La ciberseguridad en las infraestructuras críticas

Autor: Francoso Figueredo, Alberto

Director/es: Vales Alonso, Javier y Fernández García, Norberto.

Contacto: aff@interior.es

Resumen.

Con este trabajo se pretende dar a conocer la importancia de la ciberseguridad en la protección de las infraestructuras críticas españolas, así como el marco normativo que la regula en este ámbito y los nuevos proyectos en los que se está trabajando para la mejora de la misma.

Para ello, se hace un repaso por la normativa más importante que regula esta materia a nivel europeo y nacional y por los estándares internacionales más importantes en seguridad de la información. Además, se realiza un somero estudio sobre la problemática de la aplicación de la normativa sectorial en distintos sectores con marcadas diferencias entre ellos.

Se realiza un estudio del caso de transposición 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* (en adelante, Directiva NIS), a la legislación española, mediante la reutilización de estructuras y procedimientos previamente establecidos y en vigor, como es la normativa relacionada con la protección de las infraestructuras críticas o normativa PIC.

En el siguiente apartado se pone en contexto la ciberseguridad con el marco estratégico establecido por la Ley de Seguridad Nacional y se citan y estudian los documentos y actores más importantes recogidos en dicha Ley.

Así mismo, se hace un repaso por las agencias estatales de ciberseguridad y cómo se relacionan entre ellas a partir del nuevo marco de actuación definido a raíz de la transposición de la Directiva NIS.

Por último, se analizan los nuevos retos a los que habrá que afrontar a medio y largo plazo, haciendo especial mención a la lucha contra la criminalidad.

Palabras clave: Infraestructura crítica, ciberseguridad, protección, normativa, gobernanza, cibercriminalidad

1. Introducción

A raíz de una serie de atentados terroristas ocurridos en los primeros años de la década de los 2000, como el atentado contra las torres gemelas ocurrido en Nueva York el 11 de septiembre de 2001 o el ocurrido en Madrid el 11 de marzo de 2004, la Unión Europea se ve en la necesidad de proteger las infraestructuras críticas europeas, entendiendo como tales, "Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas.

Con esta finalidad, se publica la DIRECTIVA 2008/114/CE DEL CONSEJO de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, mediante el establecimiento de un procedimiento de identificación y designación de infraestructuras críticas europeas y un planteamiento común para evaluar la necesidad de mejorar la protección de dichas infraestructuras, con el fin de contribuir a la protección de la población.

El 28 de abril de 2001, se publica en España la *Ley 8/2011, por la que se establecen medidas para la protección de las infraestructuras críticas* (en adelante, Ley PIC), e inmediatamente después, el *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas* (en adelante, Reglamento PIC). Con dicha ley y su reglamento de desarrollo, se establecen los instrumentos de planificación del Sistema de Protección de Infraestructuras Críticas y constituyen los elementos esenciales para garantizar la protección de las infraestructuras críticas y, por tanto, los servicios esenciales provistos por éstas. En esta normativa, además de la creación del Centro Nacional de Protección de Infraestructuras Críticas (en adelante CNPIC), se contempla la elaboración de unos planes de actuación por parte de los operadores críticos, que conforman el conjunto de medidas de seguridad integral para elevar al máximo nivel de capacidad en la protección de las infraestructuras críticas, comprendiendo tanto aspectos estratégicos como tácticos.

De forma paralela, en el 2010 se publica el 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.

Dicho esquema (en adelante ENS), aunque regula un ámbito distinto, como es el de la Administración Pública, para la que es de obligado cumplimiento, inspirará en materia de ciberseguridad el enfoque futuro de la protección de las infraestructuras críticas, destacando la consideración de sus dimensiones de seguridad, o la división de las medidas de seguridad en tres marcos definidos como son el organizativo, operacional y de protección.

Con la entrada en vigor 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* (en adelante, Directiva NIS), cambia radicalmente el panorama de la ciberseguridad, no sólo en España, sino en toda Europa.

