Informe sobre futuras exigencias en materia de ciberseguridad en las Infraestructuras Críticas dentro de las Ciudades Inteligentes (Smart Cities)

-

CAMILO ANDRÉS HERNÁNDEZ ROA

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement n. 101007820.

This document reflects only the author's view. The Research Executive Agency is not responsible for any use that may be made of the information it contains

Abreviaturas

AAPP: Administraciones Públicas
CSIRT: Los CSIRT son los equipos de respuesta a incidentes que analizan riesgos y supervisan incidentes a escala nacional, difunden alertas sobre ellos y aportan soluciones para mitigar sus efectos. El término CSIRT es el usado comúnmente en Europa en lugar del término protegido CERT (Computer Emergency Response Team), registrado en EE.UU.
DSP: Proveedor de Servicios Digitales
EU: Unión Europea
EEUU: Estados Unidos de Norte América
IdC: Internet de las cosas
IA: Inteligencia Artificial
NIS: Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
M2M: Machine-to-Machine
OES: Operadores de Servicios Esenciales

ÍNDICE

RESUMEN

Las infraestructuras críticas por décadas han significado un eje importante en el sostenimiento y desarrollo de los Estados, es tan así que la lista de aquellos servicios, instalaciones, redes o equipos físicos o tecnológicos se ha ido ampliando y los retos en cuanto a su cuidado y manejo resultan cada vez más complejos. Es por ello que para los países que conforman la Unión Europea se ha convertido en un punto de atención y discusión.

Desde la Directiva Europea 2008/114/CE del 8 de diciembre de 2008 la cual hizo especial relevancia en identificar y designar las infraestructuras críticas y llamo la atención en prestar mayor cuidado en el tema de seguridad y protección de las mismas, se promulgó una convocatoria primordial para que los países tomaran las medidas necesarias y así evitar ataques o inconvenientes que fuesen a repercutir en un grandes daños o perjuicios a la población e instituciones de sus estados.

La escalada de internet y su posicionamiento global, trajo consigo el crecimiento exponencial y desarrollo de nuevas tecnologías de la información, la era digital ha despertado la necesidad de los estados en digitalizar sus servicios en general y la telecomunicación paso de ser un servicio ocasional a ser el motor y el precursor de las relaciones comerciales y sociales del mundo. Sin embargo, y paralelo a todo esto nacen también los peligros y riesgos que ponen en riesgo

todo este universo tecnológico y digital, encontrándonos de frente con amenazas que a pesar de ser intangibles no resultan menos peligrosas.

Las ciudades y con ello las infraestructuras que hacen que una urbe funcione organizada y adecuadamente, proporcionando bienestar a sus habitantes; no han sido ajenas a la incursión de tecnologías para mejorar sus servicios y permanecer a la vanguardia. Las empresas que prestan servicios en los diferentes sectores y en distintos niveles críticos, han implementado no solo esfuerzos en materia física, sino que han puesto especial empeño en automatizar, digitalizar y computarizar sus procesos para fusionarlos así con otras asistencias y cubrir la mayor cantidad de necesidades. Los mismos pobladores de las ciudades demandan por servicios públicos y privados que hagan sus vidas más fáciles y eficientes; y para lograr esto una ciudad debe conectar la mayor cantidad de ayudas y asistencias posibles en pro del bien común. Las Smart Cities ya son una realidad, pero también presuponen retos y riesgos en materia de seguridad de gran magnitud.

Este trabajo tiene como objetivo realizar un informe en el cual se muestren los cambios y transformaciones a los cuales se han tenido que adaptar las Infraestructuras Críticas en los últimos años, la cuarta revolución industrial (industria 4.0), el uso de las nuevas tecnologías y la participación activa con otros mercados y elementos, sitúan a este tipo de empresas en un lugar de interés significativo en temas de legislación, investigación e inversión en seguridad cibernética, que es en últimas el eje principal; todo lo anterior por supuesto de cara al futuro más próximo, en el cual los servicios que prestan no solo deberán estar integrados, sino que conformaran así mismo las Ciudades Inteligentes (Smart Cities), por este motivo resulta elemental analizar el alcance y posibilidad de aplicar la regulación que la Unión Europea ha venido anunciando en materia de seguridad a este tipo de próximas metrópolis.

La interacción de la que hablamos, no solo supone retos y esfuerzos de gobierno, organización tecnológica, arquitectura, profesionales calificados, nuevas

entidades, sino que sitúa en la mira de los delincuentes a este tipo de grandes infraestructuras, el ciberterrorismo y las ciberamenazas serán cada vez más difíciles de detectar o detener, y ello resulta ser de especial atención de cara a la sociedad digital emergente.

Se quiere que el lector tenga un acercamiento a lo que un par de años será una realidad generalizada, partimos desde la idea de ver a las ciudades inteligentes como un todo y por lo tanto también la podemos considerar una Infraestructura Crítica teniendo en cuenta el gran avance de las telecomunicaciones, el IoT, la era digital, el Big Data y la IA, todos ellos como actores protagónicos y conectados entre sí dentro de las entidades esenciales y de los cuales depende nuestra seguridad. *"Su seguridad es a la vez nuestra seguridad".*

1. INTRODUCCIÓN

Es relevante para el objetivo de este trabajo conocer y entender la manera en cómo las infraestructuras criticas han avanzado y se han convertido en uno de los activos de mayor interés para los Estados, debido no solo a lo que representa económicamente, sino por el gran riesgo que conlleva la afectación de una de ellos.

1.1 La Evolución de las Infraestructuras Críticas

Desde que la Directiva europea 2008/114/CE del 8 de diciembre de 2008, recogió todas aquellas intenciones y documentos que existían desde el 2004 cuando las infraestructuras críticas se tornaron importantes a raíz de la preocupación por los atentados terroristas que las mismas podían sufrir, se definieron como*: "el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones".* Claro está que la definición lejos de ser nueva, acuñó el concepto de las instalaciones, redes o servicios que se encontrasen ubicadas en territorio de algún Estado miembro de la Unión Europea lo que incremento la amplitud e interés en el tema.

Ahora bien, extrayendo las intenciones y objetivos de la directiva antes referenciada, se puede observar que para el momento en que la misma fue publicada, la principal amenaza que podía sufrir una infraestructura critica era el

terrorismo, es decir, ataques directos que provocaran daños a las instalaciones físicas de empresas o construcciones que afectarían gravemente a la población en general, fue desde la adopción en 2005 del Libro Verde sobre un Programa Europeo para la Protección de Infraestructuras Críticas en donde la intención de una protección comunitaria se propuso, ya que para el momento era imprescindible aumentar la capacidad de protección, de respuesta y reducir sus vulnerabilidades[1] – que hasta el momento eran pocas, debido a que el terrorismo era un problema focalizado y ya estudiado -. Pero fue realmente en el año 2007 en donde el Consejo de Justicia adoptó las conclusiones de los estudios y recomendaciones anteriores abriendo así la puerta de entrada para la redacción de la directiva 2008/114.

La anterior normativa recogía disposiciones en pro de identificar las necesidades y amenazas a las que se encontraban sujetos los sectores de energía y transportes, siendo estos los de más alto nivel de importancia desde la perspectiva de la comunidad europea, no obstante, la regulación también dejo abierto el camino para que se incluyera el sector de las tecnologías de la información y las comunicaciones (TIC) vaticinado la relevancia que este tendría en la sociedad futura.

Son infraestructuras críticas, la Administración (instalaciones, servicios básicos redes de información, monumentos del patrimonio nacional y principales activos); Industria Química y Nuclear (producción, materiales químicos, biológicos, radiológicos, almacenamiento y transporte de mercancías peligrosas); Instalaciones del Espacio; Agua (embalses, almacenamiento, tratamiento y redes); Centrales y Redes de energía (producción y distribución); Tecnologías de la Información y las Comunicaciones (TIC); Salud (sector e infraestructura sanitaria); Transportes (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico, etc.); Alimentación (producción, almacenamiento y distribución); y

[1] Programa europeo de protección de las infraestructuras críticas «el PEPIC»

Sistema Financiero y Tributario (entidades bancarias, información, valores e inversiones). (Sánchez, 2011). No obstante, a la lista se siguen sumando elementos y sistemas que con el pasar de los años resultan imprescindibles para los estados y sus habitantes y por ende merecen la atención de los mismos, dado que sus fallas o daños resultarían críticos para el funcionamiento de la sociedad. Desde hace ya varios años, la idea de automatizar el mundo se ha hecho cada vez más real, facilitar la vida de las personas a través de ayudas ofrecidas por máquinas, asistentes virtuales, aplicaciones para dispositivos digitales, inteligencias artificiales, y toda una serie de sistemas que utilizan internet y gran cantidad de datos para que el diario vivir de las personas sea cada vez más sencillo parece estar a la vuelta de la esquina.

Ahora bien, si todo lo anterior se viene desarrollando y con más frecuencia el ser humano se vuelve más dependiente de su entorno digital, podemos empezar a hablar de una nueva categoría de infraestructura critica, las Smart Cities o ciudades inteligentes ofrecen una interconexión total en donde el "habitante" es un elemento más dentro de la burbuja. Estamos hablando que las "cosas", las "personas", los "sistemas", las "calles", los "edificios"; absolutamente todo se va encontrar conectado entre sí, lo que a primera vista hace pensar que un ataque cibernético a cualquiera de las piezas que conforman esta gran pirámide, sería una catástrofe para quienes habitan determinada ciudad o Estado.

Han pasado 7 años desde que se tiene información del primer ataque cibernético a una infraestructura critica, un grupo de hacktivistas[2] logró a través de un malware (Black-Energy) dejar sin energía eléctrica a más de 200.000 mil personas durante ocho largas horas, en Ucrania[3]. Desde este suceso los ataques cibernéticos son una constante y no solo como una forma delincuencia y organizada para obtener lucro, a través de extorsiones, y pagos, también se ha

[2] Hacktivistas: Utilizan la tecnología para reivindicar posiciones políticas o sociales

[3] Huamán Farro, S.D. (4 de agosto, 2022), Análisis sobre ciberataques a infraestructuras críticas y sus consecuencias. *Policía H50*. https://www.h50.es/analisis-sobre-ciberataques-a-infraestructuras-criticas-y-sus-consecuencias/.

convertido en un arma geopolítica, en donde dichos ataques terroristas más que un beneficio económico, buscan fines políticos y sociales mediante la desestabilización de los estados.

Lo más alarmante del caso, es que la tendencia de que las infraestructuras criticas sigan recibiendo este tipo de ataques, continua al alza, los grupos, personas y organizaciones dedicadas a este tipo de acciones, se han dado cuenta que es un negocio rentable y que poner en riesgo los servicios esenciales de las personas genera un pánico colectivo, que pocos quisieran experimentar. Una muestra de ello, es el incremento de ataques cibernéticos que han sufrido los hospitales (infraestructuras criticas) desde el inicio de la pandemia (Harán 2021), el sector sanitario es visto como un blanco ideal para la extorsión y el provecho criminal, en donde una sola amenaza de interrupción en el servicio, robo de datos o fallas en el sistema, significaría en momentos de COVID-19 un impacto más que significativo en la población. Y no podemos dejar de lado las instituciones públicas de los estados las cuales se ha convertido en objetivos relevantes debido a la digitalización de sus sistemas, lo que las convierte en instalaciones vulnerables, más del 75% de las organizaciones del sector público han sido víctimas de ciberataques en los últimos años.

Los estados de la UE son conscientes de los riesgos a los que están expuestos sus entidades críticas y esenciales, conocen los peligros más aun cuando de estas dependen millones de personas, y por esto a lo largo del tiempo han proferido normativas que intentan mitigar y proteger a sus infraestructuras, han creado instituciones dedicadas a ciberseguridad o divisiones dentro de las entidades estatales y europeas, países como Francia, Alemania o España[4] no se han quedado inertes ante el gran progreso de las TIC y las redes de comunicación; los estados han ido más allá queriendo implementar regulaciones que vayan

[4] En el territorio Español se han emitido estas dos normativas - Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y - el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

cobijando los avances en temas de comunicaciones, conexión de dispositivos, sistemas de información, los proveedores de servicios digitales y esenciales. Como se mencionó el mundo cada vez más está inmerso en la sociedad de la información, y los estados deben exigir que todos los servicios en este ámbito tengan y cumplan las normativas que sirven como primer escudo para evitar incidentes y ataques cibernéticos, la prevención y la comunicación de sucesos son un pilar fundamental para conocer cómo funcionan los ataques y entrega la oportunidad de que más instituciones y estados sepan a lo que se enfrentan.

