantizar la seguridad del conjunto de instalaciones o sistemas de su propiedad o gestión. Los PSO deberán establecer *una metodología de análisis de riesgos* que garantice la continuidad de los servicios proporcionados por dicho operador y en la que se recojan los criterios de aplicación de las diferentes medidas de seguridad que se implanten para hacer frente a las amenazas tanto físicas como lógicas identificadas sobre cada una de las tipologías de sus activos *y las posibles repercusiones de la perturbación o destrucción de las infraestructuras que le dan apoyo.*

La notificación de incidentes de seguridad no aparece ni en la Ley PIC, ni en el RD, sin embargo, una instrucción de la Secretaria de Estado de Seguridad comunicó la necesidad de comunicar los incidentes; incluso el CNPIC ha distribuido, entre los operadores, la Guía de reporte preparada en colaboración con la mesa de Ciberseguridad del CNPIC, la cual elaboró una plantilla de soporte de notificación.

SEGURIDAD EN REDES Y SISTEMAS DE INFORMACIÓN

Leyes y antecedentes

La Unión Europea tras legislar incorporando la Ciberseguridad en las Infraestructuras críticas, ha estimado necesario dar un paso más y ha legislado la Directiva EU 2016/1148; la cual, tal y como se indica en el propio título de esta, buscando armonizar un elevado nivel común de seguridad de las redes y sistemas de información. Esta Directiva es la primera centrada específicamente en Ciberseguridad/Seguridad de la Información.

La transposición de la directiva al ordenamiento nacional fue publicada el 7 de septiembre por real Decreto y convalidada en ese mismo mes en trámite parlamentario. Así hablamos del RD Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

La cual en su introducción dice: «La evolución de las tecnologías de la información y de la comunicación, especialmente con el desarrollo de Internet, ha hecho que las redes y sistemas de información desempeñen actualmente un papel crucial en nuestra sociedad, siendo su fiabilidad y seguridad aspectos esenciales para el desarrollo normal de las actividades económicas y sociales.

Por ello, los incidentes que, al afectar a las redes y sistemas de información, alteran dichas actividades, representan una grave amenaza, pues tanto si son fortuitos como si provienen de acciones deliberadas pueden generar pérdidas financieras, menoscabar la confianza de la población y, en definitiva, causar graves daños a la economía y a la sociedad, con la posibilidad de afectar a la propia seguridad nacional en la peor de las hipótesis.» (Decreto-ley_12/2018)

En dicha introducción, se destaca el impacto que los incidentes, los ciberincidentes, pueden causar a la economía, a la sociedad y a la seguridad nacional.

El legislador español ha querido hacer confluir la LPIC y el Real Decreto-ley 12/2018, la primera poniendo el peso en la dimensión física (aunque no reduciéndose a ella) y la segunda con el foco en la Ciberseguridad. Ambas definiendo de una forma coherente los servicios esenciales y tratando de aclarar el espacio de responsabilidad de las Autoridades de control y de los CERTS nacionales.

Alcances: Subjetivo y Objetivo

El alcance subjetivo lo encontramos en el artículo 2, 3 y 6 mientras que el objetivo lo encontramos definido en el Artículo 1. En los Artículos 1,2 y 3 se dice literalmente:

El Articulo 1. Objeto

1. El presente real decreto-ley tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establecer un sistema de notificación de incidentes.

2. Así mismo, establece un marco institucional para la aplicación de este real decreto ley y la coordinación entre autoridades competentes y con los órganos de cooperación relevantes en el ámbito comunitario.

Artículo 2. Ámbito de aplicación.

1. Este real decreto-ley se aplicará a la prestación de: a) Los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. b) Los servicios digitales, considerados conforme se determina en el artículo 3 e), que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube.

2. Estarán sometidos a este real decreto-ley: a) Los operadores de servicios esenciales establecidos en España. Se entenderá que un operador de servicios esenciales está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios o actividades. Así mismo, este real decreto-ley será de aplicación a los servicios esenciales que los operadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España. b) Los proveedores de servicios digitales que tengan su sede social en España y que constituya su establecimiento principal en la Unión Europea, así como los que, no estando establecidos en la Unión Europea, designen en España a su representante en la Unión para el cumplimiento de la 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.