Pese a ser una directiva con un marcado carácter económico, tal y como se recoge en su articulado: "La *presente Directiva establece medidas con el objeto de lograr un elevado nivel común de seguridad de las redes y sistemas de información dentro de la Unión a fin de mejorar el funcionamiento del mercado interior*."[1], ha establecido obligaciones en ciberseguridad en sectores tradicionalmente híper regulados en esta materia como es el sector financiero, así como en sectores muy regulados en el ámbito físico pero sin regulación específica en el ámbito cibernético, como por ejemplo el subsector del transporte aéreo.

[1] *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. Art. 1*

En abril del pasado 2019, se aprobó *el 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* que refuerza las funciones de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) e intenta poner orden la hora de la certificación de productos, sistemas y procesos de la ciberseguridad, en un panorama caótico donde cada estado miembro posee sus propios esquemas de certificación, o utiliza estándares internacionales.

2. Estado del arte

Se hace un breve repaso por el estado del arte de la ciberseguridad, su regulación e iniciativas.

3. Marco normativo

3.1. Leyes europeas

Se analizan las distintas normas europeas que regulan en esta materia, como la *Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, 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 o el 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.*

3.2. Leyes españolas

En este apartado se hace un estudio sobre las normas españolas como la *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas,* el *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.* Desarrollo reglamentario pendiente de publicación o el *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.*

3.3. Normativa sectorial

Se analizan las peculiaridades de los sectores estratégicos más significativos por su nivel de desarrollo en normativa o por otras cuestiones. En particular se analizan *el Sector financiero, Sector transportes-Subsector aéreo, Sector industria nuclear y el Sector energía-Subsector eléctrico.*

2.4. Estándares Internacionales

Se hace referencia a los estándares internacionales más significativos en ciberseguridad de nuestro entorno como son el *ISO/IEC 27001*. Sistema de gestión de seguridad de la información, la serie NIST 800 o los Criterios Comunes para la evaluación de la Seguridad de la Tecnología de la Información (*Common Criteria*).

4. La convergencia de los servicios esenciales

Se analiza el caso concreto de cómo se ha abordado la transposición de la Directiva NIS en la normativa española.

5. La gobernanza de la ciberseguridad

Se repasa la gobernanza en ciberseguridad española, haciendo mención a la *Ley 36/2015, de 28 de septiembre, de Seguridad Nacional*, al *Consejo Nacional de Ciberseguridad* y a la *Estrategia Nacional de Ciberseguridad.*

6. Ciberactores principales

Se mencionan los principales actores de la ciberseguridad gubernamentales y sus cometidos, como son *el Centro Nacional de Protección de Infraestructuras Críticas, la Oficina de Coordinación de la Ciberseguridad, el Centro Criptológico Nacional, el Instituto Nacional de Ciberseguridad y el Mando Conjunto del Ciberespacio.*

7. Conclusiones y líneas futuras de actuación

7.1. Tiempos desacompasados

Los próximos retos en ciberseguridad a los que se tendrán que enfrentar la Unión Europea en su conjunto, y España de manera particular, están caracterizados por un dinamismo y una velocidad que no se ajustan a los tiempos de producción regulatoria para la resolución de los problemas que vayan surgiendo, que son mucho más lentos.

Esto implica que necesariamente la regulación normativa relativa a estos aspectos, necesariamente irá retrasada con la necesidad de solución de los problemas, existiendo una percepción en la ciudadanía de que no se abordan los problemas de manera diligente.

Las Autoridades europeas y españolas, habrán de realizar un esfuerzo para dinamizar los trámites legislativos y acortar los tiempos si quieren reaccionar a las cuestiones de la ciberseguridad en unos tiempos razonables.

7.2 La armonización normativa

La producción normativa en ciberseguridad se ha producido de manera desigual en la Unión Europea.