El camino aún está lleno de obstáculos y parece no tener fin, el avance de las TIC, y de la sociedad misma es imparable y con ello los retos en materia de ciberseguridad, las infraestructuras criticas han pasado de ser gigantes empresariales prestadores de servicios esenciales a los que nadie podía acceder, y conocer, el internet los posicionó y los ubicó al alcance de todos nosotros, una industria critica o no, grande o pequeña, que este conectada a la red se convierte inmediatamente en un blanco para los delincuentes, sus procesos, sus datos, su organización y por supuesto su servicio empieza a tener un valor incalculable para los delincuentes. El mundo nos ofrece cada vez más, facilidades y comodidades digitales, pero con ello la responsabilidad aumenta y los Estados deben estar a la vanguardia, tener presente que el enemigo es silencioso, no posee un rostro y no descansará hasta ocasionar todos los daños posibles, mientras se le permita.

2. CIUDADES INTELIGENTES, ¿UNA NUEVA INFRAESTRUCTURA CRÍTICA?

Como ya lo habíamos mencionado al inicio de este informe, la evolución y cambio que han sufrido en los últimos años, los sectores clasificados como críticos suponen también una nueva visión de los mismos, y es que lo antes parecía intocable e inalcanzable, es hoy en día es un activo vulnerable y que debe ser el

centro de atención, tanto legislativo como organizativo. Junto con este desarrollo, y como eje principal encontramos a las personas, quienes hoy en día demandan entornos más prácticos, agiles, seguros, diversos, económicos, sostenibles, digitales e innovadores, si quisiéramos confluir todos estos calificativos en un solo concepto el resultado seria "ciudad inteligente", a pesar de no existir una ciudad 100% inteligente en la actualidad, son innumerables las urbes que han empezado una mutación hacia un funcionamiento inteligente, pero por supuesto que este objetivo además de costoso requiere de esfuerzos gigantescos en materia de distribución, adaptación y educación.

¿Qué significa una metrópoli inteligente o mejor dicho ¿qué hace que una ciudad sea realmente inteligente?, en un futuro no muy lejano podremos hablar de que inteligente es sinónimo de autosuficiente refiriéndonos a espacios en donde las TIC están en función del bienestar cotidiano de sus habitantes. La ciudad inteligente es la asociación de dos tendencias marcadas del mundo contemporáneo, de una parte, la urbanización y por otra la revolución digital (Villarejo, 2016). Una ciudad inteligente es un espacio que utiliza las nuevas tecnologías para lograr que sus infraestructuras, así como sus servicios públicos y privados sean interactivos y eficientes, es una nueva forma de vivir (Villarejo, 2016). Múltiples son las definiciones que encontramos sobre las ciudades inteligentes, pasando desde las más académicas y románticas hasta las técnicas y complejas, sin embargo, existe una constante en todas ellas, y es la inclusión de término "infraestructura".

El concepto también ha evolucionado al interior de la UE, ya que para el año 2014 el Parlamento consideraba que una ciudad era inteligente si desplegaba alguna de estas características: Smart Economy, Smart People, Smart Mobility, Smart Environment, Smart Governance y Smart Living (Parlamento Europeo, 2014), para el 2016 la Comisión Europea consideró que una ciudad inteligente era un lugar en donde las redes y los servicios tradicionales se hacen más eficientes con el uso de las tecnologías digitales y de telecomunicaciones; la noción ha evolucionado, tanto así que la definición más actual que se encuentra a nivel de

la EU, es la siguiente: *"una ciudad inteligente va más allá del uso de las tecnologías digitales: también incluye edificios más eficientes desde el punto de vista energético, fuentes de energía renovables integradas, sistemas de calefacción y refrigeración sostenibles, redes de transporte urbano más inteligentes, la mejora del suministro de agua y mejores instalaciones de eliminación de residuos para hacer frente a los retos económicos, sociales y medioambientales de la ciudad. Las ciudades inteligentes dependen de un compromiso político y de un compromiso ciudadano amplio e integrador para ofrecer soluciones sostenibles e inclusivas para que las ciudades sean más resilientes".*

Parece a simple lectura una definición bastante amplia, pero detalla a la perfección lo que se entiende y se quiere de una ciudad inteligente, y es que como se indicaba al principio de este informe, la exigencia más grande a la que se debe enfrentar las empresas y entidades que prestas servicios críticos en el mundo, es la adaptación y compenetración con las demás tecnologías, pasando de ser aquellas empresas de servicios centralizados, a ofrecer conexiones distribuidas, remotas, bidireccionales y automáticas, en pocas palabras estas infraestructuras harán parte activa de las ciudades no solo porque utilizan tecnologías de última generación, sino porque deben ofrecer calidad, facilidad y sostenibilidad dentro y para los ciudadanos. Lo anterior sí que supone un reto para las entidades esenciales, pero marca el futuro de lo que se convertirá en las ciudades del futuro en donde no solo se tratara de prestar un servicio, sino paralelamente ir de la mano con la conexión de las cosas, electrodomésticos, autos, edificios, vías; el manejo de las grandes bases de datos, lo cual supone que existirá solo una gran y única base de información que será útil para todas las empresas en general; la inteligencia artificial que será la principal responsable de los procesos, alertas y respuestas automáticas ante sucesos, y no menos importante la red 5G, que será la encargada de la conexión, las redes, las comunicaciones y en general de todas las interacciones cibernéticas, ya que del internet depende que todo lo demás funcione adecuadamente. Así las cosas, como se puede observar las ciudades inteligentes en si forman a su vez una infraestructura critica debido a su complejidad y esencia, que al mismo tiempo

depende de otras entidades críticas, y esta hipótesis planteada en este trabajo espera ser comprobada a futuro, puesto que lo anterior es apenas una visión, pero que cada día se acerca más a la realidad, ya que con el transcurrir de los años las ciudades destinan más presupuesto en su transformación.

Tras la pandemia de COVID-19 la UE, ha querido impulsar varios planes de mejoramiento, impulso y recuperación, en todo lo que tienen que ver con la seguridad de internet, ya se pudo observar como las directivas y reglamentos venideros están encaminados hacia la resiliencia de las instituciones, empresas y sectores críticos o no. Pero el interés de la UE no se queda en nuevas regulaciones, sino que va más allá, el programa Europa Digital[5] destinado a ser desarrollado entre el 2021 y 2027 es un ambicioso, pero necesario plan que permitirá la implantación de nuevas tecnologías, con el fin de acelerar la mutación digital de las sociedades y las economías europeas, sin dejar de lado el componente de ciberseguridad que todo esto requiere. Las nuevas tecnologías son una realidad y cada vez más los avances en estos ámbitos son abismales, con todo y ello, que mejor que su adaptación y ejecución en las sociedades, empresas y ciudades este acompañada de normas, estudios y bases sólidas para hacerlo.

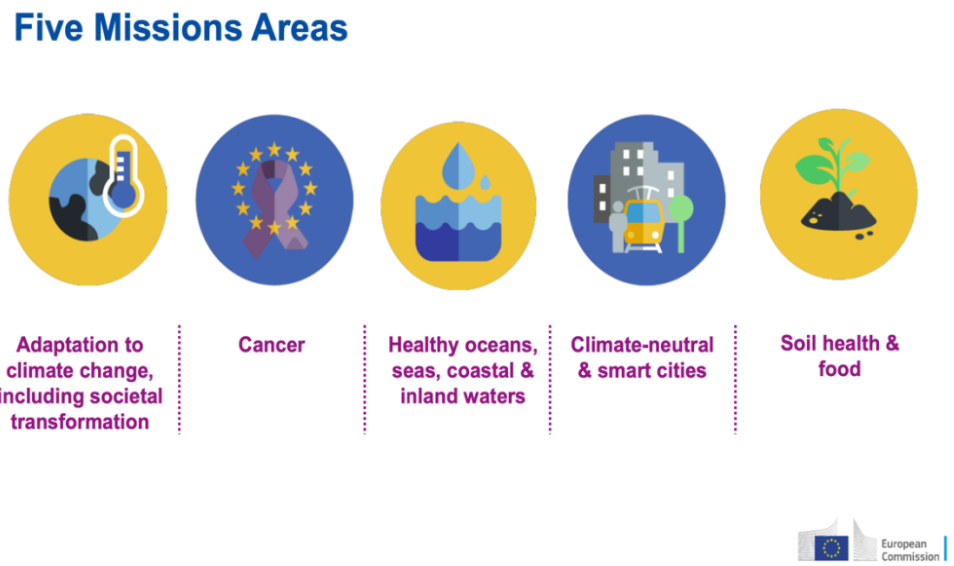
Hay un punto muy importante en toda esta inmersión, inversión y procura que tiene la UE, y es aquel de no improvisar; el mundo especializado, los profesionales del área y los países desarrollados saben que en temas de nuevas tecnologías no hay lugar a equivocaciones, es por esta razón que los nuevos programas y planes que pretende la Unión Europea se complementan entre sí, hablamos allí de las directivas de resiliencia CER, NIS2 y DORA; la Digitalización de las Finanzas; el programa Horizonte Europa[6] que se centra en la investigación y desarrollo tecnológico con el fin de conectar a Europa y hacer de las ciudades

[5] Council of the European Union. (2020). *Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027*. https://data.consilium.europa.eu/doc/document/ST-13835-2020-INIT/en/pdf.

[6] European Commission. (2021). *Horizon Europe*. [presentación] https://research-and-innovation.ec.europa.eu/system/files/2022-06/ec_rtd_he-investing-to-shape-our-future_0.pdf.

más sostenibles e inteligentes, además de avances en ciencia, y la conversión de las industrias en escenarios competitivos, seguros y digitales.

Figura 2.



Fuente: European Commission. (2021). Horizon Europe.

2.1 Internet de las Cosas IdC, Inteligencia Artificial (IA) y Big Data

Como lo hemos venido aludiendo, el principal reto que tienen las entidades criticas es la adaptación al escenario participativo con otros actores, este tipo de infraestructuras desde hace ya varios años atrás saben que deben no solo automatizar sus procesos, sino que convertirse en entes totalmente digitales y tecnológicos, que les permitan estar a la vanguardia del mundo, de las normas y de las personas a las cuales prestan servicios esenciales. La Agencia de la Unión Europea para la Ciberseguridad – ENISA – conoce que todas las nuevas tecnologías que el mundo actual ofrece y que están siendo desarrolladas y mejoradas, tarde o temprano van a ser parte de nuestro diario vivir, y no solo debemos saber cómo convivir con ellas, sino los riesgos que estas suponen en materia de seguridad informática. La atención se ha centrado principalmente en las infraestructuras críticas por excelencia, se hizo mención a que este tipo de

entidades que prestaban servicios públicos esenciales y en muchas ocasiones suplían las necesidades de más de un estado a la vez; tendrían que cambiar su modelo de distribución de prestación ya que para poder interactuar con otros servicios y con las personas mismas deberían ofrecer modelos más cercanos y eficientes.

Un ejemplo claro de ello, es el sector eléctrico europeo, en el 2020 el Centro de Ciberseguridad Industrial – CCI – publicó un informe titulado Smart Grids ante el desafío de la Seguridad[7] en este, se describe los grandes avances, desafíos y atmósferas a los que se tendrá que ver expuesto el sector crítico de la energía en los próximos años. Además de la combinación de tecnologías de la información, tecnologías de operación que abrirá la puerta a un servicio de energía "a la carta" (CCI, 2020), este se tendrá que acoplar y pasará de ser un actor pasivo a convertirse en activo, todo ello gracias a que el servicio será basado en redes inteligentes de distribución, en donde los ciudadanos experimentaran un servicio de calidad. En contexto el "juego" será protagonizado por el internet de las cosas IOT, ya que los contadores[8] y paneles solares estarán conectados a la red, así mismo los aparatos del hogar, los cuales tendrán un consumo más responsable y optimo, serán quienes indiquen sus necesidades eléctricas, claro está, que todo ello basado en los datos que acopien sobre funcionamiento, horarios, costumbres, presupuestos, mantenimientos, etc., información que será compartida 24 horas, 7 días a la semana a los contadores individuales, que a su vez transmitirán la información a la IA que recopila igualmente datos, que ayudaran a la empresa no solo a mejorar su prestación, sino que podrá gestionaran incidentes de manera inmediata, y generando una energía más sostenible y limpia. Sin dejar pasar por alto que toda esta información también será utilizada en pro de mejores proveedores de aparatos, bombillas y un sinfín de elementos que se involucran en el servicio.

[7] Centro de Ciberseguridad Industrial – CCI. (2020). *Smart Grids Before the Security Challenge*. Serie Smart OT, Número 1. Págs. 20.

