universidad de león

FACULTAD DE DERECHO
UNIVERSIDAD DE LEÓN
CURSO 2021/2022

TRABAJO DE FIN DE MÁSTER

DERECHO DE LA CIBERSEGURIDAD Y ENTORNO DIGITAL

INFRAESTRUCTURAS CRÍTICAS: ANÁLISIS DE LA LEGISLACIÓN VIGENTE EN ESPAÑA Y GUATEMALA

CRITICAL INFRASTRUCTURES: ANALYSIS OF CURRENT LEGISLATION IN SPAIN AND GUATEMALA

AUTOR/A: D. ING. MARCOS JOAQUÍN DE LA CRUZ HERNÁNDEZ

TUTOR/A: D. DRA. MERCEDES FUERTES LÓPEZ

Dedicatoria

Este trabajo inicia con la idea de poder realizar un aporte hacia mi país, en base a lo aprendido a lo largo del Máster. Por lo que principalmente se lo dedico a Dios por haber preparado el camino para que cada puerta se abriera, y cada acción se desarrollara sin problema. Seguidamente y sin duda alguna se lo dedico a mi familia, en especial a mi padre y a mi madre, que a pesar de que se encuentren lejos, desde el otro lado del mundo siempre han sabido como darme ánimo y apoyarme de una manera incondicional para que siempre siga adelante ante cualquier situación, por lo que este logro no es solo mío sino de ellos, también se lo dedico a mis hermanos por todo el apoyo dado, y a los amigos que siempre estuvieron ahí.

Agradecimientos

Principalmente debo agradecer a Fundación Carolina, al Instituto Nacional de Ciberseguridad y a la Universidad de León, por darme la oportunidad de venir aprender ciberseguridad desde el punto de vista del derecho, complementando así mi formación profesional al tener otra perspectiva con esta gran experiencia.

De una forma muy especial, agradezco los consejos, asesorías, ayudas y enseñanzas brindadas por mi tutora: Dra. Mercedes Fuertes López; por todo el contenido brindado en sus cursos, junto a todo el apoyo que me dio a la hora de conseguir materiales de estudio que no se encontraban en la biblioteca, así como también de la misma forma por todo el consejo dado en pro de mi formación a lo largo del máster y desarrollo de este trabajo.

Agradezco especialmente a los profesores y coordinadores del máster: Dra. Isabel Durán Seco, Dr. Salvador Tarodo Soria por los cursos que impartieron a lo largo del máster y por brindar ayuda y consejo.

Agradezco a los colegas profesionales del sitio de prácticas, porque en su momento creyeron en mí y me dieron la oportunidad de crecer profesionalmente.

Agradezco a todos los docentes del máster por compartir todo su conocimiento de una forma única, generosa y profesional, así como también por brindarme la disponibilidad de ayudarme ante cualquier situación

A mis amigos y compañeros del máster.

Índice

Índice de tablas

Índice de Ilustraciones

RESUMEN

El presente trabajo consiste en el análisis de la Legislación vigente en España, referente al tema de la Infraestructura Crítica, donde la finalidad se centra en conocer las bases fundamentales de cómo se desarrolló la ley 8/2011. De la mano a ello se analiza el escenario actual de la normativa que tiene Guatemala referente al tema. Por lo que de esta forma el trabajo se estructura por tres capítulos donde:

- En el primer capítulo se realiza una definición sobre que es una infraestructura crítica, y porque es importante la ciberseguridad dentro de ella; seguidamente se conoce una parte de la información de la Infraestructura Crítica en España y Guatemala, junto a la legislación vigente de Infraestructura Crítica y Ciberseguridad de los dos países. también se analizan los estándares internacionales de normalización (ISO) como posibles herramientas de apoyo.
- El segundo capítulo se enfoca en los riesgos que las Infraestructuras Críticas llegan a tener frente a los ataques dirigidos.
- El tercer capítulo se divide en tres partes que parten desde el análisis de la Ley PIC en España, las políticas de protección, y el análisis de escenario de Guatemala como los aspectos clave a contemplar para un desarrollo de normativa o política.

PALABRAS CLAVES

Infraestructura Crítica, Ciberseguridad, Ciberataques, Operadores Críticos, Operadores de Servicios Esenciales, Prestadores de Servicios Digitales, Vulnerabilidades, Riesgos, Sistemas de Información, Leyes Vigentes, Soft Law, Estrategia de Seguridad, España, Guatemala.

Abstract

The present work consists of the analysis of the Legislation in force in Spain, referring to the subject of Critical Infrastructure, where the purpose is focused on knowing the fundamental bases of how Law 8/2011 was developed. Hand in hand with this, the current scenario of the regulations that Guatemala has regarding the subject is analyzed. So in this way the work is structured by three chapters where:

- In the first chapter, a definition is made of what is a critical infrastructure, and why cybersecurity is important within it; Next, part of the information on the Critical Infrastructure in Spain and Guatemala is known, together with the current legislation on Critical Infrastructure and Cybersecurity of the two countries. International standards for normalization (ISO) are also analyzed as possible support tools.
- The second chapter focuses on the risks that Critical Infrastructures have in the face of targeted attacks.
- The third chapter is divided into three parts that start from the analysis of the PIC Law in Spain, the protection policies, and the analysis of the Guatemalan scenario as the key aspects to consider for the development of regulations or policies.

Key Words

Critical Infrastructure, Cybersecurity, Cyberattacks, Critical Operators, Essential Services Operators, Digital Service Providers, Vulnerabilities, Risks, Information Systems, Current Laws, Soft Law, Security Strategy, Spain, Guatemala.

ABREVIATURAS Y ACRÓNIMOS

CCN	Centro Criptológico Nacional
CERT	Equipo de Respuesta a Emergencias Informáticas
CNPIC	Centro Nacional para la Protección de Infraestructuras y Ciberseguridad
CNS	Consejo Nacional de Seguridad
CONCIBER	Comité Nacional de Seguridad Cibernética
CONRED	Coordinadora Nacional para la Reducción de Desastres
CSIRT-GT	Equipo de Respuesta a Incidentes de Seguridad Informática-Guatemala
CSIRT	Equipo de Respuesta a Incidentes de Seguridad Informática
ENISA	Agencia de la Unión Europea para la Ciberseguridad
GTCERT	Equipo de Respuesta a Emergencias Cibernéticas de Guatemala
IC	Infraestructuras Criticas
ICE	Infraestructuras Criticas Europeas
ICN	Infraestructura Crítica Nacional
INCIBE	Instituto Nacional de Ciberseguridad
ISO	Organización Internacional de Información
NIS	Seguridad de Redes de Información
OEA	Organización de Estados Americanos
OCC	Oficina de Coordinación Cibernética
OGDI	Observatorio Guatemalteco de Delitos Informáticos
PEPIC	Programa Europeo de Protección de Infraestructuras Críticas
RSC	Responsabilidad Social Corporativa
SCI	Sistemas de Control Industrial
SIE	Secretaría de Inteligencia Estratégica del Estado
STCNS	Secretaría Técnica del Consejo Nacional de Seguridad
TIC	Tecnologías de Información y Comunicación
TI	Tecnologías de la Información
TO	Tecnologías de Operación
UE	Unión Europea

OBJETO Y OBJETIVO DEL TRABAJO

El objetivo principal del presente trabajo será realizar un análisis de la legislación actual en España con relación a la protección de infraestructura crítica, teniendo como propósito conocer los fundamentos bases y motivos de surgimiento; de la mano a ello se analizará la influencia de desarrollo tecnológico que está teniendo Guatemala, junto a sus bases legales, para así de esta forma abordar los aspectos clave que se deben considerar a la hora de aplicar un marco normativo, en el área de las infraestructuras críticas y ciberseguridad en Guatemala.

Objetivos específicos:

1. Estudiar el concepto de infraestructuras críticas y describir los aspectos, áreas y alcances que se tienen en España y Guatemala.
2. Definir la importancia de la ciberseguridad dentro de las infraestructuras críticas Nacionales junto a los riesgos y vulnerabilidades que estas puedan llegar a presentar frente a los ciberataques.
3. Investigar los estándares internacionales de normalización que pueden llegar a ser considerados como una herramienta de apoyo en el área de la seguridad y gestión de riesgos.
4. Analizar la ley vigente 08/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas en España, con el fin de conocer sus bases fundamentales.
5. Estudiar el escenario actual de Guatemala con relación a la estrategia de seguridad vigente, con el propósito de conocer cómo es que se encuentra referente al tema de las Infraestructuras Críticas.

METODOLOGIA

Tomando como base el objetivo principal y con el propósito de realizar un trabajo correcto y ordenado, la consecución del análisis se desarrollará por medio de la técnica de revisión bibliográfica, perteneciente a la metodología cualitativa, la cual conforma un conjunto de prácticas que según Laura Velamazán[1] permiten obtener datos más detallados, gracias a que no se requiere de un plan de diseño tan estricto, por lo que de

[1] Velamanzán, Laura. 2021. QuestionPro. *Entre datos ¿Que es la Investigación Cualitativa?* [En línea] 2021. [Consulta: 24 de Marzo de 2022.] Disponible en: https://www.questionpro.com/es/investigacion-cualitativa.html#:~:text=La%20investigaci%C3%B3n%20cualitativa%20tiene%20como,de%20investigaci%C3%B3n%20flexible%20e%20interactiva..

esta forma el estudio se podrá llevar de manera más natural, consiguiendo así que la revisión bibliográfica se centre en el contexto principal, el cual será estudiar la legislación vigente por la que se establecen medidas para la protección de las infraestructuras críticas en España, conjuntamente se conocerá el contexto de cómo se encuentra Guatemala, para el establecimiento de su marco normativo en esta área.

De modo que para entrar en detalle la metodología se estructurará de la siguiente forma[2]:

Tabla 1: Matriz de fases de la metodología

Fases	Descripción
Formulación	Sin duda alguna esta es una de las fases más importantes dentro de la metodología, debido a que es donde se precisa cual será el enfoque del estudio, ya que se caracteriza por explicar que es lo que se va a analizar y porqué[3]. Partiendo de esta premisa se puede decir que parte de la formulación se inició justo en el momento en el que se establecieron los objetivos, constituyendo así una guía indicativa provisional para cuando se empiece a recabar y analizar el material de estudio. De esta forma se logra dividir el estudio en tres capítulos donde: 1. En el primer capítulo se realizará una definición sobre que es infraestructura crítica y porque es importante la ciberseguridad dentro de ella; en ese mismo capítulo se conocerá parte del escenario de España y Guatemala en esta área, junto a la legislación vigente en materia de protección de infraestructura crítica y ciberseguridad que puedan tener, así como también estándares internacionales que pueden llegar a ser una herramienta de apoyo. 2. El segundo capítulo se enfocará en los riesgos que las infraestructuras críticas pueden llegar a tener frente a los ataques dirigidos a sus sistemas de información.

[2] Fuente: Elaboración propia.
[3] Universidad de Cantabria. 2015. Grupo UNICAN. *Fases de una investigación.* [En línea] 04 de abril de 2015. [Consulta: 24 de marzo de 2022.] Recurso disponible en el siguiente enlace web: https://grupos.unican.es/mide/masterinnova/materiales/Fases%20investigacion.pdf.

	3. El tercer capítulo se dividirá en tres partes que partirá desde el análisis de la Ley PIC en España, las políticas de protección, y el análisis de escenario de Guatemala en esta área como los aspectos clave a contemplar.
Recolección de datos de estudio	En todo estudio bibliográfico esta es una de las fases más laboriosas, debido a que en esta parte es donde se recolecta toda la información necesaria para realizar la revisión bibliográfica. Para la investigación la información se obtendrá en base a libros de investigación, informes y reportes emitidos por las entidades encargadas de gestionar y velar por la protección de las infraestructuras críticas. Para ello se recurrirá a recolectar los datos por medio de los canales oficiales donde se comparte dicha información. Para el caso de la información de Guatemala la información se obtendrá por medio de la Secretaría Técnica del Consejo Nacional de Seguridad de Guatemala, (en adelante –STCNS–), y de parte del Observatorio Guatemalteco de Delitos Informáticos (en adelante –OGDI–).
Análisis	Una vez culminada la fase de recolección de datos, se iniciará la revisión bibliográfica donde en base a lo establecido en la fase de formulación, y siguiendo la guía de capítulo se procederá a ir revisando y documentando cada hallazgo importante.
Interpretación	Para este punto dentro de la metodología se puede decir que la mayoría del trabajo ya estará culminado, por lo cual la interpretación, corresponderá precisamente a la última parte del capítulo tres donde luego de haber analizado la Ley PIC y estudiado el escenario de Guatemala, en esta parte se procederá a formular las conclusiones en base a los aspectos destacados del escenario de Guatemala.

Una vez establecida la metodología a seguir, se puede proceder ya en orden al estudio.

INTRODUCCIÓN

La pasada crisis provocada por la pandemia en el año 2020 demostró la dependencia que, como sociedad se ha desarrollado hacia una infraestructura tecnológica que día a día, se encuentra más conectada que nunca, de ese modo la infraestructura global de servicios ahora opera, en mayor medida, bajo el uso de las tecnologías digitales en distintos sectores fundamentales, como la educación, salud, comercio, seguridad, servicios básicos y servicios públicos entre otros, por lo que el impacto de su uso constituye al internet como una pieza importante, para el desarrollo integral de las personas en su vida diaria y las naciones por la comunicación, intercambio de información y optimización de sistemas.

Si bien esto se puede considerar algo bueno, hay que tener en cuenta que la tendencia de un mundo cada vez más interconectado, trae consigo una serie de riesgos y amenazas tales como los ciberdelincuentes o peor aún ciberterroristas, de los cuales los ciberterroristas son los que mas llegan a poner en apuros a los gobiernos, por los distintos ataques a las infraestructuras críticas que realizan. Desde este punto y a sabiendas de que se está ante un nuevo estilo de terrorismo que busca poner en jaque desde la distancia con unos cuantos clics a un país entero, resulta más que necesario que los gobiernos aborden una gobernanza con seriedad, enfocada a la seguridad de los sistemas de las infraestructuras críticas y generen conciencia como aspecto esencial, para garantizar así la propia seguridad de los ciudadanos y del propio gobierno.

Por lo que, para esto, las políticas, los instrumentos estratégicos, la coordinación intersectorial y los marcos normativos se vuelven un tema del cual pocos países llegan a hablar, pero la realidad es, de que la seguridad física, así como la del ciberespacio se debe de garantizar y brindar.

Razón por la cual, en este trabajo se hace un análisis de la Ley de Protección de las Infraestructuras Críticas de España, para conocer la base de como fue que se encaminó el desarrollo de esta ley vigente para así, de la mano a ello luego de analizar y conocer el escenario actual de Guatemala poder establecer aspectos que pudieran encajar en la normativa Guatemalteca.

CAPÍTULO I - INFRAESTRUCTURAS CRITICAS

Las Infraestructuras Críticas de la mayoría de los países siempre estarán expuestas a una cantidad de riesgos y amenazas latentes que se deben de evaluar; para lo cual es necesario tener planes estratégicos y normas que permitan generar una protección más avanzada. Por ello, es importante, antes que nada, conocer el concepto de que es una Infraestructura Crítica junto a sus aspectos e importancia.

1.1 ASPECTOS DE LAS INFRAESTRUCTURAS CRÍTICAS

1.1.1 CONCEPTO

Para poder entender el concepto de Infraestructura Crítica, es necesario conocer la base de donde parte, la cual es infraestructura. Y ¿Qué es una infraestructura? Una infraestructura (normal) viene a ser un compendio de servicios, tales como los medios técnicos que permiten realizar una actividad en específico. Que en los usos más frecuentes las infraestructuras conforman un conjunto de obras públicas, instalaciones, redes y sistemas que soportan el funcionamiento óptimo de ciudades y países.

Teniendo este conocimiento de infraestructura como base, se puede ir formulando el concepto sobre que es una infraestructura crítica, que por otro lado y teniendo en cuenta lo que menciona Fernando Sevillano en su libro Ciberseguridad Industrial[4], las infraestructuras críticas son aquellas instalaciones o servicios cuyo funcionamiento o destrucción, repercutiría en un grave impacto sobre los servicios esenciales que ellas proporcionan para la sociedad o el funcionamiento de la misma. Por esa razón se llegan a convertir en áreas críticas que se deben evaluar y tener en cuenta el impacto que representan.