Países como Reino Unido, Alemania o España, abordaron la legislación en esta materia de manera temprana, lo que les ha permitido tener una normativa muy cohesionada en ciberseguridad. Esto ha ocasionado una colisión con las normas europeas que a posteriori se han publicado, por lo que es necesaria la armonización entre las complejas estructuras normativas de estos países y las europeas.

Dentro del propio seno de la Unión, Autoridades centrales como la del Banco Central Europeo o ENISA, han ido emitiendo numerosas normas sectoriales a lo largo del tiempo para regular el marco de sus competencias. La necesidad de transversalidad de la ciberseguridad y la uniformidad en todos los países, ha provocado la publicación de normas generalistas como la *Directiva NIS*, el *Reglamento de Ciberseguridad Europeo*, o el *Reglamento eIDAS.*

En este momento, se están revelando incoherencias con la normativa sectorial que está motivando que se prioricen estas normas específicas sobre las generalistas, lo que está debilitando el carácter uniformador con el que fueron creadas estas últimas. Ejemplo de ello son las diferentes taxonomías de los incidentes de seguridad entre las distintas autoridades. Esta disfunción permite clasificar de manera distinta un mismo incidente, según lo interprete una autoridad u otra, y consecuentemente, se exige un distinto tratamiento a la hora de aplicar procedimientos o de

cumplimentar tiempos de resolución del incidente, todo ello agravado porque, en la mayoría de los casos, su incumplimiento conlleva sanciones económicas.

Los Estados miembros de la Unión que carecían de legislación sobre ciberseguridad en el momento de la publicación de las normas europeas, han tenido mucho más fácil la adecuación a dicha normativa.

7.3. La certificación en ciberseguridad

La existencia en los Estados miembros de la Unión Europea de innumerables certificaciones en ciberseguridad, ya sea de procesos, esquemas o elementos de software o hardware regulados por las Autoridades competentes locales, sumados a las certificaciones exigidas por las Autoridades de la Unión, más las distintas certificaciones de organismos privados reconocidos internacionalmente, presentan un panorama muy complicado a la hora de obtener certificaciones por parte de los operadores, ya que para operar en determinados sectores, necesitan según sea la Autoridad competente, varios certificados en ciberseguridad con el consiguiente gasto, y donde además, se exigen los mismos controles.

El Reglamento de Ciberseguridad Europeo de 2019 ha publicado en un intento de poner orden en esta materia y crear certificaciones únicas en todo el territorio para simplificar el proceso de certificación.

No obstante, el panorama actual es que los operadores disponen de distintas certificaciones en ciberseguridad, que no son reconocidas por las autoridades y que en el ámbito privado tampoco pueden ser aprovechadas debido a que los niveles de certificación no son homogéneos.

Por parte del sector bancario, uno de los más activos en estas cuestiones, se ha creado un grupo de trabajo para la realización de una matriz de correspondencias entre los distintos certificados de su sector, que permita la racionalización en el uso de los certificados en beneficio de los operadores.

Por último, está el problema de la **re-certificación**. Para la obtención de cualquier certificado en ciberseguridad, se han de realizar determinadas acciones para garantizar que el sistema en cuestión es seguro. Ello pasa necesariamente por estudios de laboratorio si son productos, o por auditorías si son procesos o esquemas. Dichas acciones suponen un coste en dinero y en tiempo.

El problema se presenta cuando, debido al dinamismo propio de la ciberseguridad, se han de actualizar versiones, o rediseñar procesos. Estas acciones que son necesarias para el mantenimiento de los sistemas y para garantizar un determinado nivel de seguridad, provoca que las certificaciones dejen de tener validez por la modificación del alcance objeto de la certificación.

La agilización de los procesos de certificación, su menor coste, así como la flexibilización en el reconocimiento de variación de versiones, es la única manera de que se puedan abordar las re-certificaciones como una exigencia en ciberseguridad.