[8] Ibidem. El elemento más próximo al consumidor es el contador inteligente, que le permite medir el consumo en tiempo real, tarifa por horas, consultar el consumo en la web y, además, facilita a la compañía realizar remotamente la monitorización y el corte de potencia.

Lo que se acaba de exponer, es un modelo muy afable por no decir superficial de como en un mismo servicio confluyen al mismo tiempo el uso de las nuevas tecnologías, puestas en función de un servicio tan esencial como lo es la energía eléctrica; por supuesto que lo anterior a nivel técnico tiene todo un mundo de conceptos y niveles de funcionamiento más complejos, pero que para efectos de esta idea no es necesario explicar. Ahora bien, para que la prestación de un servicio de estas calidades sea satisfactorio, debemos tener claridad que están involucrados múltiples actores a la vez, lo que genera igualmente preocupación e incertidumbre, puesto que todas los procesos y esquemas que describimos en el párrafo anterior dependen de una conexión a internet, lo que nos hace pensar en que al reto de las infraestructuras críticas de acoplarse y ser parte activa de las urbes inteligentes, le nace una ramificación más, y es hacer que todas conexiones, redes y comunicaciones sean seguras – ciberseguridad -; un reto que para nada desmerece, puesto que la misma ENISA ha venido alertando y llamando la atención sobre la preparación y organización que deben tener los equipos dentro de las empresas, para saber manejar algún tipo de incidencias. La intrusión maliciosa a un contador, a una base de datos, a un centro de distribución o a un proveedor externo podría ser perjudicial, y llegar a consecuencias gigantescas, o pensemos en las implicaciones que tendría para una ciudad que su sistema de sensores de energía de alumbrado público fuese alterado tras un ataque cibernético, y esto es solo la punta del iceberg que podemos ver.

En su informe sobre :Good Practices and Recommendations on the Security of Big Data Systems[9], la agencia incluye al sector de la energía como uno de las grandes industrias en el uso de información a niveles mayúsculos y refiere:

> *"Infrastructure security: Since smart meters are the main devices to collect information, infrastructure security is a great challenge. The notion of cyber*

[9] European Union Agency For Cibersecurity. (2015). *Good Practices and Recommendations on the Security of Big Data Systems*. https://www.enisa.europa.eu

physical security, has become another important aspect we should investigate when discussing cyber security challenges. Big data is the system mostly used for the collection and analysis of data coming from sensor networks, smart meters, etc - so this challenge is directly linked to the Big Data implementation.[10]*"*

La Agencia Europea de Ciberseguridad conoce de primera mano el camino que lleva cada infraestructura critica por ello ha emitido en los últimos años informes para el transporte de tren, aeropuertos, puertos, para hospitales y centros de salud, para el sector financiero, para el sector vial, para los vehículos, para las telecomunicaciones, para los chips de móviles, entre otros, en común todos desvelan los avances y riesgos en ciberseguridad a los que se enfrentan. El funcionamiento de entidades criticas dentro de una ciudad inteligente supone un cambio en la prestación de los servicios esenciales y más básicos, utilizando la tecnología como eje principal, las ciudades inteligentes estarán inundadas de sensores, aparatos e información; la vida cotidiana tal y como la conocemos ahora será más sencilla, gracias a las nuevas tecnologías, el agua será de mejor calidad y su consumo más consiente, la energía será controlada y las fuentes de renovación serán comunes, los autos serán eficientes, las vías serán más seguras y sabrán gestionar el tráfico en tiempo real, el sector financiero será virtual y no volveremos a pisar un establecimiento físico, seremos atendidos por IA que podrán resolver cualquier tipo de situación en segundos ya que tendrán todos nuestros datos en instantes, las calles siempre estarán limpias, la policía podrá predecir altercados o delincuencia y las zonas serán más seguras, las cámaras de vigilancia y de reconocimiento facial recopilaran datos las 24 horas de todos los días, entrar a los edificios del gobierno será una tarea sencilla, la administración al igual será virtual y tan cercana que pareciese que los problemas se resuelven pocos instantes, en síntesis todo el manejo, organización, inquietudes, servicios, trámites y lo que se nos ocurra lo tendremos al alcance de nuestra mano en un

[10] Seguridad de la infraestructura: dado que los medidores inteligentes son los principales dispositivos para recopilar información, la seguridad de la infraestructura es un gran desafío. La noción de seguridad física cibernética se ha convertido en otro aspecto importante que debemos investigar al discutir los desafíos de la seguridad cibernética. Big data es el sistema más utilizado para la recopilación y el análisis de datos provenientes de redes de sensores, medidores inteligentes, etc., por lo que este desafío está directamente relacionado con la implementación de Big Data.

aparato móvil, que será la llave, y la puerta hacia un mundo conectado del que el ciudadano hará parte activa.

2.2 Servicios en la nube (Cloud service)

Sin duda es el gran protagonista en todo este panorama de las Ciudades Inteligentes y la conexión total, no solo porque la normativa Europea y local ya reconoce la importancia de salvaguardar este tipo de servicios y sus infraestructuras, sino porque es parte esencial de la prestación de servicios críticos y como tal es uno de los mayores activos de las entidades esenciales, los datos y la información suponen hoy en día un intangible de valor incalculable, lo que hace atractivo a los ojos de los ciberdelincuentes, el robo de datos, o una violación de seguridad al espacio en donde se almacenan la información privada de las personas, tendría un impacto gigantesco.

En las metrópolis del futuro los servicios de alojamiento de datos serán una entidad crítica que deberá estar más que protegida, datos de toda clase se alojaran en la nube, y lo más seguro, según los planes de la UE es que exista una sola base de datos, para que las entidades públicas y privadas la consulten y extraigan la información que requieran. La ciberseguridad entonces entrará a jugar un papel predominante y por ende las normas que existen en la materia deberán ser cumplidas a cabalidad no solo por el alto riesgo que implicaría un ataque a este tipo de entidades, sino por la cantidad de organizaciones y personas a las que afectaría. Aunque el blockchain es una alternativa a estos riesgos, aún falta investigación para que esto pueda ser aplicado, ya que no existe ningún sistema totalmente blindado.

ENISA viene hace ya algunos años, desde su informe en 2013, advirtiendo sobre los peligros, cuidados y recomendaciones que se deben implementar, cada vez son más las empresas que optan por migrar sus datos a este tipo de servicios, convirtiéndolas al instante en blancos de ataques cibernéticos. A raíz de la pandemia del COVID-19 fueron muchas las Infraestructuras Críticas que

decidieron alojar sus datos en la nube, ejemplo de ello es la banca o el sector sanitario, tal implicación tuvo esto que la agencia de ciberseguridad de la UE, publicó en junio de 2021 un informe sobre la seguridad en la nube para servicios de salud, al ser uno de los sectores que mas incrementó sus amenazas y ataques cibernéticos. En España el gobierno decidió durante la pandemia tratar a los centros de datos como Infraestructuras Críticas, catalogando además a sus empleados como esenciales, tras la importancia que tomó dicho servicio, No obstante el camino aun en largo, ya que el ideal es que todo el sector que componen este servicio, se sientan confiados para migrar la información, y allí emerge la importancia que tienen las regulaciones en ciberseguridad, generar confianza y soluciones efectivas, instituciones sólidas y una gran inversión en digitalización, son apenas los primeros elementos que se necesitan para que esta clase de servicios y los datos de que manejan sean totalmente alojados en la nube. Aunque sin duda llegaremos a ello, integrando el sector salud a otros sectores en donde se maneje una sola información.

Esta entidad crítica hará parte activa de las ciudades inteligentes y por ende cada empresa o entidad utilizará el modelo[11] de "nube" que más se ajuste a sus necesidades, sin que ello signifique que exista un modelo totalmente seguro e inmune a los ciberataques, puesto que, así como pueden violentar toda una

[11] Infraestructura como servicio: en IaaS, el proveedor entrega recursos informáticos (hardware virtual), accesibles en línea. El software que proporciona acceso a los recursos se denomina hipervisor. En términos generales, hay dos tipos de recursos: poder de procesamiento (incluidos los recursos de red) y almacenamiento (en bloque) (recursos de memoria). Los ejemplos incluyen Elastic Compute Cloud de Amazon, Compute Engine de Google, Amazon Simple Storage Service, Dropbox, Rackspace, etc. Tenga en cuenta que los servicios de almacenamiento de objetos (por ejemplo, Dropbox) a menudo se consideran SaaS.; Plataforma como servicio: en PaaS, el proveedor ofrece una plataforma, o más precisamente, servidores de aplicaciones, para que los clientes ejecuten aplicaciones. Los proveedores de PaaS a veces proporcionan una herramienta de desarrollo de software para la plataforma. Ejemplos de aplicaciones que se ejecutan en estas plataformas son los scripts (PHP, Python, por ejemplo) o el código de bytes (servlets de Java, C#). Los ejemplos incluyen el motor de aplicaciones de Google, Microsoft Azure, Amazon Elastic Beanstalk, etc.; y Software como servicio: en SaaS, el proveedor ofrece software o aplicaciones completos a través de Internet. Las aplicaciones van desde servidores de correo electrónico, editores de documentos, sistemas de gestión de relaciones con los clientes, etc. A menudo se puede acceder a los servicios SaaS con un navegador o un cliente de servicios web. Tenga en cuenta que no es raro que los proveedores de SaaS ejecuten sus aplicaciones en un IaaS o PaaS de otro proveedor. Un ejemplo es el sitio de transmisión de video Netflix (SaaS) que se ejecuta en los servicios informáticos de Amazon AWS (PaaS/IaaS).

infraestructura de la nube (IaaS), también lo pueden hacer mediante una aplicativo de software (SaaS) y de ahí llegar hasta la entidad crítica.

Hablar de servicios en la nube es mencionar el tema de protección de datos personales, el RGPD contiene obligaciones expresas en cuanto al tratamiento que se debe dar a este tipo de datos, y ello va muy de la mano con la intención futura de crear una base general de datos alojada en la nube, las futuras urbes inteligentes y toda su estructura de redes y conexiones, tendrá como activo los datos de sus ciudadanos, datos que en su mayoría serán privados, y las instituciones de ciberseguridad deberán proteger dicha información, a través de estrategias y aplicación de regulación específica, el cifrado de datos, la seudonimización, la portabilidad y la educación en protección de datos serán las primeras medidas de seguridad que se deberán aplicar en todos las Infraestructuras Críticas que manejen datos personales o sensibles, la misma ciudad será desde cualquier bando un atractivo blanco para causar daños significativos, convirtiendo a la ciudad en una entidad esencial propiamente dicha.

2.3 Red 5G

En una ciudad inteligente no solo hablamos de edificios, vías, autos, servicios, gobierno y personas conectadas, nos referimos también a las conexiones, comunicaciones y redes las cuales deben ofrecer una interoperabilidad perfecta para que todos los elementos de la ciudad funcionen y así puedan interactuar, recopilar datos y mantener una línea de seguridad constante. La UE reconoce la importancia de estas redes para el futuro de las Infraestructuras Críticas, y es consciente de la necesidad de protegerlas, además de generar medidas y normas que ayuden a mitigar los riegos cibernéticos que muy seguramente van a surgir.