En la actualidad el concepto de infraestructura crítica, así como la acción público-privada que deriva de esa parte, juega un papel importante en el espacio de las políticas públicas de seguridad, máxime si se toman como marco de una perspectiva integradora. En España la transposición de la Directiva 2008/114/CE destina las definiciones de infraestructuras estratégicas, infraestructuras críticas e infraestructuras crítica europeas, en el artículo 2

[4] Sevillano, Fernando . 2021. *Ciberseguridad Industrial e Infraestructuras Críticas.* España : RA-MA, 2021. ISBN: 978-84-1855-136-9. << Este libro logra transmitir una visión completa de las características y alcances de la ciberseguridad cuando se desea proteger activos industriales, lectura muy recomendada >>

del Título I de la Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Que a efectos de la ley se entienden como:[5]

- Infraestructura crítica:
    - Son aquellas <<infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales>> (art. 2 Ley 8/2011).

- Infraestructuras críticas europeas:
    - Son aquellas <<infraestructuras críticas situadas en algún Estado miembro de la Unión Europea, cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros >>, de acuerdo con la Directiva 2008/114/CE del Consejo, de 8 de diciembre, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección (art. 2 Ley 8/2011).

- Infraestructura estratégica
    - Son aquellas <<instalaciones, redes, sistemas equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales>> (art. 2 Ley 8/2011).

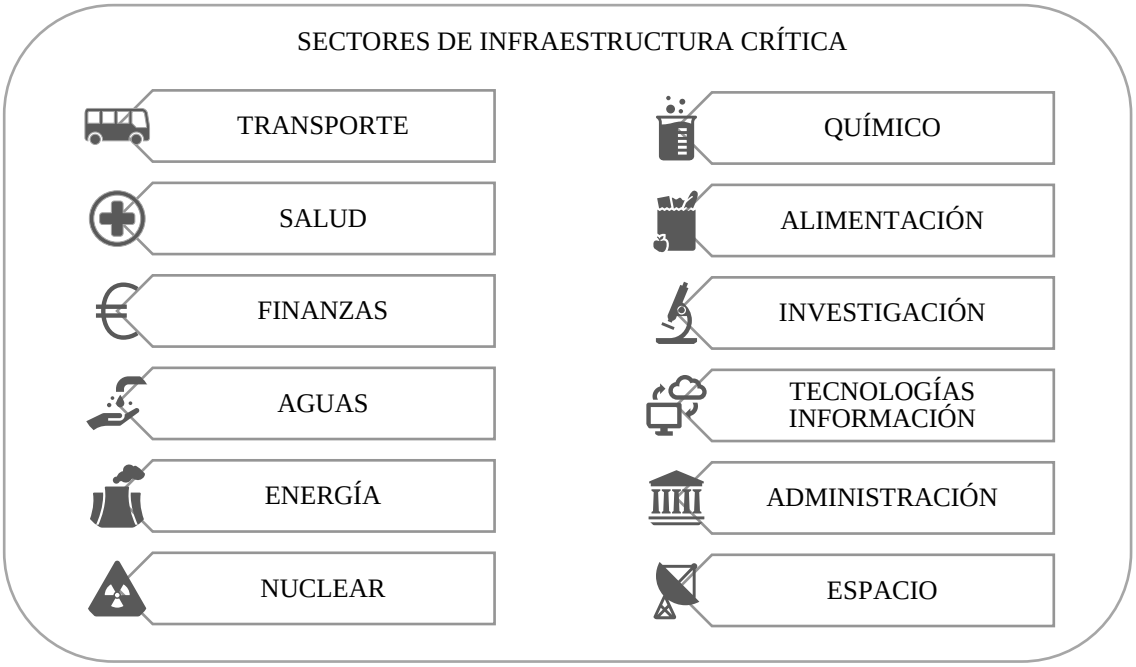
La gran mayoría de países suele considerar y catalogar como críticas las infraestructuras que brindan energía, combustible y agua; los sistemas de transporte y comunicaciones; las estructuras para el suministro de alimentos y la gestión de residuos; las infraestructuras económicas y financieras; las redes de telecomunicaciones tales como internet, telefonía y comunicaciones satelitales; los sistemas relacionados con la defensa y la seguridad nacional; los sistemas de emergencia, rescate y protección ciudadana; el sistema sanitario, sistema de justicia y en general las agencias y administraciones públicas. A la vista el concepto de infraestructura crítica puede llegar a ser un poco extenso, pero la verdad, es bueno conocer cómo es que se compone.

[5] *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas*. [En línea] 29 de abril de 2011. https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf.

1.1.2 Importancia de las Infraestructuras Críticas

Con el concepto del punto anterior encaminado, el tema de la importancia de estas infraestructuras críticas surge, y es que ¿Qué tan importante son? La pregunta, bien se puede responder por si sola, pero si se analizan los aspectos y rasgos esenciales asociados, se puede resumir todo a la prestación de servicios esenciales. Debido a que, para el mantenimiento de las funciones sociales básicas en la seguridad, la salud, el bienestar social y económico; las infraestructuras críticas se vuelven un punto de unión para el funcionamiento de los distintos sectores, tales como los que resalta Fernando Sevillano en el capítulo I de activos específicos de su libro Ciberseguridad Industrial e Infraestructuras Críticas[6]:

Ilustración 1: Sectores de Infraestructura Crítica



Como se puede observar, la dependencia que hoy en día las sociedades y los Estados tienen hacia este tipo de infraestructuras, resalta por sí sola la importancia de que los distintos servicios esenciales no se vean interrumpidos por desastres naturales, ataques terroristas o a lo que nos atañe en este caso donde la Industria 4.0 se ha consolidado, ataques informáticos que repercutan en un mayor daño; por lo que la protección de estas

[6] Sevillano, Fernando . 2021. *Ciberseguridad Industrial e Infraestructuras Críticas.* España : RA-MA, 2021. ISBN: 978-84-1855-136-9. << El capítulo I, apartado 1.5 de activos específicos, da una clara interpretación de los sectores fundamentales para las IC, el cual proyecte la dependencia de las sociedades hacia estas infraestructuras >>

por medio de normas legislativas, protocolos, procesos, y estándares internacionales; llegan a adquirir un mayor sentido de importancia.

En ese contexto y haciendo hincapié en la Industria 4.0, la base de esta industria está en la tecnología, conectividad de activos industriales y recolección de datos; donde en su totalidad toda infraestructura crítica llega a utilizar la tecnología para una mejor optimización de procesos. Esto si bien brinda una serie de ventajas también genera una serie de desventajas como las amenazas cibernéticas.

Haciendo énfasis en el punto anterior, la importancia de las infraestructuras críticas para la sociedad y para los Estados es más que notoria, esto no solo por la infinidad de servicios esenciales que se brinda hacia las personas sino también por el funcionamiento, defensa y operabilidad de un Estado. Por lo que esto llega a suponer una necesidad real a que se generen medidas adecuadas para la protección de las mismas.

1.1.3 Importancia de la ciberseguridad en las Infraestructuras Críticas

La ciberseguridad dentro de las infraestructuras críticas es crucial, sabemos que la ciberseguridad no tiene un área o sector en específico, constituye una necesidad en una infinidad de campos. En este estudio enfocaré la atención en la industria y en las infraestructuras críticas.

Se ha mencionado en reiteradas ocasiones que las infraestructuras críticas garantizan el óptimo desempeño de los servicios prestados por el Estado y por las empresas privadas y semi privadas; por lo que en ese sentido y con lo que se ha mencionado a lo largo del trabajo sobre lo que representa la integración de la Industria 4.0, la ciberseguridad es una necesidad y debe ser vista como un requisito en cualquier proyecto, empresa, industria e infraestructura, ya sea crítica o no crítica. La principal finalidad de la ciberseguridad será siempre el de robustecer los sistemas de seguridad de las organizaciones, con el simple objetivo de garantizar que los servicios siempre se encuentren disponibles, que los datos esenciales no se vean alterados y que se mantengan seguros.

La mayoría de las veces suele ser difícil realizar dicha integración, pero en sí, la ciberseguridad debe de identificarse como un requisito de la puesta en operación, más que todo por una cultura de organización dentro de las estrategias y políticas internas de cada empresa, industria o infraestructura crítica; esto con el fin de desarrollar un conjunto

de medios y procedimientos que permitan reducir el riesgo a niveles aceptables, ya que la protección del 100% es algo que no se puede garantizar.

Lo importante es tratar de reducir los riesgos y amenazas, pero ¿cómo es posible realizar esto? Lo principal es conocer a la empresa, es esencial conocer con qué tipo de tecnología es con la que se está trabajando, porque en el sector Industrial suele existir dos tipos de conceptos que suelen catalogar y entenderse por separado tales como: las tecnologías de la información (en adelante – IT–) y las tecnologías de la operación (en adelante –OT–); por lo general estos conceptos suelen ser distintos porque a veces suelen operar por separado, ya que una parte se enfoca al área física y otra al área administrativa, pero eso no quita que puedan llegar a estar combinados entre sí. Por lo que, como bien se comentaba anteriormente, es bueno saber sus utilidades por separado para potenciar así sus funcionalidades.

Siguiendo el punto anterior las medidas y controles a implementar, tanto físicos como administrativos, buscan asegurar la confidencialidad e integridad de los datos y disponibilidad de los sistemas, pero teniendo en cuenta la diferencia entre la ciberseguridad IT y la ciberseguridad OT, se pueden observar sus aspectos en la tabla 2[7]:

Tabla 2: Aspectos de IT y OT – diferencias en ciberseguridad

IT	ASPECTOS	OT
Confidencialidad integridad y disponibilidad	Objetivo	Confidencialidad integridad y disponibilidad
2/3 años con gran número de proveedores	Ciclo de vida	10/20 años con reducido número de proveedores
Práctica habitual e inversión en ciberseguridad	Evaluación cuantitativa del riesgo	Práctica realizada si llega a ser obligatoria
Habitual y en la operación	Gestión de la seguridad	En lo común no es habitual
Fácil de actualizar con políticas automatizadas y bien definidas	Antivirus y parches	Sin políticas específicas y poco habitual
Normativas genéricas	Cumplimiento normativas	Normativas especificas
Estándares más actuales	Testeo y auditorías	Inexistencia de estándares
Fácil despliegue y en ocasiones carácter obligatorio	Respuesta a incidencias y análisis forense	Poco habitual, en la mayoría no se realiza análisis forense

[7] Logitek. 2014. Industrial Cybersecurity by Logitek. *Seguridad IT versus Ciberseguridad Industrial.* [En línea] 2014. [Consulta el: 2 de abril de 2022.] https://www.ciberseguridadlogitek.com/seguridad-it-versus-ciberseguridad-industrial/. <<En esta página web se desarrolla el tema de convergencia IT&OT >>

De la tabla anterior se puede destacar una serie de diferencias, tales como que en entornos IT la confidencialidad de la información es un aspecto que prima sobre la integridad de los datos y la disponibilidad del sistema; mientras que en OT la disponibilidad llega a ser uno de los aspectos más importantes que se deben proteger. Esto se entiende debido a que los entornos OT suelen ser más físicos, generando con ello que la confidencialidad en los entornos OT llegue a ser menos crítica.

Otra de las grandes diferencias entre entornos IT y OT que se llega a observar, es en el conocimiento tecnológico que poseen los responsables de su sector, por ejemplo, en el ámbito de la ciberseguridad, los responsables del área IT, suelen conocer más a fondo los riesgos que el uso de la informática suele presentar, por lo que están más informados en como poder mitigar dichos riesgos, pero en contra los responsables de los entornos OT llegan a ser más experimentados en los procesos de automatización, pero decaen en la parte de estar al tanto de los nuevos riesgos por el uso del entorno IT. Todo esto es lo que facilita a que se dé y exista una diferencia o distanciamiento entre ellos.

Teniendo en cuenta todo lo anterior, es esencial que exista una convergencia entre IT y OT con el objetivo de que así se puedan alinear las medidas de seguridad entre ambos entornos, para que así los riesgos y amenazas no se materialicen garantizando con ello que la ciberseguridad se consolide cada vez más en la organización industrial.

En este sentido las empresas pueden implementar un sinfín de salvaguardas técnicas, pero antes que nada, se debe realizar un análisis de toda la estructura de la empresa para así tener el conocimiento de las políticas que se deben generar, permitiendo de esta forma la posibilidad de que se pueda entender cómo es que se organizará la estructura en el apartado de ciberseguridad, consiguiendo de esta manera un panorama de las herramientas informáticas de seguridad necesarias para poder garantizar un funcionamiento ideal, óptimo y seguro; que permitirá hacer frente, a las posibles intromisiones que puedan poner en riesgo a las infraestructuras críticas tales como el cibercrimen, ciberespionaje, o ciberterrorismo.

1.1.4 Información de la Infraestructura Crítica en España

España es un gran referente de la ciberseguridad para el mundo. Con el pasar de los años se ha ido consolidando como una figura modelo que la mayoría de países buscan imitar, esto se debe a que, a lo largo de los años, el establecimiento de leyes, instituciones y puesta en marcha de proyectos ha ido generando que adquiera una posición sobresaliente

como uno de los 4 países con mayor interés hacia la ciberseguridad, todo esto en base al Índice Global de Ciberseguridad publicado por el Departamento de Seguridad Nacional (en adelante DSN)[8].

No hay duda alguna de que para España el tema de la seguridad y ciberseguridad es fundamental, y máxime en el apartado de las infraestructuras críticas, ya que procura que los servicios esenciales que se proveen a lo largo del país funcionen de una manera correcta, porque esto a lo largo del tiempo se traduce en desarrollo y bienestar para los ciudadanos y no se diga funcionamiento del país.

Como se ha podido ir observando la protección de las infraestructuras críticas, resulta esencial para mantenimiento de la vida diaria, por lo que de la misma forma y como ya se ha podido ver, estas llegan a estar expuestas a un sinfín de riesgos relacionados con amenazas naturales o a lo que nos atañe en este caso; terrorismo y ciberamenazas que bien podría ser la ciberdelincuencia así como también los riesgos asociados a la seguridad física y lógicas de las Tecnologías de la Información y Comunicación (en adelante TIC).

Teniendo en cuenta lo que significa una infraestructura crítica y viendo los posibles riesgos a los que llegan a estar expuestas dichas infraestructuras, España en el año 2005 se encamina en una serie de iniciativas en materia de seguridad, de las cuales se generó el plan de prevención y protección antiterrorista o como bien se le conoce el PPPA, en ese plan, España le encomienda la tarea a la Policía junto con la Guardia Civil, la elaboración de unos listados de aquellas infraestructuras que en sus ámbitos de actuación puedan ser susceptibles de ser atacadas por elementos terroristas, estos listados posteriormente se terminaron transformando en el Catálogo Nacional de las Infraestructuras Estratégicas, pero con la elaboración del plan, España empezó a percatase de cuán importante era este tema, máxime por esos terribles acontecimientos terroristas que se llegaron a dar en los primeros años del 2000, tanto como en Estados Unidos, Inglaterra e inclusive España.

En el año 2007 en España, el gobierno presenta el Plan Nacional de Protección de Infraestructuras Críticas (PNPIC) este plan fue aprobado por la secretaría de Estado de seguridad. En este plan aparecen dos puntos muy importantes, por un lado se crea el

[8] DSN, Sala de prensa del. 2021. Departamento de Seguridad Ncional. *España, a la Cabea mundial en Ciberseguridad.* [En línea] 01 de Julio de 2021. [Consulta: 04 de Abril de 2022.] https://www.dsn.gob.es/es/actualidad/sala-prensa/espa%C3%B1a-cabeza-mundial-ciberseguridad.

Catálogo Nacional de Infraestructuras Críticas Estratégicas, el cual se mencionó anteriormente y parte del PPPA por medio de esos listados, que en el año del 2005 se empezó a elaborar por medio de las fuerzas y grupos de seguridad del Estado; además de eso en ese mismo año en España se presenta el Nivel de Seguridad o Alerta Antiterrorista, que se encuentra en la página web del Ministerio de Interior[9], donde se establecen 5 niveles de alerta, del cual la activación es responsabilidad del Ministerio de Interior y la declaración por parte de la Secretaría de Estado de Seguridad.