3. Este real decreto-ley no se aplicará a: a) Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios electrónicos de confianza que no sean designados como operadores críticos en virtud de la Ley 8/2011, de 28 de abril. b) Los proveedores de servicios digitales cuando se trate de microempresas o pequeñas empresas, de acuerdo con las definiciones recogidas en la Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresa

El extenso Articulo 3 de Definiciones, contiene la definición de Servicio esencial, como: servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas, que dependa para su provisión de redes y sistemas de información.

Artículo 6. Identificación de servicios esenciales y de operadores de servicios esenciales.

1. La identificación de los servicios esenciales y de los operadores que los presten se efectuará por los órganos y procedimientos previstos por la Ley 8/2011, de 28 de abril, y su normativa de desarrollo. La relación de los servicios esenciales y de los operadores de dichos servicios se actualizará, para cada sector, con una frecuencia bienal, en conjunción con la revisión de los planes estratégicos sectoriales previstos en la Ley 8/2011, de 28 de abril.

(..)

2. En el caso de tratarse de un operador crítico designado en cumplimiento de la Ley 8/2011, de 28 de abril, bastará con que se constate su dependencia de las redes y sistemas de información para la provisión del servicio esencial de que se trate.

(..)

4. Cuando un operador de servicios esenciales ofrezca servicios en otros Estados miembros de la Unión Europea, se informará a los puntos de contacto único de dichos Estados, sobre la intención de identificarlo como operador de servicios esenciales.

Aspectos de relevancia en materia de seguridad en el articulado

Artículo 9. Autoridades competentes.

1. Son autoridades competentes en materia de seguridad de las redes y sistemas de información las siguientes:

- a) Para los operadores de servicios esenciales: 1.º En el caso de que éstos sean, además, designados como operadores críticos conforme a la Ley 8/2011, de 28 de abril, y su normativa de desarrollo, con independencia del sector estratégico en que se realice tal designación: la Secretaría de Estado de Seguridad, del Ministerio del Interior, a través del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC). 2.º En el caso de que no sean operadores críticos: la autoridad sectorial correspondiente por razón de la materia, según se determine reglamentariamente.
- b) Para los proveedores de servicios digitales: la Secretaría de Estado para el Avance Digital, del Ministerio de Economía y Empresa.
- c) Para los operadores de servicios esenciales y proveedores de servicios digitales que no siendo operadores críticos se encuentren comprendidos

en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público: el Ministerio de Defensa, a través del Centro Criptológico Nacional.

2. El Consejo de Seguridad Nacional, a través de su comité especializado en materia de ciberseguridad, establecerá los mecanismos necesarios para la coordinación de las actuaciones de las autoridades competentes.

Artículo 11. Equipos de respuesta a incidentes de seguridad informática de referencia.

1. Son equipos de respuesta a incidentes de seguridad informática (CSIRT) de referencia en materia de seguridad de las redes y sistemas de información, los siguientes:

a) En lo concerniente a las relaciones con los operadores de servicios esenciales:

1.º El CCN-CERT, del Centro Criptológico Nacional, al que corresponde la comunidad de referencia constituida por las entidades del ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre.

2.º El INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, al que corresponde la comunidad de referencia constituida por aquellas entidades no incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre

3.º El ESPDEF-CERT, del Ministerio de Defensa, que cooperará con el CCN-CERT y el INCIBE-CERT en aquellas situaciones que éstos requieran en apoyo de los operadores de servicios esenciales y, necesariamente, en aquellos operadores que tengan incidencia en la Defensa Nacional y que reglamentariamente se determinen.

b) En lo concerniente a las relaciones con los proveedores de servicios digitales que no estuvieren comprendidos en la comunidad de referencia del CCN-CERT: el INCIBE-CERT.

Artículo 16. Obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales.

«1. Los operadores de servicios esenciales y los proveedores de servicios digitales deberán adoptar medidas técnicas y de organización, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados en la prestación de los servicios sujetos a este real decreto-ley. Sin perjuicio de su deber de notificar incidentes conforme al título V, deberán tomar medidas adecuadas para prevenir y reducir al mínimo el impacto de los incidentes que les afecten.» (..)