La seguridad de las redes 5G es un objetivo cardinal para la UE tanto así que viene trabajando en una serie de estrategias y recomendaciones que ayuden a

sobrellevar los ataques y daños que se puedan causar a este tipo de entidades críticas, los planteamientos combinados y la cooperación entre los estados serán claves para contrarrestar ataques y evitar consecuencias. Los Estados miembros acordaron que disponer medidas estrictas a los operadores y terceros que intervengan en la prestación del servicio, así como dotar de competencias a las autoridades nacionales para que sean estas las que restringir, requerir, o prohibir el suministro, despliegue de redes o la explotación de equipos; Entre las recomendaciones[12] más importantes podemos resaltar las siguientes:

- Reforzar los requisitos de seguridad aplicables a los operadores de redes móviles (por ejemplo, controles estrictos de acceso, normas sobre el funcionamiento seguro y la supervisión, limitaciones a la externalización de funciones específicas, etc.);
- Evaluar el perfil de riesgo de los proveedores; en consecuencia, aplicar las restricciones pertinentes a los proveedores considerados de alto riesgo, incluidas las exclusiones necesarias para reducir eficazmente los riesgos, en el caso de los activos clave definidos como críticos y sensibles en la evaluación coordinada de riesgos hecha a escala de la UE (por ejemplo, funciones básicas de la red, funciones de gestión y organización de la red, y funciones de acceso a la red);
- Velar por que cada operador tenga una estrategia adecuada de múltiples proveedores para evitar o limitar cualquier dependencia importante de un único proveedor o de proveedores con un perfil de riesgo similar, garantizar un equilibro adecuado entre los proveedores a nivel nacional y evitar la dependencia de proveedores considerados de alto riesgo; esto también exigirá evitar situaciones de dependencia de un único proveedor, sobre todo mediante el fomento de una mayor interoperabilidad de los equipos;

[12] ENISA y Los Estados Miembros de la Unión Europea. (2020). Report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity - Informe sobre los Procesos Registrados. https://digital-strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity

Todo lo anterior con el fin último de mantener una cadena de suministro de red 5G diversa y sostenible, y esto se logra a través del control de inversiones que quieran manipular el mercado y con objetivos de seguridad concretos, elaborando regímenes de regulación y certificación que promuevan productos, aparatos, conexiones y procesos más seguros, así como la adopción de una serie de medidas que puedan restringir la participación de operadores que signifiquen riesgo. Lo anterior de cara a lo que serán las ciudades del futuro y su seguridad, en donde las redes 5G por lo que conocemos son más centralizadas y por lo tanto es necesario la instalación de más antenas y elementos que permitan su desempeño, lo que genera un riesgo mayor al tener tantos puntos de acceso y por eso tan importante la supervisión a los operadores. En ultimas lo que quiere lograr la UE con el apoyo de los Estados, es que este tipo de entidades críticas también tengan las herramientas para hacerle frente a las ciberamenazas y lo que viene detrás de esto, al igual que sean resilientes ante cualquier daño o incidente, por lo que quiere que los operadores de la red no dependan de un solo proveedor de servicio, sino de varios, lo que permita una mayor capacidad de respuesta y una continuidad del servicio casi inmediato, no olvidemos que las Ciudades Inteligentes funcionaran gracias a la conexión y la perdida de esta ocasionaría una daño significativo en la red, y en las demás entidades críticas que funcionen con ella, generando un impacto en la propia ciudad y en los ciudadanos.

También compone una parte importante de este trabajo mostrar como estas nuevas entidades críticas que llamamos ahora nuevas tecnologías, pero que en un futuro próximo serán la base de todo el funcionamiento y despliegue digital de las ciudades; suponen nuevas exigencias y retos en materia de ciberseguridad, a pesar de que seguirá existiendo el riesgo de ataques físicos terroristas (Atenas, puntos de acceso, edificios de servidores) o la llegada fortuita de un fenómeno natural que afecte la operación, la verdad es que ahora el centro de atención está en los incidentes y peligros que se corren si un ciberataque logra desestabilizar toda una ciudad o un Estado, dejando sin servicios esenciales a sus habitantes, desconectando la ciudad por completo y teniendo acceso a todos los

datos que componen dicho sistema. Que más daño significativo que un ataque de este tipo a una metrópolis inteligente, no solo se vería afectada una sino varias por no decir todas las Infraestructuras Críticas que la componen,

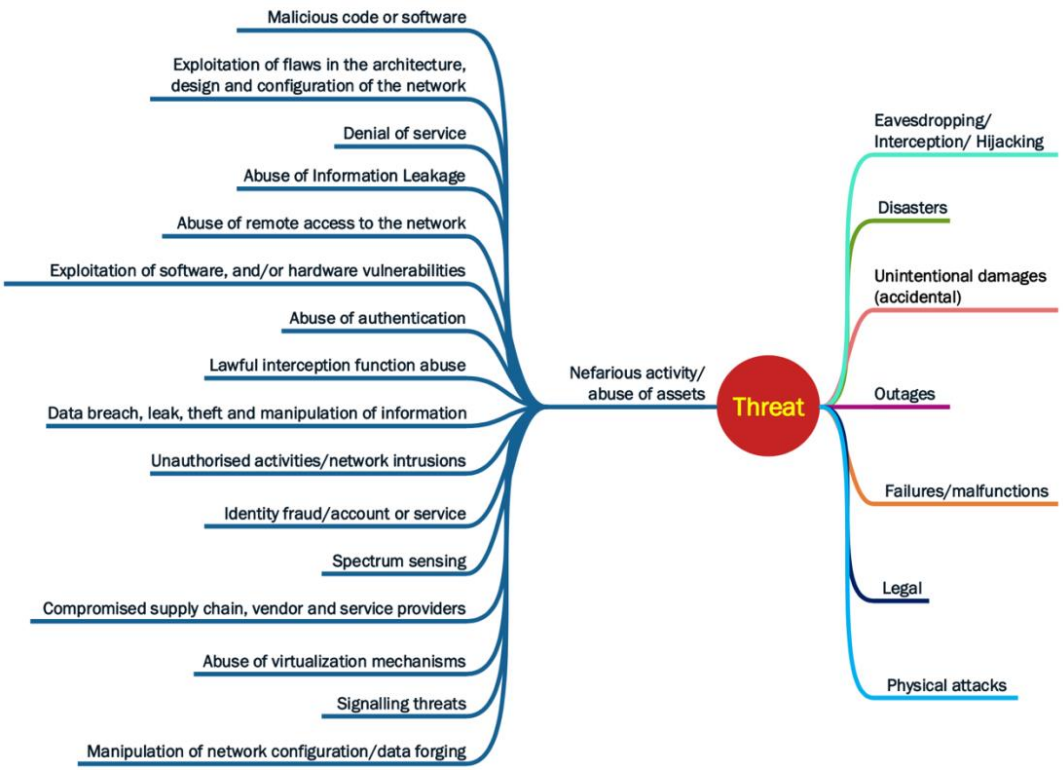
Ya se ha recalcado en la jerarquía que tiene la Red 5G para la UE y por ello sus estrategias, planes y recomendaciones van dirigidas a desarrollar estos ítems principales, como medidas que ayuden a reducir riesgos y aminorar los impactos luego de un ataque cibernético.

- Las medidas estratégicas definidas en el conjunto de herramientas se componen de medidas relativas a una mayor competencia reglamentaria de las autoridades para controlar la contratación y el despliegue de las redes, medidas específicas para abordar los riesgos relacionados con los puntos vulnerables no técnicos (por ejemplo, el riesgo de interferencia por parte de terceros países o agentes apoyados por estos), evaluación del perfil de riesgo de los proveedores e iniciativas de apoyo al fomento de proveedores de 5G sostenibles y diversos.
- Las medidas técnicas definidas en el conjunto de instrumentos van desde el estricto control del acceso a las redes y su gestión, explotación y supervisión seguras hasta la certificación de componentes o procesos de las redes 5G.
- Las acciones de apoyo constan de medidas en el ámbito de las normas de las redes 5G, consistentes en el refuerzo de las capacidades de ensayo y auditoría, la mejora de las labores de coordinación en caso de incidentes o la garantía de que los riesgos de ciberseguridad se tengan plenamente en cuenta en los proyectos 5G financiados por la UE. Estas acciones de apoyo pueden facilitar, auxiliar y mejorar la eficacia de las medidas estratégicas y técnicas.[13]

[13] ENISA y Los Estados Miembros de la Unión Europea. (2020). Report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity - Informe sobre los Procesos Registrados. https://digital-strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity.

El más reciente informe sobre la red 5G y el panorama de las amenazas *"ENISA THREAT LANDSCAPE FOR 5G NETWORKS*[14]*"* da cuenta y recalca la importancia que va a tener esta tecnología, en todos los ámbitos donde se apliquen, y a pesar de la red no está funcionando de manera total, hay algunos campos y entidades que lo usan, sin embargo y tal como lo advierte la agencia, una vez la red 5G comience a desplegar sus redes y con ellas todas las conexiones que permitirá y los avances que va a generar; en campos como la medicina, transporte, agricultura, comunicaciones, en el IdC, en las IA, en los servicios cloud por mencionar algunos, los riesgos aumentaran de manera significativa. El informe describe alrededor de 80 amenazas potenciales directas a este tipo de redes divididas en 7 categorías, un paisaje del cual se espera mucho en temas de ciberseguridad, que en ultimas resulta ser el pilar principal para que todos los elementos, servicios y redes que dependen de las redes 5G funcionen y con ello las entidades críticas a su vez puedan ofrecer bienestar a las personas.

Figure 14 - 5G Threat Landscape (Summary)



[14] European Union Agency For Cibersecurity. (2019). *THREAT LANDSCAPE FOR 5G NETWORKS*. https://www.enisa.europa.eu.

3. FUTURA NORMATIVA EUROPEA

Nos hemos referido ya, al gran avance tecnológico, físico y estructural por el que han pasado las infraestructuras críticas, ello no solo se debe a que todas estas empresas y sistemas deben estar a la vanguardia del mundo, y por ende en la capacidad de ofrecer no solo un servicio como tal, sino un servicio dotado de tecnología y soluciones digitales que respondan a las necesidades de los habitantes que las demanden. En pro de fortalecer dicho camino que aún es largo, los estamentos de Unión Europea han procurado por actualizar y crear nuevos preceptos normativos que se adapten a los cambios efectuados o los que están por venir.

Figura 1.

Fuente: cybersecurity EU external action, en www.eeas.europa.eu (2021)

Europa no es el único que ha puesto la mira en mejorar y reformar leyes, Estados Unidos uno de los países lideres en infraestructuras críticas y, por ende uno de los estados en donde sus empresas más son atacadas cibernéticamente, ha publicado a través de la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) un informe sobre las recomendaciones en ciberseguridad[15] aplicadas a las entidades críticas en territorio americano, tanto el Gobierno, como el Departamento de Seguridad Nacional reconocen la importancia que tiene el sector para el buen funcionamiento de sus ciudades y el bienestar de sus habitantes, por lo que la ciberseguridad es considerada una prioridad, por consiguiente el informe mencionado se basa entre otros en los siguientes puntos; conciencia en las ciberamenazas, implementar medidas de

[15] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. (2022). *Cross-Sector Cybersecurity Performance Goals And Objectives*. https://www.cisa.gov/cpgs.

seguridad cibernética antes de que sucedan los ataques tanto en los grades sectores como en las medianas y pequeñas empresas, la inversión temprana en ciberseguridad es más eficaz y barata, la seguridad cibernética es un valor añadido para los clientes. Además de lo anterior el actual gobierno ha destinado importantes sumas para reforzar la seguridad de sus infraestructuras críticas, poniendo en marcha planes de resiliencia y colaboración con entidades del orden mundial que le hacen frente a una ofensiva que apenas está por comenzar.

El tema está pasando por sus años más cruciales, en donde las decisiones que se tomen mundialmente ahora fijaran la hoja de ruta para los tiempos venideros, cabe resaltar que el pasado mes de mayo de la presente calenda, se celebró en la ciudad de Bilbao – España, el *ÚSEC BILBAO CONGRESS 22*, evento expositivo referente a la industria de la seguridad, movilidad y emergencia en general, allí tuvo lugar una importante y destaca mesa redonda para los fines de este trabajo; la cual fue denominada *"la protección de infraestructuras críticas y estratégicas. Optimizar su seguridad contra agresiones deliberadas, especialmente, contra ataques terroristas"*[16], en el evento se hizo presente el director del Centro Nacional de Infraestructuras Críticas de España (CNPIC) entre otros ponentes, el cual mencionó la importancia que tiene el nuevo enfoque que la Unión Europea le está brindando a las entidades críticas y que tiende a la resiliencia de las mismas como fundamento principal de la nueva regulación y planes a futuro. Además, recalcó la importancia que tiene la integración, la coordinación y la comunicación entre las entidades encargadas de la ciberseguridad en los estados de la UE.

De su intervención podemos resaltar la exposición que realizó sobre las próximas normas que la Unión Europea está debatiendo y pretende implementar en los Estados miembros, hizo hincapié en tres modelos regulatorios que serán

[16] ÚSEC BILBAO CONGRESS 22 (26 de mayo, 2022) "la protección de infraestructuras críticas y estratégicas. Optimizar su seguridad contra agresiones deliberadas, especialmente, contra ataques terroristas". https://congress.usecim.es/mesa-redonda-la-proteccion-de-infraestructuras-criticas-usec-bilbao-congress-2022/

bandera en el tema de ciberseguridad de las Infraestructuras Críticas y por ende más temprano que tarde las veremos traspuestas en las legislaciones propias de los Estados. En primer lugar, se habló de la importancia que tienen las entidades criticas dentro del bienestar para los habitantes de uno o varios Estados, en donde las empresas (públicas o privadas) al ofrecer servicios esenciales, proporcionan los medios básicos y necesarios para la subsistencia de los ciudadanos y el funcionamiento del mercado interno estatal o comunitario. El objetivo de esta regulación es que las infraestructuras críticas no solo tengan los protocolos y procesos definidos – como los tienen – ante ataques terroristas *in situ*, catástrofes naturales o incidentes de carácter técnico, sino que tengan ahora la capacidad de enfrentar además de lo mencionado, las emergencias sanitarias que se puedan presentar y las irrupciones en materia de ciberseguridad, tanto terroristas como delincuenciales.