Otra de las grandes iniciativas que realizó el Gobierno de España fue la aprobación por medio del consejo de ministros para la creación del Centro Nacional de Protección de Infraestructuras Críticas, o como bien se le conoce CNPIC, este centro es el que se responsabiliza auxiliando al Secretario de Estado de Seguridad (en adelante SES), como máximo responsable de la protección de Infraestructuras Críticas en todo lo relacionado a su protección.

Paralelo a ello, en Europa desde el año 2005 se había estado trabajando por medio de la Comisión Europea, la elaboración de un programa para la protección de las infraestructuras críticas europeas, a este programa se le conoce como el PEPIC: Programa Europeo de Protección de Infraestructuras Críticas, para ello la Comisión Europea elaboró el Libro Verde como hoja de ruta relacionada para proteger las infraestructuras críticas en todo el territorio europeo, junto a la red de alerta temprana CWIN; pero no fue hasta el año 2008 que la Unión Europea aprueba la Directiva 2008/114/UE; en esta Directiva se establecen las líneas básicas con relación a la protección de las infraestructuras críticas, cuya alteración pueda afectar a varios Estados miembros de la Unión Europea. Se trata de infraestructuras críticas europeas, de ahí que genere específicas obligaciones a los Estados miembros. Los Estados, al ver aprobada la directiva contaron con un plazo de dos años para que cada uno legislara en esta materia. A destacar de esta directiva es que se establece que existe una responsabilidad público-privada, generando así que la responsabilidad sea compartida tanto por el sector público como por el sector privado, este sin duda alguna llega a ser uno de los datos importantes para tener en cuenta.

[9] Seguridad, Secretaria de Estado de. 2017. Ministerio del Interior. *Dosier de Alerta Antiterrrorista.* [En línea] 06 de marzo de 2017. [Consulta: abril 2022.] https://www.interior.gob.es/opencms/pdf/prensa/nivel-de-alerta-antiterrorista/descargas/Dossier_NAA.pdf.

España, en base a todo ello en el año 2011 aprueba la Ley 8/2011, de Protección de Infraestructuras Críticas (en adelante Ley PIC); junto al Real Decreto 704/2011, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas, en esta ley España establece 12 sectores a proteger, en estos 12 sectores llegan a existir una serie de ministerios y organismos afectados que se les da responsabilidad sobre la protección de esas infraestructuras. En esta misma Ley, y tomando como base la directiva 2008/114, se organiza y se determinan los distintos actores públicos tanto como los privados, quienes llegarán a actuar en la gestión, implementación y cumplimiento de la Ley.

1.1.5 Información de la Infraestructura Crítica en Guatemala

Como se ha podido ir observando a lo largo de este trabajo, uno de los grandes retos a los que la mayoría de los gobiernos se enfrentan en el mundo, es el saber cómo lidiar o hacer frente a las distintas amenazas que han surgido durante el desarrollo de la tecnología, y es que no es de extrañarse, pero el mundo cada vez está más conectado y lo seguirá estando al paso que vamos. En este sentido, la mayoría de los gobiernos se enfrentan a la necesidad de formular iniciativas que fortalezcan los marcos jurídicos junto a sus ideales para la protección de sus Infraestructuras Criticas.

En el caso de la información de Guatemala, referente a este tema y en comparación con la información de España, esta llega a ser muy distinta; debido a que los intereses de parte de diferentes gobiernos que han estado en turno, nunca se han llegado a poner de acuerdo para dar seguimiento a las distintas iniciativas o proyectos de ley de gobiernos anteriores.

En Guatemala, algunas infraestructuras críticas llegan a ser propiedad del Estado, mientras que otras pertenecen al sector privado y no se cuenta con un listado claro de los tipos de infraestructuras críticas y sistemas de información nacionales como tal. Tampoco existe una ley o norma que obligue la incorporación o cumplimiento de buenas prácticas de seguridad, o protocolos técnicos adecuados.

A pesar de que Guatemala cuente con una Ley Marco del Sistema Nacional de Seguridad, la aplicación de esta llega a ser un desafío. La idea de creación de esta ley fue la de sentar las bases para que las instituciones públicas y privadas pudieran tener una coordinación, desarrollando con ello resiliencia, defensa civil, y lo que nos importa: protección de las infraestructuras críticas junto con la tecnología.

Esta Ley se crea en el año 2008 por medio del Decreto Numero 18-2008, en el Congreso de la República de Guatemala[10], con el objetivo de organizar al Estado Guatemalteco en la protección del Estado y del bien común, sus considerandos se centran en que es obligación del Estado fortalecer y garantizar la coordinación entre las instituciones competentes, en el ámbito de la seguridad, brindando así herramientas indispensables para el cumplimiento de las obligaciones que se dicten. Por medio de dicho Decreto, en el año 2008 se crea el Consejo Nacional de Seguridad (por sus siglas – CNS -) y el Sistema Nacional de Inteligencia (por sus siglas – SNI-), acá el Consejo de Seguridad tiene como finalidad Coordinar el Sistema Nacional de Seguridad, junto a la adecuación de políticas, planteamiento de estrategias, y lo más importante, asesorar al presidente de la República en la toma de decisiones en materia de seguridad.

Por otra parte, el Sistema Nacional de Inteligencia tiene como fin establecer procedimientos y normas que aborden con carácter preventivo las amenazas y riesgos de seguridad de la Nación, a este sistema se le constituyen una serie de competencias y procedimientos asignados por medio de ley, la cual es exclusiva para las instituciones públicas por lo que de esta manera el SNI realiza la tarea de coordinar las funciones de inteligencia estratégica por medio de su Secretaría en el ámbito, civil y militar. En esa línea el ámbito de gestión de riesgos y defensa civil se le es atribuido a la Coordinación Nacional para la Reducción de Desastres (por sus siglas CONRED), la cual constituye con capacidad del Estado el desarrollo e implementación de políticas de prevención, preparación, mitigación, respuesta y recuperación ante eventos de orden natural social y tecnológico. Al paso de los años CONRED, ha desarrollado distintos planes de recuperación para desastres naturales junto a ejercicios para la gestión de crisis, pero lastimosamente dentro de estos planes no se realizan ejercicios específicos para la coordinación, gestión de incidentes y ciberataques contra la infraestructura crítica nacional a pesar de que la Ley Marco lo establece.

Por último, para mencionar en este apartado de información de Infraestructura Crítica de Guatemala, cabe resaltar que se encontró que la Estrategia Nacional de Seguridad Cibernética del 2018, en su página 15 destaca que: *"El Reporte de incidentes cibernéticos*

[10] *Ley Marco del Sistema Nacional de Seguridad.* [En línea] 2008. [consulta el: 5 de Abril de 2022.] https://mingob.gob.gt/wp-content/uploads/2020/10/8.2-LEY-MARCO-DEL-SISTEMA-NACIONAL-DE-SEGURIDAD.pdf.

críticos actualmente no es obligatorio para los operadores de las infraestructuras críticas nacionales".[11]

Viendo el apartado anterior, y a modo de comentario como guatemalteco preocupado por esta área, lo único que se puede decir es que, es necesario e importante reglamentar esta práctica ya que, con una carencia de normas y políticas, los informes voluntarios de incidentes cibernéticos dentro de estas industrias serán cada vez más difíciles de implementar sin una Ley más clara o un reglamento más preciso.

1.2 ESTANDARES INTERNACIONALES – ISO – SOFT LAW

La Organización Internacional de Normalización (en adelante normas ISO) facilita un conjunto de normas orientadas a ordenar la gestión de una empresa, industria u organización; en sus distintos ámbitos. Están para poder funcionar como una herramienta y guía, que permite ayudar a las empresas en diferentes temas, la mayoría de ellas son de carácter genérico que se pueden utilizar en la mayoría de las industrias o empresas sin problemas, y otras que tienen un enfoque más específico, que va a depender del proceso y de la finalidad. Estas normas son establecidas por el Organismo Internacional de Estandarización.

Este apartado se centrará precisamente a conocer de forma general los estándares que promueven una mejor gestión de ciberseguridad y defensa cibernética; ya que presentan directrices sobre cómo administrar y como conectar la seguridad y la defensa de los sistemas en las distintas industrias, por lo que es bueno saber de ellas a la hora de que sea necesario evaluarlas como posibles normas o reglamento. A pesar de que en su mayoría son normas no vigentes podrían inspirar una incorporación o influir en el desarrollo de alguna ley.

Las siguientes normas presentan una descripción de sus utilidades en este mundo cibernético.

[11] *Estrategia Nacional de Seguridad Cibernetica.* [En línea] 20 de Enero de 2018. [Consulta el: 15 de Abril de 2022.] https://uip.mingob.gob.gt/wp-content/uploads/2019/03/Estrategia-Nacional-de-Seguridad-Cibern%C3%A9tica.pdf.

1.2.1 ISO/IEC 27005 - Gestión de riesgos de la Seguridad la Información

La norma ISO27005 ha sido un marco de referencia sobre la metodología entre la gestión de riesgos y la seguridad de la información, esto se debe a que con el pasar del tiempo se ha vuelto en un estándar internacional que se enfoca de la gestión de los riesgos precisos al área de la seguridad de información, la norma ISO27005 tiene como objetivo proporcionar directrices adecuadas y ordenadas, para una correcta gestión de riesgos de seguridad de la información[12].

Es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que puedan complicar la seguridad de la información de cualquier organización, o en este caso cualquier infraestructura. Si bien, es cierto que esta ISO no recomienda una metodología en concreto, favorece en el alcance real, ya que logra encaminara a la empresa hacia el sector adecuado de la propia industria por medio del Sistema de Gestión de Seguridad de la Información (o como se le conoce por sus siglas –SGSI-).

Los beneficios que trae su implementación se logran ver por la puesta en marcha de la gestión interna; mayor eficiencia de los procesos tales como la productividad, eficiencia de la energía, impacto ambiental y seguridad de la información. Otro punto para tener en cuenta es que la herramienta para medir sus resultados suele ser pieza clave, ya que favorece a la toma de decisiones, para cuando sea necesario integrar nuevos sistemas de gestión ya sean legales o de seguridad precisamente.

En este sentido el responsable de su aplicación elige el método que mejor se adapte, pero hay que destacar que la norma ISO 27005 proporciona cinco pasos importantes los cuales son: el plan interior y exterior; la definición del contexto organizacional interno y externo; la valoración de los riesgos tecnológicos; el tratamiento de los riesgos tecnológicos; y el monitoreo y proceso de gestión de desarrollo continuo. No obstante, así como en otras normas ISO y sistemas basado en procesos uno de los métodos considerado válido y muy recomendado en los sistemas de seguridad de la información, es el ciclo PHVA (planificar, hacer, verificar, actuar), que tiene como única finalidad la mejora continua.

[12] Technology, Department of Information Security and Communication. 2017. The Institute of Electrical and Electronic Engineers. *A framework for the information classification in ISO 27005 standard.* [En línea] 6 de febrero de 2017. [Consultado el: 20 de Abril de 2022.] Disponigble en: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7987208.

1.2.2 ISO/IEC 27032 - Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad

La norma ISO/IEC27032 fue publicada en el año 2012 con la finalidad de proporcionar un marco de orientación para mejorar los sistemas de ciberseguridad, a través de aspectos estratégicos y técnicos para la ciberseguridad y seguridad. La ISO27032 se basa en cuatro ejes principales: la seguridad de la información, seguridad de las redes, seguridad del internet y la protección de las infraestructuras críticas para la información.

Los objetivos se distinguen por brindar seguridad a todo tipo de empresa respecto con su información, tener planes de acción emergentes en caso de presentarse algún tipo de amenaza, brindar capacitaciones concretas a los miembros de la organización respecto al uso en todo lo relacionado a la ciberseguridad, crear alertas que permitan identificar posibles amenazas o amenazas ya materializadas y contar con estrategias para combatir los riesgos que se puedan llegar a presentar.

Como bien lo menciona el Centro Criptológico Nacional (En adelante CCN), *"La norma ISO/IEC 27032 facilita la colaboración segura y confiable para proteger la información de las personas en todo el mundo, ya que lo que se espera de ella es que prepare y permita combatir las distintas amenazas tales como los ataques de ingeniería social, informáticos, de intrusión como hackers, spyware y otro tipo de programas que resulten emergentes."*[13]

La gestión de la ciberseguridad según la norma ISO se basa en el análisis estratégico y la gestión del riesgo, estos llegan a ser uno de sus pilares fundamentales ya que permite tener un panorama claro de las amenazas, vulnerabilidades, zonas de riesgo y criterios de aceptación. Todo ello con la finalidad de poder optimizar la inversión en materia de ciberseguridad y priorizar la implementación de controles o salvaguardas, a lo que para ello la norma ISO27032 se apoya de la norma ISO31000 para el análisis y gestión de riesgos.

Dentro del marco de intercambio y coordinación del a información, los índices de ciberseguridad en un mundo tan hiper conectado a menudo cruzan fronteras geográficas

[13] CCN-CERT. 2012. *Norma ISO/IEC 27032, nuevo estándar de ciberseguridad.* [En línea] 17 de octubre de 2012. [Consultado el: 24 de Abril de 2022.] Diponible en la página: https://www.ccn-cert.cni.es/gl/gestion-de-incidentes/lucia/23-noticias/297-publicada-isoiec-27013.html#:~:text=M%C3%A1s%20concretamente%2C%20ISO%2FIEC%2027032,personas%20en%20todo%20el%20mundo..

entre países, por lo que es más que necesario establecer sistemas que coordinen y controlen la información para que esto ayude en la preparación de la respuesta a incidentes de ciberseguridad porque uno de los puntos estratégicos que engloba esta norma es garantizar el intercambio de información por canales seguros para hacer frente a los delitos informáticos.

Es muy importante tener en cuenta que esta norma viene a ser un tipo de guía técnica que proporciona metodologías para estar preparados y así poder preservar la confidencialidad integridad y disponibilidad de la información en el ciberespacio.

1.2.3 ISO/IEC 31000 - Gestión de Riesgos – Principios y Directrices

La norma ISO/IEC 31000 fue publicada en el año 2009 con el fin de ser una guía de referencia en lo relativo al riesgo y apoyo para los sistemas de gestión tales como la ISO90001, ISO14001, ISO45001 entre otros.[14]

A pesar de que no es una norma certificable su implementación trae una serie de beneficios que son: seguridad para los grupos de interés, eficacia ante situaciones de emergencia, acciones para posibles amenazas o riesgos. Paralelo a ello brinda credibilidad, prestigio, seguridad, confianza y competitividad para la organización.

La estructura de la ISO31000 está diseñada bajo el ciclo PHVA (planificar, hacer, verificar, actuar), y cuenta con ocho principios de los cuales la gestión del riesgo es el punto principal, así como la participación de todas las partes de la organización. La norma ISO31000 en su versión 2018 está estructurada en seis grandes clausulados distribuidos tales como: objeto y campos de aplicación; referencias normativas; términos y definiciones de principios; marco de referencia; y procesos. A nivel general podría pareciera que la gestión del riesgo está enmarcada en los principios, el marco de referencia y el proceso. Los principios vienen a ser las directrices principales del sistema de gestión, el marco de referencia es la estructura que soporta el sistema y el proceso hace referencia al mecanismo o metodología para dar un tratamiento eficaz a los riesgos. Algo que destaca es que la alta dirección debe de demostrar su compromiso.

[14] 262/STTF, Grupo ISO/TC. 2018. ISO - Online Browsing Platform (OBP). *ISO 31000:2018(es) Gestión del riesgo - Directrices.* [En línea] 1 de Febero de 2018. [Consultado el: 25 de Abril de 2022.] Diponible en: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es.