7.4, La lucha contra el Cibercrimen

El uso de las tecnologías de la información y la comunicación se ha hecho presente como un aspecto más de nuestra vida cotidiana. Cualquier actividad va estrechamente ligada de una forma de otra a estas tecnologías.

Esta normalidad tecnológica está siendo aprovechada por la delincuencia para cometer hechos delictivos a través de estas mismas tecnologías debido especialmente a los beneficios que les supone comparados con la comisión de los mismos por los métodos tradicionales, como son la dificultad de atribución, el escaso riesgo y los enormes beneficios que se pueden obtener con su comisión.

La globalización de los movimientos terroristas, ha favorecido su presencia en las redes para publicidad de sus actuaciones y sus postulados, además de para el uso de Internet como una herramienta más para atacar sus objetivos.

Nuevos delitos relacionados con las redes, motivados por prácticas de riesgo como el *sexting*[2], o por actividades delictivas, como por ejemplo el *grooming*[3] o el intercambio de material pedófilo, han sufrido también un importante incremento.

En el Estudio de la cibercriminalidad de 2019[4] publicado por el Ministerio del Interior, se observa como nuestro país ha sufrido un fortísimo incremento de la cibercriminalidad, produciéndose entre los años 2018 a 2019 un incremento del 41%, y un total, desde que se comenzaron estos registros en el año 2015, de un incremento del 210%.

El 10% del total de delitos que se cometen en España son ciberdelitos y la cifra continúa subiendo año tras año.

La *Estrategia Nacional de Ciberseguridad* considera a la cibercriminalidad como una amenaza a la Seguridad Nacional, estableciendo en la Línea de Acción tercera la responsabilidad al Estado de "*Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio*", mediante el reforzamiento del marco jurídico, el fomento de la colaboración y participación ciudadana, potenciando las capacidades de investigación, reforzando la comunicación con los órganos judiciales y fomentando el intercambio de información entre las unidades policiales de inteligencia tanto nacionales como internacionales.

Para dar cumplimiento a esta línea de acción, el Ministerio del Interior está elaborando el *Plan Estratégico contra la Cibercriminalidad*, donde recoge cada una de las acciones de la *Estrategia Nacional* y las desarrolla en planes de actuación específicos que habrán de ejecutar las Fuerzas y Cuerpos de Seguridad del Estado.

Actualmente existe un encendido debate sobre si la ciberseguridad es la parte preventiva del ciclo de la cibercriminalidad, compuesto por la prevención, la investigación y persecución de los autores y el auxilio a la víctima. El argumento es que, si la ciberseguridad cumple su función de proteger de los ciberataques, no se producirían hechos delictivos.

Por otro lado, están los que opinan que la ciberseguridad es un concepto más amplio que sobrepasa ampliamente el ámbito de la cibercriminalidad.

Una tercera corriente opina que son dos ámbitos diferentes con ciertos elementos comunes como la prevención o los ciberataques y aspectos exclusivos de cada uno de ellos como la investigación de los autores en el ámbito de la cibercriminalidad o las malas *praxis* en el de la ciberseguridad. En cualquier caso, el debate está servido.

La **mejora en la eficacia de lucha contra la criminalidad** pasa por la aplicación de determinadas medidas recogidas en el borrador del *Plan Estratégico contra la Cibercriminalidad 2020* del Ministerio del Interior, como son:

- Fomentar el conocimiento y la información a los usuarios y público en general para incrementar la prevención y la autoprotección
- Incrementar las capacidades operativas y de inteligencia de las unidades policiales y las competencias y habilidades de los agentes que las integran
- Compartir información para generar inteligencia

[2] Sexting: intercambio de imágenes de contenido sexual por Internet

[3] Grooming: acoso sexual a menores a través de Internet

[4] http://www.interior.gob.es/documents/10180/9814700/Estudio+sobre+la+Cibercriminalidad+en+España+2019.pdf/24bd3afb-5a8e-4767-9126-c6c3c256982b

- Impulsar la coordinación nacional y la cooperación internacional
- Promover un marco jurídico eficaz
- Establecer líneas de colaboración y asociación con la industria, con las Universidades y demás actores relevantes en este ámbito

Agradecimientos

Quiero expresar mi especial agradecimiento a los directores de este trabajo fin de master: Javier Alonso Vales y Norberto Fernández García por el tiempo que han dedicado a proponer ideas y sugerencias para mejorar este trabajo.