El fin último que pretende la directiva, es dotar de las herramientas suficientes para que dichas entidades criticas reduzcan sus vulnerabilidades y aumenten la resiliencia física que se debe tener ante una situación de índole sanitario o peor aún un ataque cibernético, lo último teniendo en cuenta que a futuro la gran mayoría de las cosas van a estar conectadas a internet y ello supone no solo un riesgo gigantesco, sino un reto en cuanto una infraestructura critica debe recuperarse lo más rápido posible para seguir prestando un servicio vital e impactar lo menos posible a la población, a pesar de que la Directiva no lo indica expresamente, se puede deducir que la UE está allanando el camino para establecer un marco en donde también estén incluidas las ciudades inteligentes, al ser una norma más abierta y con posibilidad de decisión por parte de los mismos gobiernos.

Con todo y lo anterior, la directiva CER[17] que actualizaría la propia de 2008, además de aumentar e incluir nuevos sectores en su aplicación, tiende a instar a que las entidades criticas detecten los riesgos que ante una situación de peligro

[17] Tabla 1 - en acápite de tablas

puedan afectar de forma significativa la prestación de los servicios, de igual forma se aspira a que luego de este análisis las empresas adopten desde una etapa temprana las medidas adecuadas que garanticen su capacidad de superación y recuperación ante cualquier acontecimiento dañino. Resulta de gran valor la intención que tiene tanto el Consejo como el Parlamento Europeo para que los incidentes que se presenten, ya sean contrarrestados o no, sean notificados inmediatamente a las autoridades pertinentes, esto con el objeto de alimentar el conocimiento sobre los mismos, en el caso puntual de los ataques cibernéticos, se quiere que casi de manera inmediata las autoridades de ciberseguridad de los Estados miembros conozcan todos los detalles de las arremetidas a través de internet y así poder ir un paso delante de los delincuentes.

En segundo lugar, se mencionó la normativa referente a las entidades financieras (reglamento DORA[18]), que sin duda representa y encabeza un sector de la sociedad esencial y crítico, no solo por ser la infraestructura encargada del capital de las personas naturales o jurídicas, sino por el gran tamaño de la información y datos que tienen en su poder las empresas de este tipo; la Unión Europea, no es ajena a la atención que merecen este tipo de infraestructuras, y por ende ha diseñado un plan aislado que se complementa con los anteriores aquí mencionados, pero que proporciona una serie de pautas especificas a las compañías que se encuentren operando dentro de la esfera bancaria y financiera, se puede incluir allí, a las compañías de seguros, y empresas de inversión.

La UE tiene preparado un paquete regulatorio, el cual consta de una serie de planes y medidas que no solo refuercen la resiliencia dentro de las organizaciones, y mitiguen los riesgos cibernéticos; también ofrece una propuesta sobre el mercado de criptoactivos, finanzas digitales (euro digital) y la descentralización de la tecnología de registro. Lo que se quiere lograr con la

[18] Tabla 2 – en acápite de tablas

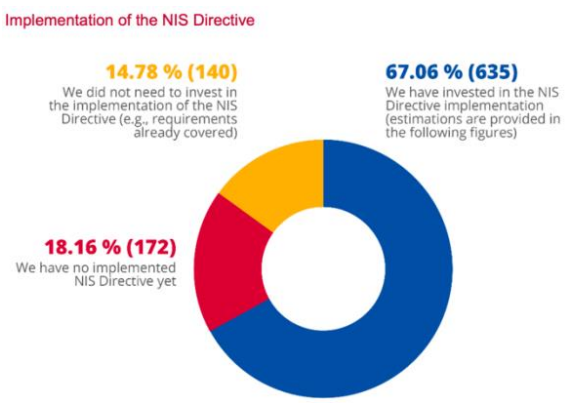
estrategia mencionada es generar confianza en el consumidor financiero, así como fomentar la inversión, contrayendo un sistema de capital digital seguro dentro y fuera de Europa, no estamos alejados de que las operaciones monetarias sean totalmente digitales, los smart contracts regulen todos los tipos de contratación, y la banca digital sea la única existente; serán entonces las ciudades inteligentes las que ofrezcan estas y otras posibilidades, es por ello que este paquete de medidas es tan llamativo y muy seguramente será de fácil aplicación en las urbes de "futuro" pues está pensado en el manejo que tendrá el mercado bancario y asegurador, además de la seguridad cibernética que esto demanda.

Por último, se explicó la actualización que tendrá la directiva NIS, y dichos ajustes merecen un apartado especial para los objetivos de este trabajo, ya que, al estar destinadas entre otras a las entidades críticas, resulta interesante realizar un análisis de como esta nueva y ajustada regulación puede ser aplicada a las ciudades inteligentes vistas como Infraestructuras Críticas.

3.1 Aspectos relevantes de la Directiva de (NIS)

La ciberseguridad es la primera línea y por consiguiente una barrera de gran importancia contra las ciberamenazas, es y ha sido una de las premisas de la Unión Europea en cuanto a ciberseguridad se refiere. Con la publicación de la primera estrategia de ciberseguridad de las redes y de los sistemas de información, y como ya habíamos hecho referencia se abrió un camino de cara a enfrentar este tipo de situaciones que con el pasar de los años sigue en aumento, así las cosas, la NIS como pionera regulación comunitaria en materia de ciberseguridad se basó en poner su atención bajo dos sectores relevantes y que usan internet para si funcionamiento y operación, y limito dos categorías, por un lado tenemos los operadores de servicios esenciales (OES), que son aquellas entidades privadas o públicas que tiene a su cargo la prestación de servicios

masivos básicos y necesarios para el funcionamiento de la sociedad y que lo hacen utilizando IT, se hace referencia entonces entre otros a las empresas del sector salud, energético, financiero, digital, etc., en otras palabras Infraestructuras Críticas[19]; en segundo lugar encontramos a los prestadores de servicios digitales (DSP) los cuales son, los mercados en línea, los moteres de búsqueda en línea, y los servicios de almacenamiento en la nube - lo que conocemos como cloud computing -.



Cabe mencionar, con fines enunciativos los aspectos más relevantes que trataba la norma (NIS), y que se convertían en obligaciones para los operadores que cumplían con las condiciones ya descritas. Por tanto, obligaba a que las empresas gestionaran medidas técnicas de ciberseguridad según su organización y estructura, además de tener en cuenta la operación que realizaba; obligaba a que cada entidad contara con un responsable de la seguridad de la información dentro de la empresa; y obligaba a que todos ataques o incidentes relevantes de ciberseguridad que sufrieran debían ser comunicados, so pena de recibir sanciones por el silencio guardado.

Como podemos dilucidar la normativa es bastante completa y diáfana sobre los sectores que aplica, y para ser verdad desde la fecha de su publicación (2016) ha desempeñado un papel radical en las entidades, y ello queda demostrado con las cifras que en 2021 ENISA público, en su informe titulado "NIS INVESTMENTS[20]" el cual recopila una serie de datos, estadísticas y análisis de la inversión, que han

[19] Según la NIS existen tres criterios para considerar que una entidad pertenece al sector crítico-esencial: las alternativas posibles al servicio que prestan, midiendo el número de (posibles) afectados y por la extensión geográfica o cuota de mercado a la que pueda afectar un incidente grave tenga efectos perturbadores, que puede ser a uno o varios estados.

[20] European Union Agency For Cybersecurity. (2021). *NIS Investments*. Págs. 1-86

realizado las empresas en el cumplimiento de las obligaciones establecidas en la directiva.

Los datos que presentó el informe se recopilaron a través de una encuesta de **947 organizaciones identificadas como OES/DSP en los 27 Estados miembros**, arrojando los siguientes datos[21] relevantes:

- En general, el 48,9 % de las organizaciones encuestadas reconoce un impacto muy significativo de la Directiva NIS en su seguridad de la información (SI).
- El 50 % de los OES/DSP establecidos dentro de la UE cree que la implementación de la Directiva NIS ha fortalecido sus capacidades de detección, mientras que el 26 % cree que ha fortalecido su capacidad para recuperarse de incidentes.
- El 67 % de OES/DSP requirió un presupuesto específico para la implementación de la Directiva NIS, con un valor medio de 40.000 € o el 5,1 % de sus presupuestos generales de seguridad de la información. Alrededor del 50 % de las organizaciones necesitaron una media de cuatro empleados adicionales a tiempo completo para la implementación, ya sea mediante contratación o subcontratación.
- El coste directo estimado de un incidente importante de seguridad es de 100.000 € de media, siendo los sectores bancario y sanitario los que experimentan los costes más elevados de este tipo.
- Entre 300.000 € y 213.000 € respectivamente. son los costos relacionados con las pérdidas de ingresos y la recuperación de datos o la gestión de la continuidad del negocio.
- El 9 % de las organizaciones ha sufrido un incidente de seguridad importante que ha afectado a las partes interesadas externas.
- Más del 50 % de los OES/DSP encuestados certifican sus sistemas y procesos.

[21] European Union Agency For Cybersecurity. (2021). NIS Investments. Págs. 1-86

- La mayoría de los OES/DSP encuestados reportan que sus controles de seguridad de la información y cumplen o superan los estándares de la industria, con solo el 5 % informando que no cumplen con esos estándares
- Los resultados indican una fuerte correlación entre una autopercepción muy positiva de madurez de ciberseguridad y la existencia de certificaciones de ciberseguridad para procesos, personas y productos dentro de una organización.

Gracias a la buena gestión implementada por España en el Esquena Nacional de Seguridad (2013) que cobijada al sector público, y que ayudó no solo a posicionar al país como un referente en ciberseguridad, sino que facilitó la transposición de la Directiva NIS en el territorio nacional, bajo los Reales Decretos Ley 12/2018 y 43/2021, el cual es de aplicación para las entidades que presten servicios de carácter esencial para la comunidad en general y que dependan de redes y sistemas de información para el desarrollo de sus actividades, se refiere más específicamente a Infraestructuras Críticas (definidas en la Ley 8/2011), al igual para ciertos proveedores de servicios digitales que por sus características transnacionales deberán limitarse a cumplir con las obligaciones en el territorio donde estén establecidos, y serán las autoridades locales quienes supervisen el cumplimiento de los deberes legales en coordinación con las autoridades correspondientes de otros estados de la UE.

Se mantiene por supuesto la obligación que tienen los OES y DSP de notificar los incidentes que sufran en las redes y servicios de información que empleen para prestar el servicio, siempre y cuando tengan efectos significativos en la labor, aunque también se solicita la notificación de aquellas incidencias que a pesar de no tener un efecto adverso sí que puedan perturbar a un servicio esencial, ello con la finalidad de perfilar dichos riesgos y poder mitigarlos en otras entidades críticas. Y de igual manera estarán obligados adoptar las medidas necesarias para gestionar los riesgos concernientes a las redes y sistemas de información, aunque esta gestión sea externa, por tanto, las obligaciones de seguridad que

asuman dependerán del nivel de riesgo que asuman con la prestación, previa evaluación.

Como punto importante, el decreto ley referenciado (RDL 12/2018) así como el que lo desarrolla (RDL 43/2021) fueron pensados de tal manera que encontrase armonización con las leyes que existían ya en algunas materias, esto para evitar cargas administrativas y legislativas fuertes. En este orden de ideas de manera horizontal se vincula directamente con las Leyes 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, y 36/2015, de 28 de septiembre, de Seguridad Nacional, y con 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, como normativa especial en materia de seguridad de los sistemas de información del sector público.

La cooperación público – privada llama la atención en la legislación, aunando esfuerzos entre los CSIRT y las autoridades públicas de vigilancia con tal de dar cumplimiento a las obligaciones y delimitando el ámbito de acción en sectores específicos, evitando así la existencia de deberes paralelos e innecesarios y reforzando el deber de cooperación y coordinación entre los equipos de respuesta de índole nacional - a través de la Plataforma nacional de Notificación y Seguimiento de Ciberdelincuentes[22]

Además del gran reto y futuras exigencias en materia de ciberseguridad de las Infraestructuras Críticas al ser parte activa de las ciudades del futuro, nacen con esto nuevos requerimientos en la materia, lo que hace que surja la duda sobre, si son suficientes las normas y medidas que se están aplicando.

[22] El procedimiento de notificación de incidentes se articula a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes (artículos 10 y 11), a fin de permitir el intercambio de información entre los operadores de servicios esenciales y proveedores de servicios digitales, las autoridades competentes y los CSIRT de referencia, garantizando la confidencialidad, integridad y disponibilidad de la información (artículos 12 a 14).