1.3 LEGISLACIÓN VIGENTE CON RELACIÓN A LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS EN LA UNIÓN EUROPEA, ESPAÑA Y GUATEMALA

1.3.1 Directiva 114/2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de las necesidades de mejorar su protección

Anteriormente se ha podido destacar la importancia de las Infraestructuras Críticas para la sociedad y para la funcionalidad de los gobiernos; como se llegó a mencionar en puntos anteriores, a la vista de las posibles amenazas a las que llegan a estar expuestos algunos gobiernos, la Unión Europea siendo una entidad geopolítica formada por múltiples Estados, a la vista del contexto que se suscitó por los ataques terroristas y por el desconocimiento del riesgo a nivel comunitario que se tenía en ese entonces. La Comisión Europea dio la puesta en marcha de establecer una Directiva que estuviera enfocada a la identificación y designación de Infraestructuras Críticas (IC) de Estado y Críticas Europeas (ICE) junto a la evaluación de las necesidades a mejorar para su protección, es así como en el año 2008 del 8 de diciembre se establece y aprueba la Directiva 114/2008/CE del consejo. Esta directiva tuvo como base la iniciativa del Libro Verde ya que sirvió como hoja de ruta para establecer el Programa Europeo para la Protección de Infraestructuras Críticas.

En este sentido lo que se busca con la Directiva 114/2008[15] es la coordinación de medidas entre los distintos actores, por lo que por medio de ella se atribuye tanto a los Estados miembros de la Unión Europea como a los mismos operadores o propietarios de dichas infraestructuras, la completa responsabilidad de su protección.

La Directiva establece las indicaciones necesarias en función de cómo establecer si una infraestructura debe de ser considerada como crítica o crítica europea, esto por medio del cálculo del número potencial de víctimas, impacto económico e impacto público, todo esto asociado a riesgos tecnológicos, catástrofes naturales y antrópicos, pero con mayor énfasis en las amenazas terroristas.

Esta Directiva es permite que los Estados miembros puedan incluir medidas de aplicación de otros sectores tales como las TICs, porque los sectores principales en los que se centra

[15] Europeo, Consejo. 2008. *Agencia Estatal Boletín Oficial del Estado . 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.* [En línea] 08 de diciembre de 2008. [Consultado el: 30 de Abril de 2022.] disponible: https://www.boe.es/doue/2008/345/L00075-00082.pdf.

esta Directiva es en el transporte y la energía, por lo que para ello la identificación de estas Infraestructuras por parte de los Estados fue y es crucial, porque no solo pretende identificar cuáles de estas llegarían a repercutir al Estado sino también a otros Estados, por temas de repercusiones transfronterizas importantes, al estar estas interconectadas. Para ello la evaluación y valoración por los criterios horizontales ya mencionados (número potencial de víctimas, impacto económico e impacto público) es más que necesario. La información de cuáles son las Infraestructuras Críticas Europeas (ICE) de cada Estado es un tema clasificado por cada gobierno y para los gobiernos que puedan verse afectados por infraestructuras críticas de otros Estados.

Una vez identificada la infraestructura crítica. se asigna un plazo no mayor a un año para que se elaboren los respectivos Planes de Seguridad del Operador (PSO), de los cuales los Estados tendrán el mismo lapso de tiempo para realizar sus propias evaluaciones de amenazas relativas a los sectores y subsectores, al mismo tiempo se dispone que se deba presentar dos informes al año sobre los distintos riesgos, amenazas y vulnerabilidades encontradas en cada sector de los cuales se haya evaluado como Infraestructura Crítica Europea (ICE), Esto con el fin de poder evaluar si existe la necesidad de introducir más medidas de seguridad adicionales. De la mano a ello se debe de tener en cuenta que en toda Infraestructura Crítica Europea (ICE) se debe de nombrar a un responsable de seguridad el cual servirá como enlace único para comunicar toda información pertinente a los riesgos, amenazas y vulnerabilidades.

La figura del responsable de enlace para la seguridad servirá precisamente como punto de contacto para temas de seguridad entre el operador o propietario de la Infraestructura Crítica Europea (ICE) y la autoridad de control establecida por el Estado miembro, para lo cual se establece de que todo Estado miembro debe de contar con un punto de control para realizar el contacto, esta figura se encargará de realizar la cooperación, comunicación y coordinación en los asuntos relacionados a la protección de estas Infraestructuras en el propio estado miembro, además de ello esta autoridad servirá de punto de coordinación con los demás Estados miembros y con la propia Comisión.

Todo esto sirve para resaltar las áreas más importantes que se deben de tener en cuenta al analizar la Directiva 114/2008 de una manera breve.

1.3.2 Ley 8/2011 Medidas de protección de las Infraestructuras Críticas

En España como consecuencia de la Directiva 114/2008 del consejo, para la identificación y designación de Infraestructuras Críticas Europeas (ICE), así como para el resto de los Estados miembros de la Unión, se realizó la trasposición adecuada de la Directiva a la legislación nacional respectiva, con la misma finalidad de proteger a la población y luchar contra las amenazas terroristas que se dirigieran a las infraestructuras críticas nacionales y las ICE; bajo esa línea y motivados a ejecutar lo dispuesto en la Directiva, España en 28 de abril de 2011 aprueba la ley 8/2011 por la que se establecen medidas para la Protección de las Infraestructuras Críticas en España (en adelante ley PIC)[16].

Esta ley se compone por dieciocho artículos que encuentran estructurados en tres capítulos, de los cuales el primero de ellos está destinado a la definición de los términos, el segundo regula los órganos y e instrumentos de planificación y el tercero se enfoca en establecer medidas adecuadas de protección y procedimientos necesarios para la correcta aplicación de la norma. Por lo que en ese sentido se puede decir que los dos grandes objetivos de esta norma son: el catalogar el conjunto de sectores estratégicos que brindan servicios esenciales a la población por medio de las infraestructuras crítica y sus sistemas; y diseñar una hoja de ruta a modo de plan donde se contengan las medidas de protección eficaces contra las posibles amenazas, tanto en el sentido físico como en el de la seguridad lógica de las TICs.

Uno de los aspectos que distingue la ley PIC, es la distinción que hace entre los servicios esenciales y las infraestructuras estratégicas. sin duda algunos puntos importantes, ya que las infraestructuras estratégicas llegan a ser las instalaciones, redes, sistemas físicos y lógicos de las TICs.

Como principales aportaciones, la ley PIC destaca por: crear un Sistema Nacional de Protección de las infraestructuras críticas, establecer las bases para el Sistema de Planificación de las PICs, organizar el Catálogo Nacional de Infraestructuras Estratégicas, y establecer un Equipo de Respuesta para Emergencias Informáticas (en adelante CERT). Así como el establecimiento de vías adecuadas para la comunicación y gestión, el

[16] *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas*. [En línea] 29 de abril de 2011. https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf.

establecimiento de la figura de Enlace como el Responsable de seguridad y el Delegado de la seguridad de estas Infraestructuras Críticas.

Otro aspecto a destacar de la Ley PIC es la forma de cómo se establece y se complementa por medio del Real Decreto 704/2011[17], por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas. En él se enmarca una serie de actividades en los cuales los Planes de Seguridad del Operador (PSO) y Planes de Protección Específicos (PPE) cobran relevancia, por los plazos que se establecen para su cumplimiento.

1.3.3 Ley Marco del Sistema Nacional de Seguridad – Guatemala

En Guatemala desde el año 2008 se aprobó la Ley Marco del Sistema Nacional por medio del decreto numero 18-2008, con esta ley se llegan a establecer las bases de los alcances para administrar y consolidar los componentes de seguridad del Estado de Guatemala, con el objetivo de hacer frente a los desafíos del siglo XXI.[18]

Dicha ley tiene como fin el desarrollo de las funciones de regulación, organización y estabilidad dentro de la seguridad del Estado de Guatemala, donde se genere una estructura de carácter orgánico funcional para que de una forma sistematizada y eficiente el País esté en capacidad de anticipar y dar respuesta segura a los riesgos, amenazas y vulnerabilidades; así como de la misma forma para prevenirlos, enfrentarlos y contrarrestarlos.

Por medio de esta ley se establece el Sistema Nacional de Seguridad, el cual representa un marco institucional del que dispone el Estado para enfrentar los desafíos que se presenten en el área de seguridad, estas acciones se realizan en el alto nivel, el cual está sujeto a controles democráticos, parte de sus actividades tiene como objetivo el contribuir con la seguridad y defensa de la nación junto al de las personas. Por lo que llega a ser un sistema abierto que contiene a otros sistemas, donde se interrelaciona con otros componentes y sistemas de administración pública que tiene un enfoque dirigido a la seguridad de la nación, tales como la Dirección de Inteligencia del Estado Mayor (DI-EMDN), Dirección General de Inteligencia Civil (DIGICI), Secretaría de Inteligencia

[17] *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.* [En línea] 20 de mayo de 2011. https://www.boe.es/buscar/pdf/2011/BOE-A-2011-8849-consolidado.pdf.

[18] Guatemala, Congreso de la República de. 2008. Ministerio de Gobernació. *Ley Marco del Sistema Nacional de Seguridad.* [En línea] 2008. [consulta el: 5 de Abril de 2022.] https://mingob.gob.gt/wp-content/uploads/2020/10/8.2-LEY-MARCO-DEL-SISTEMA-NACIONAL-DE-SEGURIDAD.pdf.

Estratégica del Estado (SIE) y Secretaría Técnica del Consejo Nacional de Seguridad (STCNS). Como aspecto a destacar y mencionar, esta ley llega a tocar muy pocos aspectos de la Infraestructura Crítica, pero sienta un punto de partida.

1.4 LEGISLACION VIGENTE CON RELACIÓN A LA CIBERSEGURIDAD EN LA UNIÓN EUROPEA, ESPAÑA Y GUATEMALA

1.4.1 Directiva 1148/2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea

Con el paso del tiempo las amenazas han ido evolucionando y en ese sentido surge la necesidad de establecer medidas elevadas para garantizar la seguridad lógica en materia de información, por lo que recordando un poco la Directiva 114/2008, el objetivo de esta se enfoca en la identificación de las infraestructuras críticas, para así evaluar las medidas de protección que estas disponen y así poder contrarrestar las amenazas pertinentes en materia de terrorismo; por un lado eso esta perfecto, pero hay que recordar que el mundo evoluciona y lastimosamente las amenazas también, por lo que las normas del juego con el paso de los años empezaron a cambiar pasando del terrorismo al ciberterrorismo. Por lo que con esta Directiva lo que se busca en su apartado normativo es el generar un espacio de trabajo y de comercio seguro dentro de la unión donde todos los Estados, para que así todos cuenten con las mismas normas y mismas protecciones, en este caso se entiende que la protección se enfoca hacia los ataques de ciberseguridad.

La Directiva destacó en el año 2016, que las capacidades existentes de ese entonces no bastaban para garantizar un elevado nivel de seguridad de las redes y sistemas de información que había en la Unión Europea, además se tenía en consideración la diferencia de preparación de los distintos Estados miembros, porque en materia de protección de infraestructuras críticas todo se estaba acomodando e igualando, pero con el tema de la informática había distintos desarrollos generando así una normativa muy fragmentada. Por lo tanto, se generaba un peligro inminente tanto como para consumidores como para empresas o como para la administración pública en general y las propias infraestructuras críticas de toda la Unión Europea, por lo que había que darle forma.

Por esa razón y antes del surgimiento de esta Directiva, se crea en el año 2013 la Estrategia de Ciberseguridad de la Unión, la cual recogía todas las preocupaciones antes

mencionadas. Este documento comprende los aspectos del mercado interior, justicia y política externa relacionada con el Ciberespacio. Sirviendo así de complemento a la Directiva 1148/2016 (conocida como directiva NIS)[19].

Bajo esa línea la directiva NIS, habla de una serie de mínimos de formación común, donde se expone una serie de requisitos mínimos en materia de desarrollo en capacidades de planificación, intercambio de información cooperación y requisitos comunes de seguridad para operadores de servicios esenciales (OES) y proveedores de servicios digitales (DSP), a los proveedores de servicios digitales se les insta desde la Unión Europea a adoptar las medidas oportunas para gestionar todo tipo de riesgo de seguridad, y además se les insta a notificar los problemas que presenten, En esta Directiva se propone la misma acción para que notifiquen los incidentes que podrían tener un efecto perturbador significativo para los Estados.

Siguiendo el punto anterior de la Directiva NIS, a la vista de que es oportuno que se realicen las notificaciones de incidentes, se propone la creación de una red de cooperación entre los distintos estados miembros, el cual bajo su artículo 12, establece la RED de CSIRTS, donde la Comisión Europea participa como observador y la Agencia de la Unión Europea para la Ciberseguridad (ENISA) apoya con la cooperación de los CSIRT.

Otro de los puntos que resalta en la Directiva NIS, es el de establecer a que todos los Estados miembros deben crear una Estrategia Nacional de Seguridad de Redes y Sistemas de Información, para así poder alcanzar y mantener un buen nivel de seguridad. De la mano ello establecer auditorías de seguridad, donde se comprueben los niveles de cumplimiento de las medidas establecidas por la estrategia de cada Estado e implementadas por los operadores de servicios esenciales.

De esta forma la directiva NIS, determina el objeto el cual es: regular la seguridad de las redes y sistemas de información utilizados para la provisión de servicios esenciales y servicios digitales. Junto a la creación de un sistema de notificación de incidentes que cada Estado miembro, bajo el establecimiento de un marco institucional determine para las autoridades competentes, junto a los órganos relevantes en el ámbito comunitario.

[19] Comisión Europea. 2016. Diario Oficial de la Unión Europea . *DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO.* [En línea] 6 de julio de 2016. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148&from=ES.

1.4.2 Directiva NIS 2

La Directiva NIS 2, representa una actualización de la Directiva NIS (anterior). Si bien, la Directiva NIS 2, sustituirá a la Directiva actual sobre la seguridad de las redes y sistemas de información, esta nueva Directiva tiene como objetivo mejorar la resiliencia y capacidad de respuesta del sector público y privado, a los incidentes en toda la Unión Europea.

Sentará las bases para las medidas de gestión de riesgos en materia de ciberseguridad, y establecerá la obligación de notificación en los sectores de transporte, energía, sanidad e infraestructura digital. A pesar de todas estas mejoras o cambios lo que se busca precisamente es que la Directiva NIS 2 elimine las diferencias que cada estado miembro de la Unión actualmente presenta en el campo de medidas de aplicación de ciberseguridad. Por lo que de esta forma en esta nueva Directiva se establecen normas mínimas para un marco regulador junto a mejores mecanismos de cooperación entre autoridades de cada Estado miembro.

Como novedad se establecerá la Red Europea de Organización de Enlaces de Crisis Cibernética (EU-CYCLONe) con el fin de mejorar como ya se mencionó la coordinación en la gestión de incidentes de ciberseguridad a gran escala.[20]

La ampliación en el ámbito de aplicación de normas destaca por su cambio, ya que en la anterior Directiva (que a la fecha aún sigue vigente), los Estados llegan a ser responsables de determinar cuáles son las entidades que cumplen con los criterios para ser considerados como operadores de servicios esenciales (OES), en esta nueva Directiva se establece una norma que determina el tamaño máximo para ello. Por lo que bajo esa línea se incluyen disposiciones adicionales para que se garantice su proporcionalidad, mayor nivel de gestión de los riesgos y criterios específicos para determinar cuáles son las entidades que están cubiertas.

La directiva NIS de la misma forma será de aplicación para las administraciones públicas, dado los constantes ciberataques que se han ido registrando.

[20] Equipo CCN-CERT. 2022. CCN-CERT SEGURIDAD AL DIÁ . *La Unión Europea refuerza su ciberseguridad y resiliencia con la aprobación de la directiva NIS 2.* [En línea] 25 de mayo de 2022. [Consulta el: 25 de mayo de 2022.] https://www.ccn-cert.cni.es/seguridad-al-dia/actualidad-ccn/11799-la-union-europea-refuerza-su-ciberseguridad-y-resiliencia-con-la-aprobacion-de-la-directiva-nis-2.html.

1.4.3 Real Decreto Ley 12/2018 de seguridad de las redes de sistemas de la información

Tras la aprobación de la Directiva 1148/2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (NIS), cada Estado miembro debía trasponer la Directiva al ordenamiento jurídico. España no fue la excepción y en el año 2018 por medio de un Real Decreto Ley 12/2018, aprueba a modo de urgencia dicha ley.