También me gustaría agradecer al director del Centro Nacional de Protección de Infraestructuras Críticas, Teniente Coronel de la Guardia Civil D. Fernando José Sánchez Gómez y al jefe de la Oficina de Coordinación de Ciberseguridad, Comisario del Cuerpo Nacional de Policía D. Juan Carlos López Madera por todo lo que me han enseñado en estos años de trabajo en la Secretaría de Estado de Seguridad del Ministerio del Interior.

Por último, me gustaría agradecer a todos los compañeros del Máster Universitario en Dirección TIC para la Defensa en su edición 2019/2020 por su compañerismo y atención demostrada, y a los profesores del Centro Universitario de la Defensa y de la Universidad de Vigo por su profesionalidad, compromiso y buen hacer en la impartición de las distintas asignaturas.

Referencias

Norma europea	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 en las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº. 526/2013 (Reglamento sobre la Ciberseguridad). *Diario Oficial de la Unión Europea*, núm. 151, de 7 de junio de 2019, pp. 15-65
Norma europea	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. *Diario Oficial de la Unión Europea* L 194/1, 19 de julio de 2016, pp. 1-30
Norma europea	Directiva (CE) 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de mejorar su protección. *Diario Oficial de la Unión Europea* núm. 345, de 23 de diciembre de 2008, pp. 75-82
Norma española	Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. *Boletín Oficial del Estado*, de 29 de abril de 201, núm. 1092, pp. 71548-71586
Norma española	Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. *Boletín Oficial del Estado,* de fecha 21 de mayo de 2011, núm. 121, pp. 50808-50826

Norma española	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 Boletín Oficial del Estado, de 29 de enero de 2010, núm. 25, pp. 8089-8138
Norma española	Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Boletín Oficial del Estado, de 8 de septiembre de 2018, núm. 218, pp. 87675-87696
Norma española	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. *Boletín Oficial del Estado*, de 18 de septiembre de 2015, núm. 224, pp. 82405-82425
Norma española	Instrucción 3/2015 de la Secretaría de Estado de Seguridad por la que se actualiza el Plan de Prevención y Protección Antiterrorista
Norma española	Consejo de Seguridad Nacional. 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. *Boletín Oficial del Estado*, de 30 de abril de 2019, núm. 103, pp. 43437-43455
Norma española	CNPIC-CCN-DSN. Guía Nacional de Notificación y Gestión de Ciberincidentes
Norma española	CNPIC. Guía de Buenas Prácticas Plan de Seguridad del Operador, de 8 de septiembre de 2015
Norma española	CNPIC. Guía de Buenas Prácticas Plan de Protección Específico, de 8 de septiembre de 2015
Estándar	ISO 27001 Sistema de gestión de seguridad de la información.
Estándar	ISO 27002 Código de prácticas para los controles de seguridad de la información
Norma EEUU.	NIST SP 800-82 Guía para la Seguridad de los Sistemas de Control Industrial (ICS)

NOMBRE DEL RECURSO	**FECHA DE CONSULTA**	**URL**
Departamento de Seguridad Nacional	24/10/2020	https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional
INCIBE	20/12/2020	https://www.incibe-cert.es/blog/diferencias-ti-to
normaiso27001.es	13/10/2020	https://normaiso27001.es
National Institute of Standars and Technology USA	27/12/2020	https://csrc.nist.gov/publications/sp800