3.2 Directiva NIS2 vs las Ciudades Inteligentes

A pesar de que la directiva NIS como se expuso, ofrecía un panorama amplio en cuanto temas de ciberseguridad en los entornos físicos y que tuvieran tecnología de por medio, de los sectores que cobijaba, la comisión consideró que, dicha regulación se quedaba corta ante el vertiginoso crecimiento y avance de la era digital, la pandemia uno de los muchos causantes de dicho salto, forzó a que la mayoría de los sectores diera un presuroso pero necesario cambio hacia la digitalización de sus sistemas, procesos y métodos de ofrecer servicios, si bien es cierto que en el caso de las Infraestructuras Críticas ya existían sectores en donde la tecnología hacia parte de sus procedimientos, los últimos años obligaron a que gran cantidad de empresas esenciales volcaran su atención hacia la digitalización y nuevas técnicas de ofrecer servicios. Sin embargo, todo esto generó una inquietud al interior de la Unión Europea, ya que las amenazas a las que estaban expuestos los sectores críticos aumentaban exponencialmente y con ello las graves consecuencias para los ciudadanos.

Es por todo lo anterior, que la nueva directiva NIS2 quiso hacerle frente a la situación, y de cara al futuro próximo publicó el texto regulatorio, con una premisa principal, aquella de reforzar la ciberseguridad y la resiliencia en entidades y empresas de infraestructuras críticas del sector público y privado en toda la Unión Europea; en este orden de ideas, dicha normativa se basa en 3 áreas claves:

- La ciber resiliencia como factor principal ante las inminentes amenazas que se espera aumenten en los años venideros, según el Centro Criptológico Nacional, en una encuesta publicada por McAfee[23], y realizada a 600 directores de ciberseguridad de compañías criticas alrededor del mundo,

[23] Informe "En el punto de mira: las infraestructuras críticas en la era de la ciberguerra", comisionado por McAfee y realizado por el Centro de Estudios Estratégicos e Internacionales (CSIS)

arrojó[24] que el 54% han experimentado algún tipo de ataque, igualmente un tercio de los indagados, afirmó que considera que el sector en donde trabaja no se encuentra preparado para hacerle frente a posibles ataques cibernéticos de alto nivel. Cabe mencionar que un aspecto relevante de la nueva disposición es la ampliación de los sectores implicados, así las cosas, estarán incluidas además de las infraestructuras críticas que ya se conocen, las grandes y medianas empresas que tengas vinculación o trato directo con empresas críticas o esenciales.

Además, es importante mencionar que esta actualización elimina la distinción entre operadores de servicios esenciales y proveedores de servicios digitales, avance que se torna significativo en tanto que se dará una clasificación basada en la relevancia de la empresa y categorizándolas entre esenciales e importantes.

- La elaboración e implementación de planes operacionales con el objetivo de prevenir, disuadir y responder; a través de la creación de la Unidad de Ciberseguridad[25] la Comisión espera que los Estados Miembros se comprometan y cooperen entre sí, con el único fin de responder y mitigar las consecuencias que puedan dejar los ataques cibernéticos. La idea es fortalecer a las entidades de cada Estado, y firmar una red de cooperación que permita responder de manera efectiva a los ciberataques a infraestructuras críticas.

- La creación de un ciberespacio abierto, esto con el fin de mejorar no solo la seguridad web de la Unión Europea, sino llevarla a un nivel global, siendo los pioneros en leyes, procedimientos y requisitos de seguridad para que sean los demás países o instituciones quienes se adapten a parámetros estandarizados, por medio de los diálogos y la cooperación internacional se

[24] Como resultados relevantes: De media, el coste de la inactividad por los mayores incidentes es de 6,3 millones de dólares al día.
[25] Red Europea de Organización de Enlace de Crisis Cibernéticas (EU CYCLONe)

espera que hasta los países en vía de desarrollo adopten normativas y procesos uniformes que les permitan contrarrestar los ciberataques y de igual forma aportar sus experiencias y métodos para fortalecer el sector cada vez más.

Tabla 1. Cambios más significativos frente a la NIS

NIS	NIS2
CAPACIDADES	
Los estados miembros tienen que mejorar sus capacidades de ciberseguridad.	Mayores medidas de supervisión y ejecución.
	Lista de sanciones administrativas.
COOPERACIÓN	
Mayor nivel de cooperación de la Unión.	Establecimiento de una red europea de organización de enlace en crisis cibernéticas (EU-CyCLONe) para coordinar la dirección de ciberataques a gran escala y crisis a nivel europeo
	Mayor flujo de información entre los Estados miembros y el grupo de cooperación.
	Eliminación coordinada de riesgos identificados en toda la Unión.
GESTIÓN DE RIESGOS	
Los operadores de servicios esenciales y los proveedores de servicios digitales tienen que adoptar prácticas de gestión de riesgos y notificar incidentes a las autoridades nacionales.	Mayores requerimientos de seguridad con una lista de medidas incluyendo respuestas a incidentes y gestión de crisis, manejo de vulnerabilidades, test de ciberseguridad y uso efectivo de la encriptación.
	Aumento de ciberseguridad de la cadena de suministros en especial de las tecnologías de comunicación.
	Responsabilidad de las empresas para cumplir con las medidas de ciberseguridad.
	Obligaciones de informar incidentes, con mayor precisión en los informes.
SECTORES CUBIERTOS	
Salud; Transporte; Financiero;	Salud; Transporte; Financiero;
Infraestructuras digitales;	Infraestructuras digitales;
Proveedores de agua y energía,	Proveedores de agua y energía,
	Proveedores de servicios y redes de comunicaciones electrónicas públicas;
	Servicios digitales: plataformas, centros de datos, redes sociales;
	Gestión de residuos;

	Manufactura de productos críticos
	Servicios postales; Comida;
	Administración Pública

Los ciberataques son el común denominador de esta creciente pero no repentina atención de la Unión Europea, las alarmas se encuentran encendidas hace años, no obstante, con la vertiginosa evolución que han tenido las TIC y el insospechado brinco de la era digital tras la pandemia, el cual la humanidad no tuvo otra alternativa que afrontar y adaptarse de manera casi inmediata, los riesgos en este aspecto se han incrementado, para nadie es un secreto que vamos hacia la "construcción" de ciudades inteligentes, o más que edificación es un tema de conversión, y ello ya lo podemos ver materializado, en la actualidad existen ciudades que han empezado con esta transformación, y si bien aún no se pueden catalogar como Ciudades Inteligentes, han empezado a dar el primer paso para convertirse en metrópolis del futuro, todo esto supone importantes cambios no solo físicos sino, estructurales, ambientales y culturales; además de tecnología y conectividad una urbe inteligente debe ofrecer servicios sostenibles, energías renovables y confianza en materia de seguridad.

En España existen cinco importantes ciudades que están a la cabeza de esta llamada renovación digital hacia una ciudad inteligente, ubicadas en puestos cardinales en el ranking elaborado IESE Business School, el objetivo es estar a la altura de ciudades como Londres, Nueva York, Paris o Tokio; en esta línea han presentado grandes avances en temas de desarrollo aplicando las nuevas tecnologías a la vida cotidiana de sus habitantes, Barcelona, Madrid, Valencia, Sevilla y Málaga han mejorado la calidad de vida de los que allí residen; instalando sensores para mejorar la red eléctrica pública y ahorrando energía; para vigilar la humedad; para controlar el estacionamiento y hasta para controlar el tráfico, instalando cámaras para mejorar la movilidad urbana, implementando sensores para gestionar el ruido, desarrollando planes para el tratamiento de residuos más eficientes, implementando plataformas de atención inmediata al ciudadano, o mejorando la flota de autobuses a 100% eléctricos. Todos estos

avances en parte gracias a Plan Nacional de Ciudades Inteligentes[26] que viene impulsando España desde el 2014 y que quiere posicionar al país como referente en evolución y adaptación tecnológica.

Ahora bien, a lo largo de este escrito se ha dilucidado un panorama bastante amplio en cuanto al futuro y evolución de las Infraestructuras Críticas y su inminente incorporación a las ciudades inteligentes como participantes activos y coordinados, convirtiendo a las urbes en candidatas perfectas a ser catalogadas como entidades esenciales; no obstante la duda se concentra en analizar si las regulaciones y estrategias descritas párrafos arriba, son suficientes para generar un panorama de seguridad en todo lo que tienen que ver con las conexiones, redes y comunicaciones.

El primer punto que merece un examen, y tal vez uno de los más relevantes, es aquel que refiere a la eliminación de la distinción entre operador de servicios esenciales y proveedores de servicios digitales, la Directiva NIS2 da la posibilidad a los propios estados, de que clasifiquen las empresas basadas en la importancia de los mismos, un avance importante en materia de autonomía puesto que aunque se mantendrán las Infraestructuras Críticas de antaño también se situaran en un lugar importante las empresas que desarrollen nuevas tecnologías, lo anterior es la puerta de entrada para que las ciudades inteligentes puedan ser catalogadas como entidades críticas. De igual forma la regulación NIS2 pretende aumentar la seguridad y supervisión de las cadenas de suministros, exigiendo a compañías y gobiernos análisis de riesgos antes y durante la relación, con las entidades esenciales y los proveedores que tengan relación directa con los mismos, sobre todo aquellos especializados en las tecnologías de la información y comunicación – fundamentales en las ciudades inteligentes -. Otro sustancial cambio en miras a aplicar las mencionadas obligaciones dentro de las ciudades inteligentes puesto que la integración de las nuevas tecnologías, la sostenibilidad, y la mejora en la calidad de vida de los

[26] Plan desarrollado por Red.es

ciudadanos comprometen relaciones contractuales con empresas de todo tipo, las cuales a la luz de esta nueva normativa estarán obligadas a implementar y seguir protocolos de seguridad, análisis de riesgos y notificación de incidentes cibernéticos entre otros, fortaleciendo desde base la seguridad y efectuando de manera temprana las medidas de mitigación y eliminación de riesgos.

Cómo no considerar entonces a las ciudades inteligentes Infraestructuras Críticas cuando estas en si albergan a los servicios esenciales, haciendo de los mismos bienes y mercados más sostenibles, además de que comprenden toda una extensa red de comunicaciones, mejorando la vida de los viven en ellas, cualquier incidente de seguridad cibernética podría afectar significativamente a un gran número de la población al mismo tiempo que a otras empresas. Ello a su vez se convierten en una responsabilidad para las propias urbes, la NIS2 le traslada la responsabilidad directa a las entidades críticas de hacer cumplir las medidas y estrategias de seguridad, bajo el lema de la resiliencia y respuesta inmediata ante situaciones de emergencia, esto aplicado a las metrópolis inteligentes es la preparación para que los gobiernos locales preparen y supervisen el acatamiento de las regulaciones, ampliando su responsabilidad ya no solo a la administración digital y las entidades públicas, sino a toda la red privada a través de los canales de cooperación, tal y como lo dispone la actualización NIS2.

En este orden de ideas, podemos afirmar que la UE ha venido labrando el camino y ajustando las disipaciones reglamentarias que en un futuro serán las leyes de los Estados miembros hacia un enfoque totalmente especializado en la era digital, dándole la importancia que se merecen a las nuevas tecnologías y permitiendo que sean estas consideradas también como entidades críticas, los planes y estrategias que hemos mencionado muy someramente en este trabajo dan muestra de la ideología que quiere empezar a implementar la UE, pensamiento que comparten también muchos Estados, los cuales se han adelantado a considerar este tipo de tecnologías y procesos como importantes activos los cuales hay que proteger. La ciberseguridad al igual que la tecnología, son campos que se encuentran en constante cambio, y evolucionan sin freno

alguno, la NIS2 es una normas más abierta y autonómica que permite a Estados y empresas adoptar medidas, clasificar entidades, endilgar responsabilidades y darle un manejo a la seguridad de las redes según sus necesidades siempre aplicando y ciñéndose a los protocolos básicos pero con la posibilidad de ampliarlos hasta donde les sea posible, y claro está con la obligación de comunicarlos y compartirlos con las organizaciones y autoridades de toda la UE.

Las urbes europeas están preparadas para la trasformación que se avecina, sus entidades críticas a pesar de estar cada vez más en riesgo, también están preparadas para afrontarlo, existen a la fecha instituciones estatales, europeas, internacionales de todo tipo, públicas y privadas encargadas de la ciberseguridad con planes y procesos establecidos acoplados a las leyes actuales y siempre listas para hacerles frente a los riesgos que la conexión total implica. El trabajo ahora se centra en generar confianza en las pequeñas empresas, en los ciudadanos que serán los que en un futuro cercano habitaran las ciudades inteligentes; que una persona tenga la certeza de que a pesar que todos sus datos privados o no, se encuentran en nube, que su auto, su casa, su edificio, y los aparatos que lo rodean están recopilando datos las 24 horas, y que todo su entorno, calles, administración, energía, agua, limpieza y demás depende de internet, es un objetivo gigantesco. Educar a la gente en la importancia de la ciberseguridad es un paso que se tiene que dar desde los primeros momentos y al cual propende la UE en sus nuevas normativas.