En esta ley surge una palabra interesante, aunque ya algo conocida y esta es la de: Operador de Servicios Esenciales (OES), como ya se sabe un operado de servicios esenciales: es cualquier entidad pública o privada que preste un servicio que dependa de redes y sistemas de información para la ejecución de actividades sociales o económicas; al mismo tiempo en el texto surge otro agente, el cual se establece como Operador de Servicios Digitales (DSP), esta figura es toda persona jurídica que presta un servicio de manera digital, dicho servicio puede ser esencial o no.

Al ver este escenario con los dos agentes OES y DSP, el panorama cada vez más se va tornado a que la sociedad está dependiendo últimamente en gran manera de las TICs, lo que significa que cada vez más los ataques informáticos pueden llegar a ocurrir a gran escala; por lo que bajo ese contexto, cobra mayor sentido la necesidad de aumentar la protección frente a ataques y vulneraciones en la redes, ya que al final la Unión Europea viene a ser una cadena donde si un eslabón se ve afectado por ser débil puede llegar a afectar a toda la cadena que representa, por lo que de esta forma y con estas medidas cada Estado se ve obligado a fortalecer las medidas de protección.

Para cumplir adecuadamente lo contemplado en la Directiva NIS, la ley se enfoca en: establecer una Estrategia Nacional de Ciberseguridad; así como también evaluar la seguridad de los sistemas de información; redes; documentación de las políticas de seguridad de los operadores de servicios esenciales; y aplicar infracciones catalogadas c como: muy graves, graves y leves al no cumplir con las respectivas obligaciones.[21]

De la mano a lo anterior, se puede entender que el enfoque se centra en el establecimiento de los CSIRTs, los cuales tienen la tarea de analizar los distintos riesgos y supervisar los

[21] Consejo de Gobierno. 2018. Boletín Oficial del Estado . *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y.* [En línea] 8 de septiembre de 2018. Disponible en la pagina web: https://www.boe.es/boe/dias/2018/09/08/pdfs/BOE-A-2018-12257.pdf.

incidentes de seguridad a escala nacional junto a la notificación y difusión de alertas y soluciones para su mitigación. Para ello se establecen y distribuyen los equipos de respuesta a incidentes para cada caso, tales como los que se describen en la siguiente tabla[22]:

Tabla 3: Distribución de los CERTs en España.

Organismo competente	Ámbito de competencia
CCN-CERT Centro criptológico nacional de Inteligencia	Su ámbito competencial se enfoca al sector público general, autonómico, local y sistemas que manejan información clasificada
INCIBE-CERT Instituto Nacional de Ciberseguridad	Su ámbito competencial se enfoca en la ciudadanía y el sector privado; al mismo tiempo el INCIBE-CERT presta servicios de respuesta a incidentes a las instituciones afiliadas a la RedIRIS, red académica y áreas de investigación española que se coordina con el CCN-CERT cuando estos son organismos públicos
CNPIC Centro Nacional de Protección de Infraestructuras Críticas y Ciberseguridad	Su ámbito competencial se centra en las Infraestructuras Críticas y operadores críticos, las capacidades de respuesta técnica se llevan a cabo por medio de los CSIRT de referencia. Al mismo tiempo figura como autoridad competente para los operadores de servicios esenciales que son críticos, siendo en este caso la oficina de coordinación cibernética (OCC) la responsable de coordinar en lo supuestos previstos de la ley PIC
ESP-DEF-CERT Mando Conjunto de Ciberdefensa	Su ámbito de competencial se centra en los sistemas de información, redes y telecomunicaciones de las Fuerzas Armadas, así como redes que específicamente y a modo confidencial se le encomienden y que afecten a la Defensa Nacional.

[22] INCIBE. 2020. INCIBE CERT. *GUÍA NACIONAL DE NOTIFICACIÓN Y.* [En línea] 21 de febrero de 2020. [Consultado el: 1 de Junio de 2022.] Disponible en la pagina web: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf.

1.4.4 Iniciativa de Ley 5601 contra la ciber delincuencia – Guatemala

Guatemala actualmente reconoce que carece de un marco legal que permita velar por la seguridad y control del cibercrimen, por la ausencia de coordinación y cooperación entre las distintas instituciones de los sectores, y con la escasa cultura de ciberseguridad en la sociedad, el desarrollo de una estrategia trasversal que permita establecer leyes en esta área se ve limitado. Sin embargo, existe una iniciativa de ley contra la ciberdelincuencia a través de la cual se busca tener una vía para regular diversos delitos que lleguen a ocurrir en el ciberespacio. Esta iniciativa de ley propone aprobar una ley para la prevención y protección de contra la ciberdelincuencia, por medio de la adecuación de normas penales existentes, así como regular y constituir conductas prohibidas en materia y pena a efecto de fortalecer las reglas de convivencias social y digital en el país[23].

De esta manera se motiva a los diputados a proteger a los ciudadanos de Guatemala de la delincuencia y ciberdelitos por medio de la ciberseguridad, derivado del extendido uso del entorno digital en actividades diarias que abarcan espacios de vida económica, cultural, industrial, escolar y de comunicación entre otras. Se ve impactada la globalización digital en la sociedad generando así un nuevo escenario de delincuencia basada en el anonimato y utilizando todo tipo de información personal o institucional que se resguarda en el entorno digital, ampliando así el campo de acción de los hechos delictivos no regularizados, que amenazan la seguridad y afectan la identidad, propiedad y la seguridad de las personas, empresas e instituciones. Ciberdelincuencia, ciberdelitos, ciberdefensa, fraude informático y protección de datos personales en internet son algunos de los términos que se oficializarán e incluirán en la legislación guatemalteca gracias a esta iniciativa de ley, por medio de importantes reformas a la ley contra la delincuencia organizada y a la ley del sistema nacional de seguridad.

Además de esto esta iniciativa propone la creación de centros de seguridad institucionales de respuesta técnica ante incidentes informáticos (CSIRT), así como la de un CERT que brindará alertas para detectar y dar atención eficaz y eficiente a los casos de emergencia de ciberseguridad y ciberdefensa, así como la realización de acciones para que los guatemaltecos puedan prevenir los ataques a sus datos o sistemas informáticos.

[23] Direccion Legislativa. 2019. Congreso de la Republica de Guatemala . *Iniciativa que dispone aprobar ley de prevención y protección contra la ciberdelincuencia*. [En línea] 6 de agosto de 2019. https://www.congreso.gob.gt/detalle_pdf/iniciativas/5614.

CAPÍTULO II – RIESGOS DE LAS INFRAESTRUCTURAS CRÍTICAS FRENTA A CIBERATAQUES DIRIGIDOS

2.1 ACTIVOS DE INFORMACIÓN

2.1.1 Gestión y clasificación de la información

Una vez vista las distintas leyes y directivas vigentes enfocadas por un lado a la Protección de las Infraestructuras Críticas, es necesario abordar y entrar en detalle sobre lo más importante dentro de la seguridad y esto viene a la aplicación de una correcta gestión y clasificación de la información. Para ello se es necesario disponer de datos precisos porque al ser conscientes de su importancia junto con los riesgos críticos que se puede suscitar, esto implica que toda la información que esté relacionada a los sectores críticos y estratégicos se maneje con carácter confidencial, por lo que para ello se deben abordar medidas adecuadas que consigan proteger la información. Al ser consciente de esta necesidad se establecen distintos canales de comunicación adecuados entre los Operadores Críticos y las Autoridades Encargadas de coordinar y vigilar que las políticas de seguridad impuestas por el CNPIC y las leyes vigentes se cumplan. Por lo que, en ese sentido, la figura del Responsable de Seguridad de la Información (en adelante RSI) deben de cumplir las directrices para establecidas para garantizar una correcta gestión de la información, así como también el cumplimiento de la obligación de reportar los incidentes en materia de ciberseguridad, hacia las administraciones públicas, Infraestructuras Críticas y Operadores Estratégicos que se detallan en el Real Decreto Ley 12/2018. Estas entidades de control y canales de comunicación son[24]:

Tabla 4: Esquema orientativo de autoridades competentes

AUTORIDAD COMPETENTE		
Tipo de Operador	Subtipo	Organismo Competente
Operador de servicios esenciales	Operador crítico	Centro Nacional de Protección de Infraestructuras y Ciberseguridad CNPIC
	No operador crítico	Centro Criptológico Nacional – CCN –
		Autoridad Sectorial
Proveedor de servicios digitales	Sector Privado	Centro Criptológico Nacional CCN
	Sector Publico	Centro Criptológico Nacional – CCN –

[24] INCIBE. 2020. INCIBE CERT. *GUÍA NACIONAL DE NOTIFICACIÓN Y.* [En línea] 21 de febrero de 2020. [Consultado el: 1 de Junio de 2022.] Disponible en la pagina web: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf.

2.2 RIESGOS QUE ENFRENTAN LOS SISTEMAS DE INFRAESTRUCTURAS CRÍTCAS

Algo que llega a caracterizar a las distintas leyes a lo largo del estudio son los análisis de riesgos que se proponen. En la ley PIC este estudio conlleva la tarea de definir, y plantear escenarios posibles de las distintas amenazas que se puedan suscitar, por lo que para ello se requiere, como ya se ha mencionado, que se realicen evaluaciones de las vulnerabilidades que posiblemente estén exponiendo a los sectores estratégicos, que brindan apoyo a las infraestructuras críticas. De la misma forma dicha evaluación sirve como un estudio para conocer en que aspecto es donde se debe mejorar. Estos análisis de riesgos se realizan si bien con la implementación de un Sistema de Gestión de Seguridad de la información (SGSI) por medio de la norma ISO27001, o por medio de la certificación del Esquema Nacional de Seguridad (en adelante ENS). Cuando se realiza el estudio de los activos de información más importantes para la empresa o industria, es fundamental realizar dicho análisis para garantizar o al menos mantener la integridad, disponibilidad y confidencialidad de los distintos activos esenciales. Por lo que para llegar a ello se deben de evaluar y estar en constante conocimientos de las distintas vulnerabilidades que se llegan a dar, junto a las ciberamenazas y ciberataques más comunes.

2.2.1 Vulnerabilidades más explotadas

Como bien se sabe una vulnerabilidad puede afectar a múltiples niveles de seguridad.[25] Para que una acción llegue a alterar el funcionamiento normal de un entorno industrial físico/lógico debe existir alguna vulnerabilidad que lo facilite, esto no tiene que ser visto como algo malo, ya que las vulnerabilidades deben de ser evaluadas para así poder considerar la razón de su existencia, junto a al escenario necesario para que se lleve a cabo determinando así de alguna forma el nivel de criticidad.

Como suele ser comúnmente las vulnerabilidades técnicas son las que centran más el foco de atención, si bien esto es completamente aceptable, no se debe de pasar por alto el

[25] Sevillano, Fernando . 2021. *Ciberseguridad Industrial e Infraestructuras Críticas.* España : RA-MA, 2021. ISBN: 978-84-1855-136-9. <<En el capitulo 4 del libro se reflejan los distitnos puntos a tener en cuenta de la seguridad de redes y sistemas, al mismo tiempo aborda temas como el desarrollo de las tecnologias asi como la incorporación de otras nuevas al los entornos industriales, este capitulo sin duda engloba los temas mas escenciales a tratar al momento de evaluar las amenazas y vulnerabilidades>>

análisis de otras variables que faciliten el hecho de que algo o alguien de una forma intencionada o no intencionada, pueda realizar esta situación.

Si bien es cierto que no todos los entornos, empresas u organizaciones se llegan a enfrentar al mismo tipo y cantidad de riesgos, amenazas y vulnerabilidades, es bueno al menos partir o tener en cuenta las siguientes áreas para analizar como un punto de partida:

- Arquitectura y diseño:
    - En el área de redes de sistemas la fase de diseño es un punto que no debe de pasar por alto, porque el diseño en la arquitectura de red así como su integración con otras redes, determinara como está la seguridad de las conexiones internas, estos puntos llegan a ser vulnerabilidades que no se deben de pasar por alto, porque esto da lugar a que existan equipos comprometidos, por lo que es esencial que se tenga documentada la definición del perímetro de red junto a sus puntos de control y se tenga en cuenta la revisión de políticas de seguridad.
- Configuración y mantenimiento
    - En entornos de Infraestructuras Industriales es muy común la presencia de equipos no gestionados, esto impide llevar acabo configuraciones necesarias de control, si bien la mayoría de ellos se diseñan de esa forma, sin funcionalidades relativas a la seguridad como la confidencialidad, integridad y autenticidad de las comunicaciones, algunas nuevas versiones cada vez más están integrando dichas funcionalidades, que en la mayoría de los casos los administradores no suele incorporar, desaprovechando de esta forma la protección en el intercambio de información generando así una vulnerabilidad.
- Áreas físicas
    - Las vulnerabilidades no solo se generan por los sistemas lógicos o por el equipo de base, las áreas físicas influyen en gran medida, porque no se puede pensar que el único acceso a los sistemas se va a realizar de forma lógica por medio de softwares o servicios de red.[26] La seguridad física debe de ser considerada también, contando con restricciones físicas y

[26] Sevillano, Fernando . 2021. *Ciberseguridad Industrial e Infraestructuras Críticas.* España : RA-MA, 2021. ISBN: 978-84-1855-136-9.

políticas que impidan que una persona propia o ajena obtenga las capacidades para realizar conexiones indebidas.

2.2.2 Ciberamenazas y Ciberataques más comunes

Teniendo en cuenta que las vulnerabilidades son un aspecto que se debe abordar por las repercusiones negativas que esto generaría, hay que tener en cuenta también que las ciberamenazas y ciberataques se pueden traducir como incidentes, al momento de tener vulnerabilidades no cubiertas. Por lo que el realizar un análisis de los incidentes más comunes acorde al sector es recomendable.

Algunos tipos de incidentes de seguridad de la información se basan en lo siguiente[27]:

- Acceso no autorizado
- Robo de contraseñas
- Pérdida de datos
- Infección por virus o malware
- Denegación de servicio y modificación de información indispensable.

Estos incidentes se pueden dar por diversos ciberataques tales como el: ciberespionaje, intrusión en la red de la empresa, ataque de denegación de servicio (DDoS), phishing o suplantación de identidad, puertas traseras, infección por malware o virus y fuga de información. Estos incidentes de seguridad pueden provocar la interrupción del servicio u operación en el caso de las Infraestructuras Críticas lo cual se traduce a la palabra riesgo.

Algo que hay que tener en cuenta es que las infecciones por malware y la recepción de spam son los incidentes más reportados, por lo que disponer de personal interno que realice las tareas de análisis adecuadas incide de manera directa en la percepción de este tipo de incidentes, debido a que tras un incidente normalmente se identifica lo más visible, pero en ocasiones se deja de lado las consecuencias de carácter más técnico, como bien se mencionó en el punto anterior. Pero en si los incidentes con mayor ocurrencia son los que afectan al tiempo de trabajo, así como los que implican problemas de disponibilidad o conexión de las redes.

[27] INCIBE. 2020. INCIBE CERT. *GUÍA NACIONAL DE NOTIFICACIÓN Y.* [En línea] 21 de febrero de 2020. [Consultado el: 1 de Junio de 2022.] Disponible en la pagina web: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf.

CAPÍTULO III – ANÁLISIS DE LA LEGISLACION VIGENTE Y DEL ESCENARIO ACTUAL DE GUATEMALA

3.1 ANALISIS DE LA LEY PIC VIGENTE EN ESPAÑA

A lo largo del desarrollo de este trabajo, por medio de distintas fuentes, informes, libros, Directivas y Leyes, se ha podido recalcar que las Infraestructuras Críticas son vitales para la economía y desarrollo de cualquier estado moderno, ya que estas son la pieza central en una buena parte del sistema productivo, de la misma forma los múltiples sectores como el transporte, ya sea por carretera, vía aérea, ferroviaria o marítima; estas en sí, también son esenciales para la sociedad actual, pues este sector es el eje que mantiene la cadena productiva y de consumo abastecida, así como también la vida diaria de los ciudadanos. Partiendo ahí y utilizando las palabras de Rafael Catalá Polo, que expone: *"La necesidad de garantizar simultáneamente el derecho a la seguridad y el derecho a la libertad de movimientos recogidos en la Constitución española, obliga a los poderes públicos a realizar esfuerzos en aras de diseñar un sistema óptimo de seguridad en los transportes públicos y las Infraestructuras Críticas que los soportan."* – Por lo que, partiendo de esa premisa, la Ley 8/2011 o como usualmente se le llama Ley PIC por la que se establecen medidas para la protección de las infraestructuras críticas, cumple con el objetivo si bien de la Directiva Europea 114/2008, pero más que todo cumple con lo establecido en la Constitución española lo cual es garantizar el derecho a la seguridad y libertad de movimiento de los ciudadanos.