«3. Los operadores de servicios esenciales designarán y comunicarán a la autoridad competente, en el plazo que reglamentariamente se establezca, la persona, unidad u órgano colegiado responsable de la seguridad de la información, como punto de contacto y de coordinación técnica con aquella.» (..)

Artículo 19. Obligación de notificar.

«1. Los operadores de servicios esenciales notificarán a la autoridad competente, a través del CSIRT de referencia, los incidentes que puedan tener efectos perturbadores significativos en dichos servicios. Las notificaciones podrán referirse también, conforme se determine reglamentariamente, a los sucesos o incidencias que puedan afectar a las redes y sistemas de información empleados para la prestación de los servicios esenciales, pero que aún no hayan tenido un efecto adverso real sobre aquéllos.

2. Así mismo, los proveedores de servicios digitales notificarán a la autoridad competente, a través del CSIRT de referencia, los incidentes que tengan efectos perturbadores significativos en dichos servicios.» (..)

PUNTOS COMUNES, QUE NOS PERMITEN CUMPLIR Y MEJORAR

Todas estas leyes, con sus particulares alcances subjetivos y objetivos, contienen en su desarrollo una serie de elementos comunes (que no siempre un mínimo común denominador), entre los cuales destacan:

- La identificación de la autoridad de control. Con la peculiaridad, que, en muchos casos, la Organización puede tener la misma Autoridad en diferentes regulaciones.
- El foco se pone en la protección de la información. Tenga esta, su naturaleza en los datos de carácter personal, o bien, en el mantenimiento de los servicios esenciales.
- Los análisis de riesgos como mecanismo para la preservación adecuada de la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de los controles adecuados a las redes y sistemas de información.
- La inclusión de la seguridad en el diseño y por defecto.
- La notificación de los incidentes de seguridad a la autoridad de control y a los afectados.
- La comunicación de esos incidente a través del CERT /CSIRT de respuesta asociado a la autoridad; salvo en el caso de la AEPD que (al menos hasta el momento) es directamente.
- La figura del CISO o responsable de seguridad.
- La segregación de funciones para poder supervisar y ejecutar, evitando así el conflicto de intereses.

- La identificación de un responsable de la supervisión del cumplimiento (DPD en la RGPD, RSE en la LPIC..).
- La Auditoría.
- Un régimen sancionador (RGPD y NIS, y por ende en el futuro en LPIC)

Pongamos un ejemplo; para poder cumplir y mejorar en la seguridad, un organismo público que:

- Esté en el alcance subjetivo del ENS, por formar parte de la AGE.
- Esté en el alcance del RGPD por tratar un volumen importante de información de ciudadanos (o de clientes si fuera una entidad pública empresarial).
- Haya sido declarada Operador de infraestructuras críticas por su función en la provisión de servicios esenciales (alcance LPIC) y que para esa provisión haga uso intensivo de redes y sistemas de información (¡y quien no!) y en consecuencia también le aplique NIS deberá alinear de forma inclusiva e integradora, en su estrategia de seguridad y en consecuencia su Política de Seguridad, los requerimientos comunes. Ese alineamiento, se puede traducir en:
- Análisis de riesgos, multi-objetivo regulatorio, efectuándolo desde la fase más temprana (diseño), e incorporando
  - Personal capaz, metodología y herramientas que permitan realizar y documentar con calidad estos análisis.
  - La identificación de las leyes que le son de aplicación.
  - La valoración de la información y los sistemas que la tratan.
  - La inclusión combinada de nuevas necesidades (por ejemplo, como hace la herramienta Pilar para MAGERIT, con las obligaciones RGPD)
  - La trazabilidad (para garantizar la investigación y la responsabilidad proactiva).
  - Los controles de supervisión y auditoría.
  - La agrupación en dominios de riesgo, con controles similares, aunque los datos sean de alcances objetivos, diferentes; por ejemplo, un sistema de riesgo ALTO para RGPD probablemente disponga de un conjunto de controles de seguridad muy similar que para un sistema de riesgo ALTO para NIS.
- La definición de un proceso de gestión y notificación de incidentes (con sus procedimientos).
  - Informando a los empleados de la trazabilidad de sus acciones.
  - Diseñando los mecanismos de detección e incorporando recursos de investigación (o al menos identificándolos en el mercado).
  - Teniendo identificada la autoridad o autoridades de control, por entorno de incidente.
  - Teniendo identificado al responsable de reportar y coordinar con las diferentes autoridades de control y CERTs.
  - Disponiendo de un formato (lo más común posible) de notificación de un mismo incidente a una o más de una autoridad.
  - Un plan de escalado del incidente a crisis y a continuidad de Negocio.
- La identificación en la organización de las figuras responsables en ultima instancia de la información: responsable de la información en el ENS o en el RGPD el responsable del tratamiento (aunque la Ley no lo dice, para una eficacia pragmática es recomendable tenga en la organización un responsable interno del tratamiento -una persona que se responsabilice internamente de las decisiones-).
- La segregación de funciones para una correcta supervisión y asesoramiento.