4. BUENAS PRÁCTICAS EN MATERIA DE CIBERSEGURIDAD

Durante este recorrido en el cual se han expuesto la importancia de las Infraestructura Críticas, su evolución y adaptación a las nuevas tecnologías, y su futuro haciendo parte activa de las ciudades inteligentes; fue importante hacer un análisis regulatorio del contexto en que las normas próximas se aplicaran en

los ámbitos y escenarios que están por venir y en donde las entidades esenciales y las urbes están directamente relacionadas. Las reglas, políticas, estrategias y planes que ha emitido la UE o que esta por publicar, dan una clara muestra de la gran relevancia que tiene la seguridad en el futuro próximo, y no solo porque la mayoría de las cosas se encontrarán conectadas a internet, sino más allá porque nuestros datos, bienestar y cotidianidad dependerán de la seguridad que todo este complejo esqueleto debe procurar ofrecer.

No solo se trata únicamente de emitir normas, imponer obligaciones y realizar estudios y análisis, cooperar y notificar, realizar supervisiones y saber responder; el tema también está en aprender a prevenir y empezar a que la ciberalfabetización sea cada vez más común. La gran mayoría de ataques tienen éxito gracias a descuidos humanos, sea por desconocimiento o por falta de consciencia, como se expuso, las amenazas son cada vez mayores y la onda de expansión de daño que pueden causas cada vez afectará a más personas y servicios a la vez. Las agencias de todo el mundo encargas de la ciberseguridad y la propia ENISA en cada publicación que realizan, dedican un espacio para hablar de recomendaciones y prevención de incidentes, lo que quiere decir que conforma una línea de defensa importante ante las ciberamenazas.

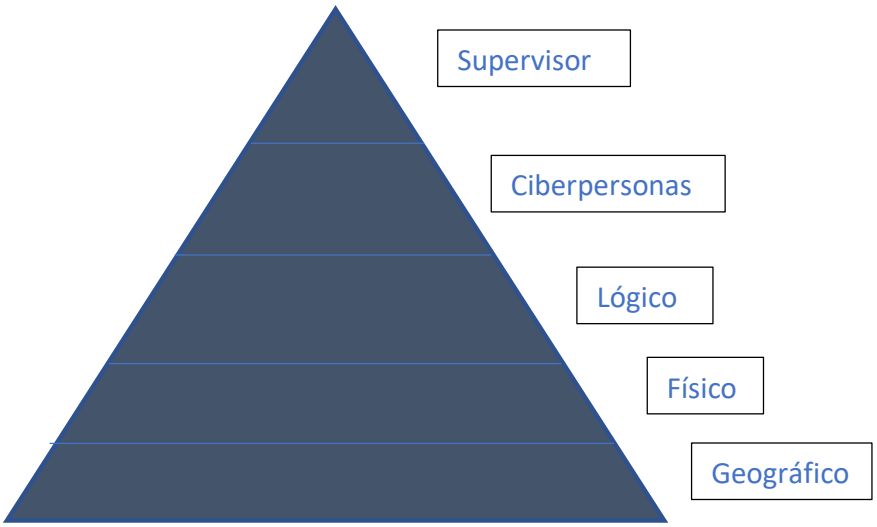
4.1 Planificación y construcción de las Ciudades Inteligenes con ciberseguridad

Mucho se habla sobre las ventajas y beneficios que ofrecen las Ciudades Inteligentes, sobre la llegada de la era digital en su total esplendor y sobre lo sostenible que hará del mundo, sin embargo, es tal la dependencia de este tipo de entidades a las tecnologías de la información, que se convierte en un arma de doble filo. Bajo esta premisa, surge también la necesidad de construir y estructurar las futuras urbes o transformar las que ya existen y están dando el

paso hacia la aplicación de las nuevas tecnologías; alrededor de la ciberseguridad como base fundamental de todo el cambio.

Es evidente que no todas las ciudades son iguales, cada una va a un ritmo distinto y sus problemas son variados, teniendo en cuenta esto y por ende la solución que se quiera dar, cada urbe empezará su metamorfosis tecnológica por un punto distinto, así las cosas, el desarrollo de las ciudades inteligentes será diferente en EEUU al de Europa y África y a su vez al de América. En donde el desarrollo poblacional, la modernización, o la sostenibilidad serán prioridades dependiendo sus necesidades. Sin embargo, hay un punto en el cual todas las ciudades deben confluir, y es aquel en el que sea la transformación que decida, se debe empezar sentando las bases de la ciberseguridad, protegiendo primero las entidades críticas y esenciales. La actualización de la NIS, la directiva NIS2 es más cercana hacia este objetivo, requiriendo un análisis de riesgos previo y constante sobre el funcionamiento de las empresas críticas y todas aquellas que tengan que ver con estas.

Un informe de la Fundación Telefónica sobre la construcción de ciudades inteligentes basadas en ciberseguridad, menciona que conocer de primera mano los planos del ciberespacio en una metrópoli, ayudara a entender como está organizada su infraestructura y TIC desde 5 ángulos, el geográfico, el físico, el lógico, el de las ciberpersonas y el supervisor.



En la base está el plano geográfico, donde reside el físico con los sistemas y los dispositivos de tecnologías de la información. A continuación, está la capa del plano lógico, formado por el modelo de interconexión de sistemas, las aplicaciones, los protocolos de red y los controladores de los dispositivos. Encima se encuentra el plano de las ciberpersonas, que son cuentas asociadas a individuos o grupos. Por último, está el plano supervisor, que incluye las personas, las organizaciones y los sistemas encargados del mando y control (Martín 2015).

Con todo y lo anterior conocer y comprender las interdependencias que tienen las Infraestructuras Críticas es el primer paso para evaluar sus debilidades dentro de las ciudades inteligentes, la NIS2 abre la posibilidad de realizar análisis de riesgos más constantes y tomar las decisiones que sean necesarias para mitigarlos, en razón a esto se deben entonces analizar todos los escenarios posibles de un efecto cascada ante un incidente de ciberseguridad, la conexión y dependencia reciproca que existe entre los sistemas de telecomunicaciones, agua, gas, energía, información y transporte es más de lo que se cree hasta el momento, un simple ataque exitoso al sistema eléctrico de una ciudad inteligente, afectaría de inmediato la generación de comunicaciones, de agua, y de gas, ocasionando perdidas en el agro, el sistema financiero y el transporte por mencionar algunos afectados.

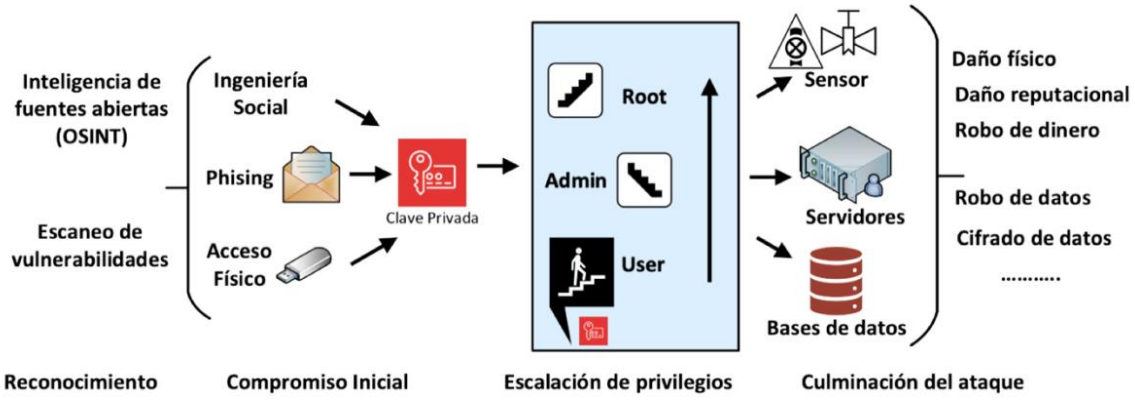
De los que se trata entonces es de construir las ciudades alrededor de la ciberseguridad, y no al revés, aunque resulta más costoso y demorado, en un futuro será más beneficioso para todos, saber cómo es la red antes de implantarla conllevara a la mitigación de daños, la ciberseguridad vista desde los elementos de confidencialidad, privacidad, integridad y disponibilidad debe estar siempre presente antes de edificar o transformar algún sistema. En los futuros planes y estrategias sobre las ciudades inteligentes debe estar presente el tema de la ciberseguridad, y más allá una concepción sobre la “security by design”.

4.2 Estrategias para mejorar la ciberseguridad

No hay mejor táctica de seguridad cibernética que dar cumplimiento a las normas, certificar sus procesos, servicios y elementos, e ir de la mano con las instituciones locales e internacionales creadas para fines cooperativos, no obstante, a lo largo de los informes que la Agencia Europea de Ciberseguridad ha publicado recogen varias recomendaciones generales que se pueden poner en práctica al momento de reforzar la ciberseguridad en las Infraestructuras Criticas.

- Análisis de riesgos, para este asunto es necesario se evalué y conozca uno a uno los activos de la entidad, tanto de software como hardware, así como la ubicación y clasificación de la información, además de saber si se tienen un soporte de la misma o no. Luego de ello es posible ir paso a paso identificando y categorizando las distintas amenazas que pueden surtir y afectar los procesos o sistemas específicos, cabe recordar que las amenazas pueden ser externas o internas y a su vez intencionadas o accidentales. Con esto estudiado se puede entonces identificar qué elementos o servicios poseen mayor valor, y que efectos adversos podría causar un daño en ellos, hay que tener en cuenta que sobre la mesa se deben desplegar la mayor cantidad de escenarios posibles desde el más leve hasta el más grave, luego de realizado lo anterior se podrán implementar soluciones, medidas de seguridad concretas, correctivas, de control y de resiliencia (NIS2).
- Instituir un gobierno de la seguridad, a través de lo anterior se trata de constituir un grupo de trabajo con un marco claro, que conozca de primera mano los recursos tecnológicos y la alineación que tienen con la empresa, con ello es posible realizar estrategias de seguridad de cada tecnología presente, realizando pruebas y midiendo el éxito de las mismas, en otras palabras, se debe implementar un sistema de gestión de seguridad de la información exclusiva de la entidad crítica.

- Diseño de forma integral la seguridad, aquí adquieren valor las operaciones tales como sistemas operativos, antivirus, bases de datos, y todos aquellos elementos que permiten las operaciones de la entidad, es importante conocer los riesgos que tiene el software y saber cómo responder ante un incidente, recuperando lo más pronto posible la operabilidad utilizando las aplicaciones en pro de la seguridad y midiendo el tiempo en cuanto es posible recuperar la información. Las copias de seguridad periódicas según la operación e importancia de la información.
- Definir una arquitectura de seguridad, para esto la red de comunicaciones, de operaciones y de información debe estar diseñado junto con los dispositivos que se utilizan en la entidad.
- Garantizar la seguridad del software principal; aquí los sistemas operativos que utilice la entidad crítica deben estar actualizados, así mismo como gestores de correo, página web, usuarios y contraseñas.
- Controlar de manera adecuada el acceso al sistema, para esto adquiere importancia las instalaciones físicas externas e internas, generar medidas adecuadas para el ingreso y control del personal, así como gestionar los contratos nuevos y extintos, implementando sistemas de bloqueo de accesos y contraseñas una vez las personas no están vinculadas con la empresa.
- Medir la seguridad de forma continua, así como la NIS y la NIS2 lo requerían, esta es una medida muy importante para conocer de primera mano, los riesgos y amenazas según el tipo de operación que desarrolle la entidad. Cubriendo así la mayor cantidad de riesgos posibles y su posible solución.
- Formación y alfabetización, tal vez una estrategia y practica primordial en la prevención de amenazas, es concientizar al personal de los riesgos, mostrando ejemplos reales de phishing, errores en usuarios y contraseñas, robo de datos y las consecuencias significativas a escala que esto puede ocasionar, aplicar esta medida de manera adecuada y constante puede evitar en gran medida el éxito de los ataques cibernéticos, cerrando una puerta de entrada muy amplia y común utilizada por los delincuentes.



Santos, Leopoldo. 2021. “Ciberseguridad e infraestructuras críticas” en: UEM STEAM Essentials

5. TABLAS Y FIGURAS

Tabla 2. Aspectos relevantes de la Directiva de resiliencia de entidades críticas.