Algo que en lo personal me llamó la atención al momento de realizar el estudio de las bases de esta Ley, fue el Sistema de Protección de las Infraestructuras Críticas (en adelante – Sistema –), sin duda esto es uno de los rasgos que llega a caracterizar esta ley, y es que la creación del llamado Sistema estableció la denominación para agrupar el conjunto de órganos y unidades organizativas que llegan a tener algún grado de intervención en el ámbito de la Protección de las Infraestructuras Críticas. Para entrar en detalle en el artículo 5 del primer texto se contempla su composición de manera que en los Sistema se integraron representantes de:

a) La Secretaría de Estado de Seguridad
b) Los ministerios y organismos delegados en materia de Protección de Infraestructuras Críticas
c) Las Delegaciones del Gobierno en las Comunidades Autónomas

d) Los operadores Críticos tanto del sector público como del sector privado, entendiendo por tales los propietarios o gestores de las infraestructuras mencionadas
e) La Comisión Nacional para la Protección de las Infraestructuras Críticas

Junto a ello también se incorpora el CNPIC, el Grupo de Trabajo PIC, las Comunidades Autónomas y las entidades locales. Con esto, el texto por sí solo demuestra la importancia organizativa que representa. Ya que al ser una Ley de este tamaño la óptica de coordinación necesaria para lograr la eficacia y la agilidad operativa deseada tanto en el plano económico y presupuestario se vio implicado desde un inicio, aspecto que fue clave en el recorrido administrativo inicial de esta norma.

Pese a que el proceso de aprobación de dicha Ley desde el año 2009 se vio afectado por una serie de modificaciones que fueron retrasando su aprobación hasta el año 2011, se puede decir que dicho retraso favoreció en convertir el texto del Proyecto Ley presentado, en dos de rango diferente: uno como rango de Ley y forma de Anteproyecto, y otro con rango reglamentario y forma de Proyecto de Real Decreto, ya que el consejo de estado exigía la existencia de un rango legal para aquellos preceptos que imponían obligaciones a los operadores y un rango reglamentario aparte, obteniendo así la promulgación en 2011 de la Ley 8/2011, de 28 de abril por la que se establecen medidas para la Protección de Infraestructuras Críticas, y su reglamento de desarrollo mediante el Real Decreto 704/2011, de 21 de mayo, por el que se aprueba el reglamento de Protección de Infraestructuras Críticas.

Por parte de la Ley 8/2011, esta cuenta con 18 artículos, estructurados en tres títulos [28], el Título I, se destina a profundizar en las definiciones de los términos acuñados por la Directiva 114/2008/CE, así como a establecer las cuestiones relativas al ámbito de aplicación y objeto. El Título II, se enfoca precisamente a regular los órganos e instrumentos de planificación que se integran en el sistema de Protección de las Infraestructuras Críticas. El Título III, establece finalmente las medidas de protección y los procedimientos que deben derivar de la aplicación de dicha norma. Ahora de la parte del Real Decreto 704/2011, este consta de 36 artículos estructurados en cuatro títulos de

[28] ***Ley 8/2011,*** *de 28 de abril, por la que se establecen medidas para la.* [En línea] 29 de abril de 2011. Disponible en: https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf.

los cuales se destaca lo siguiente[29]: En su Título I, resalta el área de definición y desarrollo del Catálogo Nacional de Infraestructuras Estratégicas, donde se enfoca en el registro administrativo del Ministerio del Interior que contiene la información completa, actualizada y contrastada de todas las infraestructuras estratégicas ubicadas en el Estado Español, así como también de las clasificadas como Críticas Europeas que afecten a la misma España por medio de otros estados. El Título II, se enfoca al Sistema de Protección de Infraestructuras Críticas, en esta parte se describen todas las competencias de los agentes que forman parte de dicho Sistema, así como las previsiones legales relativas a los órganos creados por la Ley tal como el CNPIC, la comisión nacional para la Protección de las Infraestructuras Críticas y el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas. El Título III, habla sobre los instrumentos de planificación exigibles a los agentes del Sistema, centrándose en cada uno de los Planes que se estructuran secuencialmente, así como el registro y revisión de los mismos, para ello se define un plazo para elaborar lo siguiente:

Tabla 5: Planes exigibles a los agentes del Sistema PIC

PLANES	ENFOQUE
Planes de elaboración administrativa	• Plan Nacional para la Protección de las Infraestructuras Críticas, aprobado por el secretario de Estado de Seguridad • Planes Estratégico-Sectoriales, que deberán elaborar los distintos agentes del Sistema como los ministerios y cuya aprobación corresponde a la comisión de Protección de Infraestructuras Críticas • Planes de Apoyo Operativo, a elaborar por el Cuerpo policial Estatal o, autonómico en su caso, que será supervisado por la delegación del Gobierno.
Planes elaborados por Operadores Críticos, públicos y privados	• Plan de Seguridad de los Operadores, encargados de definir las políticas generales para garantizar la seguridad de las instalaciones. • Plan de Protección Especifica, es un documento operativo donde se define las medidas concretas a implementar en cada una de las infraestructuras

[29] *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.* [En línea] 20 de mayo de 2011. https://www.boe.es/buscar/pdf/2011/BOE-A-2011-8849-consolidado.pdf.

Siguiendo con el Título IV, este se enfoca en la definición de los Responsables de Seguridad, enlace, y Delegado de Seguridad. El Responsable de seguridad y enlace se caracteriza por representar al Operador Crítico ante la Autoridad Competente, que viene a ser la Secretaría de Estado de Seguridad de toda la Infraestructura junto al reporte de los planes. Otro aspecto de este Título es que se ve alineado a la seguridad de las comunicaciones, que para garantizar dichas comunicaciones se requiere de la certificación adecuada por el Centro Criptológico Nacional y del Centro Nacional de Inteligencia.

Finalmente, de esta forma es como se estructura y aprueba tanto la Ley 8/2011 (ley PIC) como el Reglamento por medio del Real Decreto 704/2011, siendo así un complemento ideal.

3.2 POLÍTICAS DE PROTECCION DE INFRAESTRUCTURAS CRÍTICAS

Como se ha podido ver, dentro del marco normativo asociado a la protección de infraestructuras críticas y al aspecto asociado a la ciberseguridad industrial, tiene especial relevancia en España la Ley 8/2011, junto al reglamento 704/2011 que sirve de complemento para poder cumplir con los dos grandes objetivos de esta norma, tales como: el establecimiento de un escenario donde se diseñe un planteamiento que contenga medidas de prevención y protección eficaz contra posibles amenazas tanto como en el plano de seguridad física, así como el de la seguridad lógica. Para lo cual el establecimiento del catálogo del conjunto de servicios esenciales, y estratégicos para la sociedad sirve como punto de partida para que así se proceda con el diseño y planteamiento de las medidas.

No es de extrañarse que desde los atentados del 11-S y desde los atentados ocurridos en 2004 y 2005 en Europa, los Estados vieran la necesidad de instaurar políticas de protección para los servicios esenciales que dan vida a la sociedad y al propio Estado. Y es que en su mayor parte los servicios proporcionados por la sociedad se realizan gracias a las instalaciones, redes o, sistemas, que han pasado a tomar en un escaso espacio de tiempo un protagonismo extraordinario por su relevancia y dependencia en el marco de la gestión de riesgos y crisis.

En esa medida, la implementación de políticas, leyes o estrategias desarrolladas por distintos gobiernos y en este caso por España han valorado lo que es importante en aras de la sociedad. Algunas de ellas llevadas a cabo por iniciativas de la Comisión Europea

con el lanzamiento del Programa Europeo de Protección de Infraestructuras Críticas (EPCIP) en 2004 y la posterior Directiva 114/2008/CE. En el caso de España sus primeras aproximaciones casi que en paralelo al EPCIP, pero no fue hasta en 2007 que con la firma por parte del Secretario de Estado de Seguridad del Plan Nacional de Protección de Infraestructuras Críticas (PNPIC) se creara y se estableciera el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC). Desde entonces en España por medio de dicho centro se ha venido trabajando en la arquitectura, composición y establecimiento de un sistema de Protección de Infraestructuras Críticas que con el paso del tiempo y con el año en fecha de 2022 se puede decir que se han estado trabajando de manera formidable, aunque se debe de tener en cuenta que los hitos en el establecimiento de las Leyes PIC han ayudado en gran manera a que se consolidara una base como punto de partida en este tema tan complejo.

Bajo esta línea lo que se pretende es analizar las líneas maestras de las políticas que conforman y constituyen el fundamento de esta normativa PIC española, junto a la hoja de ruta abordada por el CNPIC. Como base evidentemente se utiliza la *Ley 8/2011, ley PIC*[30], el Reglamento por el *Real Decreto 704/2011*[31] y el Libro: *"Marco legal y de gestión de la protección de las Infraestructuras Críticas en España"*[32].

Partiendo de la necesidad de la PIC, a lo largo de este trabajo en muchas ocasiones, se ha reiterado los riesgos y repercusiones que conllevaría el no tener normas, sistemas, canales de comunicación, y equipo de respuesta ante emergencias/incidentes informáticos, operando en el escenario del Estado o gobierno. Esto debido a la dependencia que cada vez es mayor de parte de la sociedad, así como la del gobierno para el desenvolvimiento normal de los sectores de producción y de gestión en la vida ciudadana. Aunque hay que tener en cuenta, que, así como el Estado y las personas dependen de los servicios que estas brindan, las infraestructuras críticas también suelen ser dependientes entre ellas mismas para optimizar sus procesos y brindar mayores servicios o soluciones. Esto no tiene nada de malo, pero al mismo tiempo los problemas de seguridad pueden llegar a

[30] *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la.* [En línea] 29 de abril de 2011. Disponible en: https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf.
[31] *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.* [En línea] 20 de mayo de 2011. https://www.boe.es/buscar/pdf/2011/BOE-A-2011-8849-consolidado.pdf.
[32] Vanaclocha, Francisco J. 2013. *MARCO LEGAL Y DE GESTIÓN DE LA PROTECCION DE LAS INFRAESTRUCTURAS CRÍTICAS* . Madrid : McGRAW-HILLI INTERAMERICANA DE ESPAÑA , 2013. 978-84-481-8593-0.

desencadenarse en cascada, si no se contemplan medidas adecuadas, por esa razón la clasificación e identificación se vuelve un tema crucial, ya que, se debe evaluar y conocer cómo es que está el escenario para no tener sorpresas. Por esa razón España en su política de seguridad, dentro del sistema PIC cuenta con la identificación y clasificación en base al impacto potencial de una serie de criterios, para determinar las vías que llevarían a suscitar una interrupción de la misma. Es por ello por lo que se maneja una base de cuatro criterios fundamentales, (los famosos criterios horizontales de criticidad[33]). De los cuales es importante conocer:

1. Número de personas que afectas, valorado en función del número potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública.
2. El impacto económico en función de la magnitud de las pérdidas económicas y el deterioro de productos y servicios
3. El impacto medioambiental, degradación del lugar y sus alrededores
4. El impacto público y social, por la incidencia en la confianza de la población sobre la capacidad de las Administraciones públicas, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales.

La mayoría de países desarrollados que implementaron, e inclusive países en vías de desarrollo que están empezando a ver este tema, llegan a coincidir en las mismas necesidades de abordar esta problemática, aunque la idea es que en un mundo tan globalizado como el de hoy en día, donde la cadena de suministros ya no depende precisamente de los operadores de servicios esenciales del propio estado, se llegue a abordar este tema de forma global a manera de cooperar con socios estratégicos, en el caso de España y la Unión Europea, se abordó por medio de la Directiva 114/2008, esto vino bien, ya que se fundamentaron las bases adaptando lo propuesto por la Directiva al marco normativo español, junto a los aspectos que el propio Estado Español contempló como la organización política-administrativa, así como también las condiciones sociales y culturales.

[33] Art. 2 de la Ley 8/2011, *de 28 de abril, por la que se establecen medidas para la.* [En línea] 29 de abril de 2011. Disponible en: https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf.

Siguiendo con el análisis, pero esta vez no desde un punto de vista de la necesidad de la PIC, resalta el apartado de los aspectos que las políticas PIC deben contemplar, si bien va un poco de la mano al punto anterior, donde se hace hincapié en la necesidad de identificar las infraestructuras críticas, conforme a los propios intereses nacionales, así como la necesidad de establecer o promover una colaboración con la PIC, que se ve más que sustentada por los efectos que ocasionaría la caída en cascada. Así que desde ese punto queda claro que se debe de conocer todo el escenario, pero siendo honestos, no todas las infraestructuras críticas llegan a ser propiedad del estado, para ello existen sectores privados que operan su propia industria. Por lo que es más que necesario establecer un punto de cooperación entre el Estado y la empresa privada, junto a la cooperación ciudadana. España lo supo abordar al momento de establecer la ley, debido a que por medio de este análisis surge el concepto de asociación público-privada. Este concepto lo llevó a cabo el CNPIC desde sus inicios, y se le dio un refuerzo con la aprobación de la Estrategia Nacional de Seguridad de España en 2011, En esta Estrategia, la gestión de riesgos es un proceso clave porque llega a estar focalizado a identificar los riesgos posibles y establecer escenarios hipotéticos de lo que pudiera llegar a ocurrir, para así evaluar las vías adecuadas que se deben de seguir, así como las medidas preventivas.

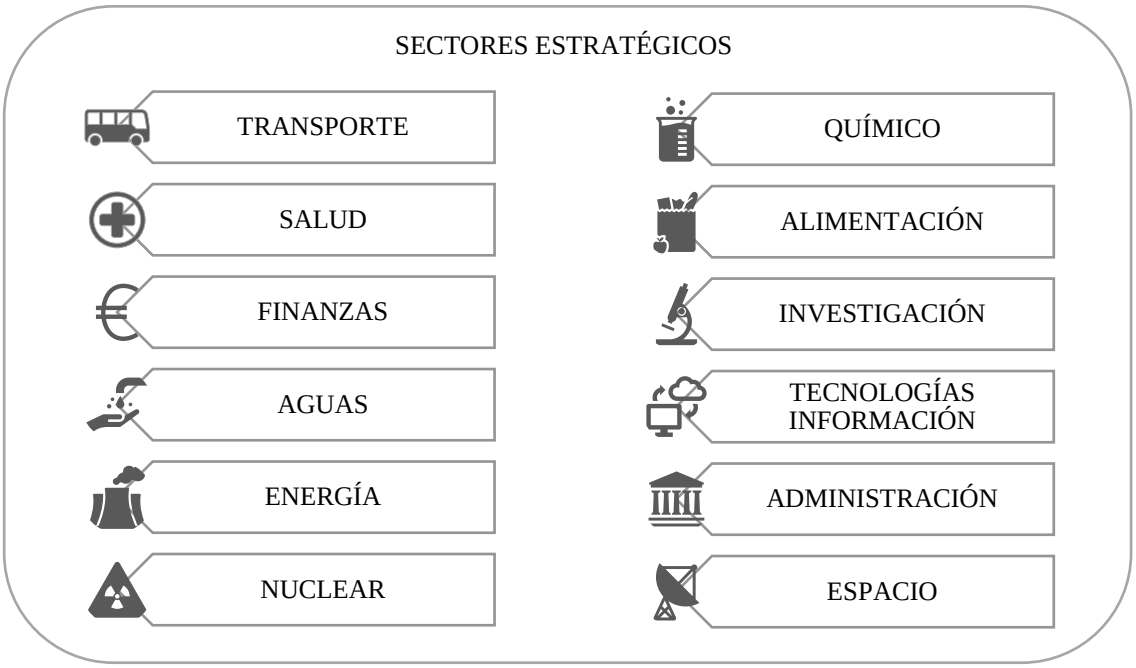
La implantación de estas medidas suele variar por lo visto según cada Estado o País (entiéndase País fuera de la Unión Europea), porque algunos al momento de implantar este tipo de medidas optan por utilizar vías como la cooperación público-privada, que está bien para mejorar la protección de la infraestructura crítica; otra vía que suele utilizarse y pareciera que es la vía más adecuada es la de implantar medidas legales dirigidas a los sectores en específico. Pero sea una u otra se debe tener en cuenta tres parámetros importantes como: el grado de participación del sector privado; el tipo de estructura sobre la cual se fundamentará la colaboración ya sea por enfoque voluntario o enfoque regulado; o bien, la madurez del Sistema.