Todo ello, para cumplir y mejorar en la protección de la información, sea ésta de la naturaleza que sea, aunando esfuerzos e incluso para Organizaciones aún no muy concienciadas con la Ciberseguridad, permite enviar hacia la Alta Dirección un mensaje simple, pero claro: hay que hacerlo seguro, porque las leyes nos lo exigen.

CONCLUSIONES

En la actualidad, la Ciberseguridad es un punto esencial en todas las nuevas regulaciones que la UE está legislando, en el futuro también estará presente en otras nuevas que afecten específicamente a sectores, productos o servicios tales como el transporte, la alimentación o la Salud (entre otras muchas). A nuestra vida cotidiana se incorporarán masivamente elementos como los IoT, la hiperconectividad o los servicios digitales; no se podrá entender, una regulación sin protegerse de las ciber amenazas. Las organizaciones deben aprender a incorporar la ciberseguridad a la totalidad de sus procesos y los diversos requerimientos en esta materia, a cohesionarlos y dar una respuesta coordinada.

BIBLIOGRAFÍA

Beamonte, P. (31 de agosto de 2017). *Más de 400 mil pacientes actualizaron su marcapasos para evitar un hackeo.* Obtenido de https://hipertextual.com/2017/08/465-mil-pa-

cientes-tuvieron-que-actualizar-su-marcapasos-evitar-hackeo.

CCN-STIC-830. (Septiembre 2016). *GUÍA DE SEGURIDAD (CCN-STIC-830). ÁMBITO DE APLICACIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD.*

Decreto-ley_12/2018, R. (s.f.). Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de informació.

Ley_8/2011, B. (Abril de 28 de Abril 2011). Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

RD_3/2010. (8 de Enero de 8 de enero 2010). Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.* BOE.

Otras referencias web:

NICK FARRELL (10 Abril 2012). «Hackers can control your implants». https://fudzilla.com/home/item/26720-hackers-can-control-your-implants

B.T (29 mayo. 2017). «Los marcapasos se pueden hackear muy fácilmente «, Diario el Mundo, Sección de tecnología.

BILLY RIOS, JONATHAN BUTTS (MAYO 2017). *Security evaluation of the implantable cardiac device ecosystem architecture and implementation interdependencies. Estudio WhiteScope.*

E.A (27/06/2017). «Ucrania confirma el «peor ataque de ciberseguridad» de su historia».Diario Expansión. http://www.expansion.com/economia-digital/2017/06/27/5952770b46163f20118b45b8.html.

MERCÈ MOLIST (21 Enero 2016).«Así es como un ciberataque deja toda una ciudad a oscuras». El Confidencial. https://www.elconfidencial.com/tecnologia/2016-01-21/amenazas-en-la-oscuridad-como-los-hackers-pueden-provocar-un-apagon-en-tu-ciudad_1138837/

Canal electrónico de la AEPD para la notificación de brechas de seguridad: https://sedeagpd.gob.es/sede-electronica-web/vistas/formBrechaSeguridad/procedimientoBrechaSeguridad.jsf