NUEVAS CUESTIONES DE LA DIRECTIVA CER
1. Las entidades críticas deben estar preparadas para afrontar emergencias sanitarias, ataques cibernéticos y terrorismo; protegerse, responder y recuperarse de ellos.
2. El texto incluye además de la energía y el transporte; entidades como la salud, el agua potable, las aguas residuales, o el espacio, además incluye a las administraciones públicas.
3. Los estados miembros deberán contar con una estrategia nacional para aumentar la resiliencia de las infraestructuras críticas, también deberán realizar una evaluación de riesgos al menos cada cuatro años.
4. Los estados podrán determinar cuáles son las entidades críticas que prestan servicios esenciales.
5. Las infraestructuras criticas deberán de ahora en adelante identificar los riesgos pertinentes a sus servicios y que puedan perturbar significativamente la prestación de los mismos, con el fin de tomar las medidas necesarias que garanticen su resiliencia y la posibilidad de notificar los incidentes a las autoridades del estado.
6. Se establecen normas para que se puedan establecer e identificar entidades críticas de importancia europea (aquellas que prestan un servicio esencial a seis o más Estados Miembros)

Tabla 3. Aspectos relevantes del Reglamento sobre la resiliencia operativa digital

ASPECTOS RELEVANTES DEL REGLAMENTO DORA
1. Ofrece requisitos uniformes para la seguridad de las redes y sistemas de información de las entidades u organizaciones que operen dentro del sector financiero, así como de terceros esenciales que les presenten servicios con tecnologías de la información y comunicación, servicios de nube o servicios de análisis de datos.
2. El principal objetivo es prevenir y mitigar las ciberamenazas que afectan al sector, el marco normativo está dirigido a la resiliencia operativa digital.
3. Los proveedores esenciales de servicios TIC de terceros países que presten sus servicios a entidades del sector financiero de la UE, serán obligados a establecer una filial dentro de la UE, con el fin de ejercer supervisión sobre ellos.

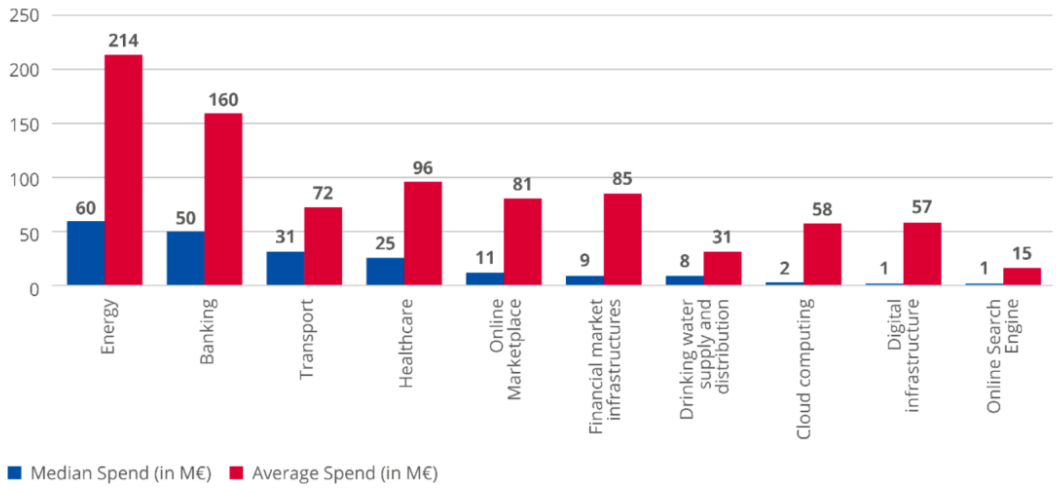
4. El presente reglamento se basa en la Directiva NIS2 y aborda los vacíos que esta pueda dejar al sector en específico.

Table 1: Categories of OES/DSP as defined in the NIS Directive

Categories of OES and DSPs	
OES	**DSPs**
• Energy (electricity, oil and gas) • Transport (air, rail, water and road) • Banking • Financial market infrastructures • Health • Drinking water supply and distribution • Digital infrastructure	• Online marketplace • Online search engine • Cloud computing service

European Union Agency For Cybersecurity. (2021). *NIS Investments*. Págs. 1-86. https://www.enisa.europa.eu.

Figure 16: IT spending by sector



n=930
[17 organisations responded with – "I have no visibility on the budget"]

European Union Agency For Cybersecurity. (2021). *NIS Investments*. Págs. 1-86. https://www.enisa.europa.eu.

Imagen 4: catálogo de servicios de consultoría.

6. CONCLUSIONES

El objetivo propuesto en este escrito, además de mostrar como las Infraestructuras Críticas harán parte activa en las ciudades inteligentes y como de hecho ya lo están haciendo, contribuyendo a la sostenibilidad, conectividad, y mejoramiento de la calidad de vida de los habitantes, a través de herramientas tecnológicas que no solo facilitan la vida sino que acercan a los usuarios a los servicios más esenciales; también se centró en analizar la viabilidad que las normas y regulaciones en materia de seguridad de entidades críticas podrían tener dentro de las urbes del futuro. Aplicando por ende las directivas NIS y catalogando a las ciudades inteligentes como una entidad de Infraestructura Critica.

Luego del estudio normativo, académico y literario que se realizó, es posible concluir que las futuras amenazas en ciberseguridad en las entidades críticas están directamente relacionadas con la inclusión de las mismas dentro de las ciudades del futuro, como también con la implementación de las nuevas tecnologías a raíz del salto a la era digital que muchas de ellas tuvieron dar.

Si bien es complejo vaticinar cuáles serán las nuevas amenazas cibernéticas a las que se verán enfrentadas este dipo de empresas esenciales, si es posible pronosticar que el aumento de los ataques y riesgos aumentara de manera

exponencial, el uso de las tecnologías y el vuelco total hacia ellas, generara en las organizaciones delictivas cibernéticas, blancos fijos para atacar. Los ciberataques por el momento serán los mismos, no obstante, la frecuencia y los puntos arremetidos serán constantes.

Además de acoplarse al nuevo método de ofrecer servicios, las entidades críticas deberán cooperar dentro de las ciudades inteligentes para hacer de las mismos entornos seguros, las exigencias que nacen entonces serán la de proteger los datos de sus usuarios (servicios cloud), las redes de comunicación que son la base del servicio (big data y 5G), y los elementos físicos que recopilan datos y junto con el entorno hacen de las urbes, espacios conectados y funcionales. La directiva NIS2 como actualización de la NIS, propende por la autonomía de los gobiernos en identificar y catalogar las entidades que consideren necesarias para el correcto funcionamiento de los mismos estados. Además de ello en imponer obligaciones de seguridad a las empresas que provean tecnología, comunicaciones o cualquier tipo de servicio de información, ello con la intención de cerrar brechas y zonas grises desde la base de los servicios.

A pesar de que las ciudades inteligentes no se encuentran dentro de la directiva NIS2, las entidades de tecnologías de la información que las componen si, siendo todas ellas Infraestructuras Críticas, debido al gran impacto que generaría un daño. Que no sean tenidas en cuenta no quiere decir que estén rezagadas, la UE y ENISA como grupo especializado en ciberseguridad, han desarrollado a lo largo de estos años planes significativos hacia la transformación de las ciudades inteligentes. Horizonte Europa, Europa Digital, Europa financiera Digital, y los informes que en materias específicas se han realizado para las entidades criticas como la energía, el transporte, las comunicaciones, las entidades públicas; son una muestra de que la Unión Europea entiende la importancia de este camino y la llegada en un futuro de las ciudades inteligentes, lo que para ese momento tendrá que ser regulado y debatida una directiva en pro de estos nuevos espacios que integran todo lo que hoy conocemos como empresas esenciales.

Las certificaciones, el cumplimiento de las regulaciones europeas junto con las estatales y las buenas prácticas son la mejor manera de contrarrestar estas futuras exigencias que vienen en seguridad. Gracias a las nuevas tecnologías los activos de las empresas son cada vez mayores y por ende la realización constante de análisis e identificación de riesgos se hace innegable, la educación y formación del personal dedicado a la seguridad es un pilar fundamental para cada entidad, y la concientización del propio ciudadano que dentro de las ciudades inteligentes se convierte en un blanco igual de importante, cada sensor, cada contador, cada móvil, cada elemento conectado a internet se convierte en una ventada de entrada para causar daños y depende de todos que estos sean mínimos o de magnitudes catastróficas.

Por último, la Directiva NIS2, centro de análisis de este escrito, empieza a labrar el camino hacia regulaciones de seguridad más específicas, entiendo el concepto de interdependencia, y reconociendo la importancia de la prevención y la resiliencia. Condiciones que deben tener las ciudades del futuro para responder de manera inmediata cualquier incidente sin que los daños sean significativos.

7. BIBLIOGRAFÍA

1. Huamán Farro, S.D. (4 de agosto, 2022), Análisis sobre ciberataques a infraestructuras críticas y sus consecuencias. *Policía H50*. https://www.h50.es/analisis-sobre-ciberataques-a-infraestructuras-criticas-y-sus-consecuencias/.
2. Council of the European Union. (2020). *Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027*. https://data.consilium.europa.eu/doc/document/ST-13835-2020-INIT/en/pdf.
3. European Commission. (2021). *Horizon Europe*. [presentación] https://research-and-innovation.ec.europa.eu/system/files/2022-06/ec_rtd_he-investing-to-shape-our-future_0.pdf
4. Centro de Ciberseguridad Industrial – CCI. (2020). *Smart Grids Before the Security Challenge*. Serie Smart OT, Número 1. Págs. 20.
5. European Union Agency For Cibersecurity. (2015). *Good Practices and Recommendations on the Security of Big Data Systems*. https://www.enisa.europa.eu
6. ENISA y Los Estados Miembros de la Unión Europea. (2020). *Report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity - Informe sobre los Procesos Registrados*. https://digital-

strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity

7. European Union Agency For Cibersecurity. (2019). *Threat Landscape For 5G Networks*. Págs. 1-54. https://www.enisa.europa.eu.
8. Cybersecurity & Infrastructure Security Agency. (2022). *Cross-Sector Cybersecurity Performance Goals And Objectives*. https://www.cisa.gov/cpgs.
9. ÚSEC BILBAO CONGRESS 22, (26 de mayo, 2022) "*la protección de infraestructuras críticas y estratégicas. Optimizar su seguridad contra agresiones deliberadas, especialmente, contra ataques terroristas*". https://congress.usecim.es/mesa-redonda-la-proteccion-de-infraestructuras-criticas-usec-bilbao-congress-2022/
10. European Union Agency For Cybersecurity. (2021). *NIS Investments*. Págs. 1-86. https://www.enisa.europa.eu.
11. European Union Agency For Cybersecurity. (2021). *Cloud Security For Healthcare Services*. Págs. 1-46. https://www.enisa.europa.eu.
12. European Union Agency For Cybersecurity. (2021). *Industry 4.0 Cybersecurity: Challenges & Recommendations*. Págs. 1-13. https://www.enisa.europa.eu.
13. European Commission. (2020). *The impact of the EU's changing electricity market design on the development of smart and sustainable cities and energy communities.* Págs. 1-43. https://www.enisa.europa.eu.
14. *Villarejo Galende, H. (2015).* Smart Cities: Una Apuesta De La Unión Europea Para Mejorar Los Servicios Públicos Urbanos. *Revista de Estudios Europeos*. (No. 66). 25-51. http://www.ree-uva.es/
15. Agencia Estatal Boletín Oficial del Estado (BOE). (2022). *Ámbitos de la Seguridad Nacional: Protección de Infraestructuras Críticas.* www.boe.es/biblioteca_juridica/
16. MARTÍN IBÁÑEZ, E. (2017). El valor de construir ciudades inteligentes con ciberseguridad. *Revista de Pensamiento, Sociedad y Tecnología. (105). 1-16.* https://telos.fundaciontelefonica.com

17. Comisión Nacional del Mercado de Valores. (2017). *Ciberseguridad en las infraestructuras de los mercados*. www.cnmv.es.
18. Santos, Leopoldo. 2021. "Ciberseguridad e infraestructuras críticas" en: UEM STEAM Essentials
19. IOActive, Inc. (2015). *An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks.* www.ioactive.com
20. Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
21. 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»)
22. 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.
23. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
24. 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
25. https://cnpic.interior.gob.es
26. https://www.ccn-cert.cni.es
27. https://www.enisa.europa.eu
28. https://www.consilium.europa.eu
29. https://congress.usecim.es
30. https://www.europarl.europa.eu
31. https://www.smartcitiescouncil.com/resources
32. https://www.cci-es.org