En el caso de España y de la mano con la Ley PIC, se puede ver que el enfoque abordado fue el Regulado, aunque para ese entonces con los sucesos del 2004, España ya había empezado a establecer buenas prácticas para las infraestructuras críticas.

Ahora bien, para el área de identificación de las infraestructuras críticas, a nivel global existen dos formas para llevar a cabo la tarea de identificarlas por los diferentes Estados o países. Para ello se da la evaluación de abajo-arriba, la cual se hace por medio de un

estudio de todos los activos existentes en el país, aplicando así criterios de evaluación para determinar el grado de criticidad. Esto la verdad llega a ser una tarea muy extensa por la cantidad de posibles infraestructuras que pueden ser evaluadas, por lo que resulta un proceso muy costoso; por otro lado, se tiene la evaluación de arriba-abajo, mediante el cual previamente se determina el número de sectores y de los que de ese sector se desprenden, con el fin de conocer la cadena de producción o del servicio esencial. En el estudio de la Ley PIC, España lo llega a abordar bajo la evaluación de arriba-abajo, esta fue la que se implementó a la hora de determinar cómo se iban a identificar los sectores, de los cuales se identificaron doce sectores estratégicos, que a su vez se llegan a subdividir en subsectores, ámbitos de operación y segmentos. A manera de recordar España identificó los siguientes sectores estratégicos para su protección[34]:

Ilustración 2: Sectores estratégicos identificados para la PIC



Una vez identificado los sectores, se sigue con al proceso de clasificación, el cual se realiza a través de los Planes Estratégicos Sectoriales (PES)[35] creados por la Ley 8/2011, Estos PES sirven para definir y clasificar cual es el perfil de cada sector estratégico.

[34] Sevillano, Fernando . 2021. *Ciberseguridad Industrial e Infraestructuras Críticas.* España : RA-MA, 2021. ISBN: 978-84-1855-136-9. << El capítulo I, apartado 1.5 de activos específicos, da una clara interpretación de los sectores fundamentales para las IC, el cual proyecte la dependencia de las sociedades hacia estas infraestructuras >>

[35] Art. 14 de la Ley 8/2011, *de 28 de abril, por la que se establecen medidas para la.* [En línea] 29 de abril de 2011. Disponible en: https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf.

Una vez identificado y clasificado los servicios esenciales, por medio de los Planes Estratégicos Sectoriales, se realiza un estudio sobre cuál es el funcionamiento característico en general, junto al estudio de la estructura interna a nivel nacional, logrando así identificar el tipo de Infraestructura; posterior a ello cada Plan Estratégico Sectorial identifica y realiza una referencia a las interdependencias con otros servicios esenciales prestados, de la misma forma con sectores, o subsectores, sean específicamente del país o del exterior. Todo esto con la ayuda y ejecución siempre del CNPIC junto al apoyo de los ministerios técnicos competentes en cada sector, para así de esta forma poder identificar aquellos operadores propietarios de infraestructuras, o gestores de las infraestructuras, sobre las que recaen los servicios esenciales.

Puede que sea un poco complicado, pero entender la base es fundamental, ya que una vez identificadas en su totalidad las infraestructuras críticas estratégicas mediante los métodos previamente mencionados se clasifican en cinco categorías. Tales como críticas, complementarias y no consideradas. De acá es donde se forma el catálogo nacional de Infraestructuras Críticas, proceso que es custodiado y acompañado siempre por el CNPIC. Cabe destacar que solo las infraestructuras críticas están afectadas por las disposiciones de la Ley 8/2011 y el Real Decreto 704/2011 en el reglamento de aplicación.

A modo de representar las 5 categorías de los niveles con su clasificación de Infraestructura. La tabla de impacto se muestra en el anexo I, junto con la tabla de incidencia sectorial anexo II, así como la composición del sistema PIC español[36] en el anexo III.

Seguidamente luego de analizar el modelo que utiliza España sustentado por el artículo 3 y 13 del Real Decreto 740/2011, es crucial entender los análisis de la dependencia e interdependencia de las Infraestructuras críticas, para este punto la premisa de que las infraestructuras críticas son fundamentales para el funcionamiento de la sociedad está más que claro, pero aparte estas mismas como ya se ha dicho, llegan a estar altamente interconectadas para los aspectos de las funciones societarias básicas, y al mismo tiempo son mutuamente dependientes de muchas formas. Como se ha podido ver anteriormente, en el proceso de identificación de las infraestructuras críticas, las dependencias pueden llegar a ser esenciales, ya que esto puede llegar a determinar si una infraestructura es

[36] Sevillano, Fernando . 2021. *Ciberseguridad Industrial e Infraestructuras Críticas.* España : RA-MA, 2021. ISBN: 978-84-1855-136-9. << El capítulo III página 71 se encuentran las tablas correspondientes a la Tabla General de Impacto, Tabla de Incidencia Sectorial, y Sistema PIC >>

crítica o no, y esto no por su impacto primario sino por el efecto que se puede llegar a dar en cascada al producirse una amenaza.

Para ello los análisis de dependencia se llegan a utilizar como una base en el aspecto de la continuidad del negocio, porque se permite priorizar de forma correcta como es que se realizará la distribución de recursos, medidas y contramedidas, haciendo posible que se mejore el proceso de toma de decisiones. Es por eso por lo que se debe de entender y tener en cuenta los conceptos y tipos de (inter)dependencia.

La dependencia viene a ser la relación entre dos productos o servicios, en donde un producto o servicios se vuelve necesario para la generación de otro producto o servicio. Seguidamente la interdependencia se define como la mutua dependencia entre productos o servicios. En el área de la PIC se incluye en las dependencias los servicios esenciales y las infraestructuras que las llegan a soportar. Para todo esto la (inter)dependencia se distribuye en tres tipos tales como:

- Dependencia geográfica: esto es cuando un suceso ambiental de la región puede generar cambios en una infraestructura, usualmente estos solían ser los más esperados y los que más se contemplaban.
- Dependencia física: esto es cuando el estado y composición de una infraestructura depende de los resultados materiales de otra, acá es donde se empieza generar una posible cascada que tiene que ser evaluada por la cadena de producción.
- Ciberdependencia: esto es cuando el estado y funcionamiento de una infraestructura está ligada y depende de la información trasmitida por otras infraestructuras que brindan información esencial, en este punto también se contempla la posibilidad de sub incidentes por cascada.

Como se menciona la interdependencia física, así como la cibernética llegan a ser transversales a los sectores estratégicos junto a la titularidad pública o privada de las distintas empresas que son operadoras. Por esta razón en España se llega a contemplar la interdependencia en el ámbito de las PIC según la Ley 8/2011[37] en su artículo 2 inciso j, como los *‘‘efectos que una perturbación en el funcionamiento de la instalación o servicio produciría en otras instalaciones o servicios, distinguiéndose las repercusiones en el*

[37] Art. 2. j) de la Ley 8/2011, *de 28 de abril, por la que se establecen medidas para la.* [En línea] 29 de abril de 2011. Disponible en: https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf.

propio sector y en otros sectores, y las repercusiones de ámbito local, autonómico, nacional o internacional"

Por esta razón, la base y estructura por la que España tiene formulada la Ley PIC, se puede decir que llega a contemplar cada escenario posible, ya que en el año 2011 seguidamente de la publicación de la Ley 8/2011 y el RDL 704/2011, el Ministerio del Interior publica una serie de Guías de Contenidos Mínimos para que el operador crítico realice el estudio y evaluación dentro de sus Planes de Seguridad del Operador (PSO), y de la misma forma en sus Planes de Protección Específicos (PPE), con el fin de contemplar las interdependencias que, en cada caso se lleguen a identificar, explicando de forma breve los motivos de cómo se originan dichas interdependencias. Para así poder reflejarlas en el Catálogo Nacional de Infraestructuras Estratégicas, permitiendo de esta forma poder relacionar las distintas infraestructuras a nivel operativo.

Para poder conseguir todo lo expuesto anteriormente, la cooperación público-privada (CPP) como bien se ha mencionado, es esencial y en la Ley PIC se contempla, y esto porque es una realidad que la necesidad de la CPP en la protección de las Infraestructuras Críticas es más que necesaria, porque así como en muchos países desarrollados la mayoría de las infraestructuras críticas suelen estar operadas o llegan a pertenecer a empresas privadas, en el caso de España la información de la totalidad de infraestructuras críticas que cuenta el país, es información clasificada pero en España se calcula que el 80% y un poco más, suelen ser de empresa privada[38]. Situación que hace necesaria una cooperación y coordinación adecuada tanto por el sector público como con los operadores privados para obtener buen grado de resiliencia ante, durante y después de un eventual desastre. El Éxito de la CPP en España se debe primero que nada al Marco Regulatorio, la Transparencia, Confianza, Respeto Neutralidad, Interés Común y expectativas realistas. La fórmula puesta en práctica por el Gobierno de España para la construcción de una fructífera CPP se basa como ya se mencionó en los puntos anteriores, en una cooperación regulada por la Ley 8/2011, con la finalidad de obtener un alto grado de control de los procesos, a pesar de esto la Ley puede ser flexible propiciando con esto una cooperación sobre la base. En todo caso la ley maneja un conjunto equilibrado.

[38] LISA institute. 2019. LISA institute. *Infraestructuras críticas: definición, planes, riesgos, amenazas y legislación.* [En línea] 28 de octubre de 2019. https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas. << España dispone de más de 3.700 infraestructuras críticas reconocidas, el resto es confidencial>>

3.3 ANÁLISIS DE ESCENARIO EN GUATEMALA

3.3.1 Análisis actual

El estado actual de Guatemala frente a la seguridad cibernética es un poco curioso por la carencia de marcos legales, esto sin duda alguna es una necesidad y Maxime hoy en día con la hiper conectividad de este mundo globalizado. Enfocando el análisis hacia el eje objetivo de las Infraestructuras Críticas dentro de este trabajo, y con el deseo de articular y destacar aspectos importantes, para tener en cuenta a la hora de que en Guatemala se llegue a establecer un marco legal para la coordinación nacional, referente a las infraestructuras críticas, se realiza este análisis de cómo se encuentra Guatemala para esta área.

Uno de los grandes retos que la mayoría de países enfrentan en Latinoamérica sino es que, en todo el mundo, son las amenazas tecnológicas que han surgido durante el desarrollo de la misma tecnología. Aunque, a decir verdad, esto suele pasar a segundo plano cuando los países se enfrentan al reto de poder formular iniciativas, que fortalezcan los marcos jurídicos, para poder formular vías de protección de las infraestructuras críticas.

Es importante destacar que los objetivos principales de los actos delincuentes relacionados al cibercrimen se centran en los ataques hacia las Infraestructuras Críticas, dentro de las cuales sobresalen la red eléctrica, red de telecomunicaciones, y transporte. Por lo que en ese sentido es más que importante fortalecer los marcos regulativos y normativos, relacionados con las infraestructuras críticas, debido a que, cómo se sabe, si se interrumpe el funcionamiento de alguna, el impacto será devastador, esto considerando la seguridad, salud, bienestar económico y el eficaz funcionamiento de las administraciones públicas.

En el caso de Guatemala no solo afectaría a todas las áreas previamente mencionadas dentro del país, sino que también puede llegar afectar a los países vecinos en Centroamérica, porque Guatemala brinda servicios esenciales tales como la red eléctrica entre otros. Por esa razón, la existencia de un catálogo que establezca medidas de definición, y junto a ello se identifiquen las infraestructuras críticas, se hace cada vez más necesario, y esto por los sucesos vistos en los países vecinos tales como Costa Rica, que últimamente han ido experimentando un gran número de ataques informáticos, que han llegado a paralizar las administraciones públicas.

Analizando los pasos establecidos en el eje legislativo de la estrategia de seguridad de la nación 2020-2024 de Guatemala[39] se contempla la posibilidad de crear, aprobar e implementar una ley de Infraestructuras Críticas que permita identificar y analizar, las características principales de los distintos sectores que proveen servicios esenciales, junto al establecimiento de medidas de prevención, protección y recuperación contra amenazas. Esto sin duda es una noticia que abre la puerta a que por fin Guatemala establezca las bases adecuadas para trazar una hoja de ruta que permita dar continuidad, aunque los gobiernos cambien, más que todo porque de acuerdo con el Reporte 2020 del Banco Interamericano de Desarrollo (BID) y la Organización de Estados Americanos (OEA), sobre la "Ciberseguridad, Riesgos y Avances de América Latina y el Caribe"[40] el crimen en línea ya supone, aproximadamente, la mitad de todos los delitos contra la propiedad que tienen lugar en el mundo, y estos daños económicos solo por ataques cibernéticos se estima que sobrepasen el 1% del PIB y los ataques a las infraestructuras críticas podría alcanzar hasta el 6% si no se establecen medidas de coordinación, control y cooperación público-privado en este tema.

Según el reporte previamente mencionado del BID y la OEA, basado en el Modelo de Madurez de la Capacidad de Ciberseguridad, que mide los niveles de respuesta de los distintos países en cinco dimensiones por indicadores, Latinoamérica aún no se encuentra preparada suficientemente para hacer frente a diversos ataques del ciberespacio, ya que únicamente 7 de 33 países tienen un plan de protección de sus infraestructuras críticas, pero no todo está perdido ya que desde el año 2016 la región ha ido mejorando poco a poco, no es suficiente pero el promedio ha ido subiendo, aunque el promedio regional aún se sitúa entre 1 y 2, donde en la escala 1 llega a significar la etapa de inicio; 2 la etapa formativa que empieza a crecer; 3 la etapa de consolidación donde todo lo establecido ya está funcionando; 4 la etapa estratégica donde nacen decisiones importantes; y 5 la etapa dinámica donde la tecnología responde a las amenazas. Centroamérica en esa escala como bloque, presento un promedio de 2 en el apartado de Tecnologías, 2 con 3 en el apartado de Marcos Legales y Regularización, y un promedio demasiado bajo en el apartado de

[39] Consejo Nacional de Seguridad -CAP-. 2020. Secretaría Técnica del Consejo Nacional de Seguridad República de Guatemala. *ESTRATÉGICA DE SEGURIDAD DE LA NACIÓN 2020 - 2024.* [En línea] 5 de Abril de 2020. https://stcns.gob.gt/wp-content/uploads/2022/05/Agenda-Estrategica-de-Seguridad-de-la-Nacon-2020-2024.pdf.

[40] Banco Interamericano de Desarrollo; Organización de los Estados Americanos. 2020. Banco Interamericano de Desarrollo. *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe.* [En línea] 16 de julio de 2020. https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Divulgación Responsable por la falta de cooperación al compartir información de las vulnerabilidades descubiertas.

En el caso de Guatemala en junio del 2018, se crea la Estrategia de Seguridad Cibernética, donde se contemplan temas importantes referente al establecimiento y creación de un Comité Nacional de Seguridad Cibernética, así como también el comité Técnico. El primer comité, de seguridad cibernética se establece con la intención de favorecer e incentivar los espacios de coordinación de políticas interinstitucionales y sectoriales, así como establecer esfuerzos para vincular planes estratégicos de visión compartida con el fin de alcanzar los objetivos de la Estrategia Nacional de Seguridad Cibernética.

La creación de dicho comité se pudo realizar hasta octubre del año 2021, por medio de un Acuerdo Gubernativo 200-2021[41] en el cual la Secretaría Técnica del Consejo Nacional de Seguridad consolido la creación del mismo, llegándolo a llamar CONCIBER. Sin duda alguna esto representa un gran avance y una gran oportunidad para que se empiecen a establecer y formular las bases de las políticas junto a un marco normativo de las Infraestructuras Críticas y la Ciberseguridad, porque en base a los informes se deben establecer políticas y estrategias de seguridad cibernética, así como también Marcos Legales de Regulación, ya que por esa parte no existe avance alguno. Ya que según el reporte del BID junto a la OEA hacen ver que la ciberseguridad en Guatemala no ha ganado presencia en la agenda política cosa que es muy cierto, si bien se identifica el peligro y se hace ver la problemática, no se llegan a tomar medidas contra las ciberamenazas que no solo afectan a la economía del país sino también al mismo funcionamiento del propio gobierno, en el aspecto de seguridad, libertad y democracia.

Por lo que, conociendo el escenario actual, y las repercusiones que esto puede significar para Guatemala y la región Centroamericana, es importante que se tomen acciones adecuadas que establezcan las bases legales para que se aborden estos temas y no se quede en una mera intención o reconocimiento político.

[41] Secretaría Tecnica del Consejo Nacional de Seguridad . 2021. Secretaría Tecnica del Consejo Nacional de Seguridad . *COMITÉ NACIONAL DE SEGURIDAD CIBERNÉTICA.* [En línea] 29 de octubre de 2021. https://stcns.gob.gt/comite-nacional-de-seguridad-cibernetica/.

3.3.2 Aspectos para tener en cuenta del escenario guatemalteco

- En el apartado de estrategia nacional:
    - Guatemala publicó en 2018 su estrategia nacional de seguridad cibernética, pero pese a que existe dicha estrategia nacional, aún no se ha desarrollado un plan con componentes que determine la gestión de incidentes y respuesta cibernética; y esto a pesar de que en el país exista una Ley Marco de Seguridad Nacional, las organizaciones encargadas aún no han determinado una entidad global que se encargue de la coordinación de ciberseguridad, por lo que ante la falta, los contenidos así como la seguridad cibernética se llega a manejar de forma independiente en todos los sectores del país, y a como mejor llegue a pensar el personal encargado.

- En el apartado de cultura, sociedad y mentalidad de seguridad cibernética
    - A raíz de un aumento en ciberataques contra la estructura del gobierno en los últimos años, las entidades de Guatemala han puesto en marcha una serie de medidas para proteger los activos nacionales, aunque con una poca comunicación formal al respecto. Ahora por otra parte los Operadores de Infraestructuras Críticas han desplegado medidas de seguridad acordes con la Norma ISO27000 junto a otras normas Internacionales, aunque por esta parte la Infraestructura tecnológica con regularidad suele delegar a un tercero donde el gobierno llega a tener poco control sino es que un mínimo como tal.

- En el apartado de Marcos Legales
    - La legislación enfocada a la seguridad de las tecnologías de la información y comunicación, infraestructuras crítica y ciberseguridad aún es deficiente porque no existe, los esfuerzos para llamar la atención sobre esta necesidad de crear un Marco normativo jurídico sobre la ciberseguridad se han quedado en meras intenciones sin mucho esfuerzo, salvo la iniciativa de ley de ciberdelincuencia que si ha tenido ligeros avances.

- En el apartado tecnológico
    - En la adhesión de normas y prácticas mínimas, se adolece de un esfuerzo para aplicar a nivel nacional una adopción de prácticas para la seguridad de la información. Por lo que resurge el tema de la no existencia de un centro de mando para el control y coordinación a nivel nacional para la ciberseguridad, ya que la capacidad de incidentes no es coordinada generando así que se lleven de manera ad-hoc.

      La resiliencia nacional del gobierno debe mejorar el control de la Infraestructura Tecnológica, porque las redes y sistemas llegan a ser delegados a terceros, abriendo la puerta a mercados poco confiables que posibilitan una dependencia de otros países en tecnologías de ciberseguridad.

- En el apartado de Infraestructuras Críticas Nacionales (ICN).
    - En cuanto respecta a la identificación de las ICN, se entiende poco de los activos y las vulnerabilidades por la falta de una categorización formal. En cuanto a la organización, llega a existir meras interacciones que son básicas entre los ministerios gubernamentales y los propietarios de los operadores críticos, pero no existe un mecanismo que garantice o promueva una colaboración formal, por lo que en la planeación, de lo que respecta a la coordinación se carece de los parámetros adecuados para garantizar una respuesta efectiva, ya que la sensibilización de amenazas existe por los operadores de las ICN de forma aislada, pero la gestión de riesgos se maneja por cuenta de ellos bajo la línea de ciberseguridad y protección de datos que mejor consideren.

Las necesidades son más que claras a la hora de realizar el análisis del escenario de Guatemala, por medio de la Estrategia Nacional de Seguridad Cibernética e informes específicos, por lo que a la vista de lo estudiado, es necesario referirse al gobierno tanto como a las distintas instituciones y hacerles ver la responsabilidad que poseen junto al deber de establecer políticas y normas para proporcionar ciberseguridad para el ámbito interno, así como para el ámbito externo en el área regional.

3.3.3 Informe del Análisis

Una vez culminado el estudio y análisis de la legislación vigente, referente a la gestión de la Protección de las Infraestructuras Críticas en España, se pudo conocer las bases, estructuras, hoja de ruta y orientación que España fue abordando con el paso de los años, con la finalidad de llegar a tener un nivel de coordinación y protección enfocado a garantizar la funcionalidad, continuidad e integridad de las infraestructuras críticas; para lo cual, el establecimiento de un marco legal claro y preciso fue fundamental, ya que por medio de él, se pudo integrar la protección de dichas infraestructuras al corazón de las políticas publicas de seguridad, permitiendo así que con el paso de los años el enfoque siguiera adelante, porque gracias a las bases se pudo crear un sistema robusto orientado por la Ley 8/2011, y un Real Decreto 704/2011, que sirvió como punto de partida y que a día de hoy sigue respaldando la gestión de la protección.

Ahora bien, por otro lado, y al mismo tiempo. Se realizó el estudio y análisis del escenario actual de Guatemala, referente al mismo tema, con el objetivo de conocer cómo se encuentra actualmente con su marco legal. A lo que, en aras del estudio, de Guatemala se pudo conocer la existencia de una Ley Marco que viene a ser un poco básica, comparada con las leyes en España. Esta ley del año 2008 establece una base para que se pueda desarrollar una ley enfocada a la Protección de las Infraestructuras Críticas. Por parte de Guatemala, los esfuerzos para llevar a cabo el desarrollo de esta ley han sido paulatinos, debido a que los cambios de gobierno junto al gabinete y agenda política han llegado a retrasar enfoques que se tenían de años anteriores, generando con esto que los esfuerzos se vayan perdiendo, así como también que los riesgos aumenten por una falta de control y coordinación. A la vista de todo este escenario la Agenda de Seguridad Nacional junto con la Estrategia de Seguridad Cibernética, en el año 2018 por medio del Consejo Nacional de Seguridad, propone la creación del Comité Nacional de Seguridad Cibernética en el marco del Sistema Nacional de Seguridad, del cual su creación se consolida hasta en octubre del año 2021. Con la creación de este comité Guatemala tiene una oportunidad clave para que se pueda proponer el desarrollo, de un marco legal específico, en materia de Gestión y Protección de las Infraestructuras Críticas, y menciono la palabra clave debido a que este comité se crea con una duración de cuatro años, por lo que las propuestas por parte del sector público profesional serán tomadas en cuenta. Por lo que, llega a existir una oportunidad para fomentar una correcta aplicación de un marco normativo haciendo que esto no se quede como una mera intención.

CONCLUSIONES

Siguiendo los objetivos trazados al inicio de este trabajo como referencia y con los puntos anteriores abordados, donde se analizó el marco legal de gestión y protección de las infraestructuras críticas en España; y junto a ello también el análisis del escenario actual de Guatemala referente al mismo tema; formulo las siguientes conclusiones:

Primero: Para entender lo que representa el concepto de infraestructura crítica en España, se debe de estudiar a profundidad, como se estructura la Ley 8/2011. Parte del objetivo principal de este trabajo se enfoca en estudiar cómo se compone el marco legal de las infraestructuras críticas, así como el de entender sus razones y sus objetivos. con lo que, en base a lo estudiado, se determina que la construcción de normas y políticas enfocadas a la protección de las infraestructuras críticas se produce como consecuencia de una toma de conciencia del gobierno Español, ante las vulnerabilidades y amenazas latentes. Por consecuencia, en el caso preciso de Guatemala, es determinante que se enfoquen los esfuerzos para el desarrollo de normativa en aras de asegurar la confidencialidad, continuidad, funcionalidad, e integridad de las infraestructuras críticas, como en el caso de España.

Segundo: El avance de la tecnología hoy en día, representa sin lugar a duda, un beneficio para todos los sectores de la sociedad, gracias a ella la optimización de procesos permite cada vez más la digitalización de servicios, y conforme la tecnología avance las áreas productivas irán integrando cada vez más tecnologías, basadas en arquitecturas comunes tales como las redes, programas específicos y arquitectura de sistemas. Con lo que la ciberseguridad se debe de volver un tema prioritario en el marco de gobernanza de cada industria del sector. En España por medio de la Directiva NIS, y con lo que propone la Directiva NIS II, se establecen requisitos mínimos comunes en materia de seguridad para los operadores de servicios esenciales; los proveedores de servicios digitales; y los prestadores de servicios esenciales establecidos en la Ley 8/2011. La ciberseguridad es un aspecto que no se debe de descuidad y mas ahora con la nueva era del ciberterrorismo.

Tercero: La Organización Internacional de Normalización –ISO– desempeña un papel importante en la ciberseguridad y gestión de la información de las empresas, industrias y países, debido a que presenta directrices sobre cómo administrar y relacionar la gestión de la seguridad, con las distintas tecnologías que integran funciones específicas dentro de la empresa o industria. En este trabajo se estudiaron las normas ISO 27005, 27032 y 31000, de estas normas se analizaron las características principales y enfoques primordiales y se pudo determinar, que la incorporación de estas normas a la estrategia de la empresa favorece en la eficacia de la gestión de riesgos, y cuidado de la información. En España si bien se cuenta con la certificación del esquema nacional de seguridad –ENS– el uso de las normas –ISO– serían meramente de apoyo, trayendo consigo un beneficio de imagen, seguridad y mayor confianza, aunque con el –ENS– estos beneficios también se tienen. Ahora bien, para el caso de Guatemala al no tener una certificación nacional como el esquema. El uso de las normas ISO es más que necesario y recomendado.

Cuarta: El Estudio y análisis de la Ley 8/2011, sirvió para entender cómo se llega a desarrollar dicha ley, si bien, es sabido de que proviene de la Directiva Europea 114/2008/CE, el propósito del estudio y análisis en sí, fue el poder conocer sus bases fundamentales, En el estudio se pudo encontrar de que, en España, antes de que se creara esta ley, no existía ninguna norma que regulara de manera específica la protección de las infraestructuras críticas, aunque lo que si existía era un conjunto de normas sectoriales, en ellas no se daba el enfoque como se le da en la ley PIC, donde hasta el 2 de noviembre del 2007 bajo la línea del Consejo de Ministros se aprobó un acuerdo de protección de las infraestructuras críticas, lo que constituyó en ese factor fundamental determinante, ya que por medio de ese acuerdo es como se crea el CNPIC, órgano que con el apoyo del la Secretaría General Técnica del Ministerio de Interior realiza los trabajos correspondientes a trasponer la Directiva previamente mencionada. Determinando así que el órgano fundamental para la elaboración del a ley PIC fue el CNPIC, donde las bases para su transposición radicaron en establecer una cooperación público-privada, consolidar el Catálogo Nacional de Infraestructuras Críticas, establecer los canales de comunicación adecuados y diseñar planteamientos que contuvieran medidas de prevención y protección.

Quinta: Analizando el escenario de Guatemala se pudo determinar que el uso de la tecnología en Guatemala, así como el creciente acceso y uso de servicios en internet, juegan un papel transformador cada vez más significativo en todos los sectores económicos, sociales y servicios del país, debido a que estas herramientas digitales, así como para el resto de países, se han convertido en un factor clave para la sociedad, empresas, industria y gobierno, por lo que en ese sentido, la existencia de amenazas ponen en riesgo la funcionalidad de los servicios y operabilidad del país, al no saber como hacerles frente. Por lo que es esencial que se encaminen esfuerzos para la elaboración de un marco enfocado a la seguridad y protección de infraestructuras. Para ello y en base al estudio, en Guatemala en octubre del 2021 se creó el Comité Nacional de Seguridad Cibernética (CONCIBER), con un plazo de cuatro años. A la vista de lo que acontece en el escenario actual, y con la creciente ola de ciberataques que está empezando a experimentar la región, el CONCIBER tiene la capacidad de encaminar esfuerzos, y desarrollar políticas que permitan establecer un marco legal para la gestión de futuros incidentes, teniendo como base el análisis de la Ley 8/2011 de España, y sabiendo como se desarrolló la misma por medio del estudio; en Guatemala se debe utilizar la Ley Marco del Sistema Nacional de Seguridad para extender el plazo de duración del CONCIBER, y así evitar planteamientos fragmentarios que obstaculicen la coordinación interinstitucional, por medio de una visión integral y coherente en base a al artículo 10 de la Ley Marco, donde se establecen las competencias del Consejo Nacional de Seguridad. Eso, por un lado, por otro lado, teniendo la posibilidad de establecer políticas por medio del CONCIBER, lo primordial es establecer una cooperación público-privada para conformar e identificar un catálogo nacional de infraestructuras críticas donde se planifiquen las actuaciones necesarias en materia de seguridad y protección de las mismas.

BIBLIOGRAFÍA

262/STTF, Grupo ISO/TC. 2018. ISO - Online Browsing Platform (OBP). *ISO 31000:2018(es) Gestión del riesgo - Directrices.* [En línea] 1 de Febero de 2018. [Citado el: 25 de Abril de 2022.] https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es.

Banco Interamericano de Desarrollo; Organización de los Estados Americanos. 2020. Banco Interamericano de Desarrollo. *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe.* [En línea] 16 de julio de 2020. https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe.

Comisión Europea. 2016. Diario Oficial de la Unión Europea . *DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO.* [En línea] 6 de julio de 2016. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148&from=ES.

Consejo de Gobierno. 2018. Boletín Oficial del Estado . *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y.* [En línea] 8 de septiembre de 2018. https://www.boe.es/boe/dias/2018/09/08/pdfs/BOE-A-2018-12257.pdf.

Consejo Nacional de Seguridad -CAP-. 2020. Secretaría Técnica del Consejo Nacional de Seguridad República de Guatemala. *ESTRATÉGICA DE SEGURIDAD DE LA NACIÓN 2020 - 2024.* [En línea] 5 de Abril de 2020. https://stcns.gob.gt/wp-content/uploads/2022/05/Agenda-Estrategica-de-Seguridad-de-la-Nacon-2020-2024.pdf.

Dirección Legislativa . 2019. Congreso de la Republica de Guatemala. *Iniciativa que dipone aprobar ley de prevención y protección contra la ciberdelincuencia.* [En línea] 6 de agosto de 2019. https://www.congreso.gob.gt/detalle_pdf/iniciativas/5601.

DSN, Sala de prensa del. 2021. Departamento de Seguridad Ncional. *España, a la Cabea mundial en Ciberseguridad.* [En línea] 01 de Julio de 2021. [Citado el: 04 de Abril de 2022.] https://www.dsn.gob.es/es/actualidad/sala-prensa/espa%C3%B1a-cabeza-mundial-ciberseguridad.

Equipo CCN-CERT. 2022. CCN-CERT SEGURIDAD AL DIÁ . *La Unión Europea refuerza su ciberseguridad y resiliencia con la aprobación de la directiva NIS 2.* [En línea] 25 de mayo de 2022. [Citado el: 25 de mayo de 2022.] https://www.ccn-cert.cni.es/seguridad-al-dia/actualidad-ccn/11799-la-union-europea-refuerza-su-ciberseguridad-y-resiliencia-con-la-aprobacion-de-la-directiva-nis-2.html.

Europeo, Consejo. 2008. Agencia Estatal Boletín Oficial del Estado . *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.* [En línea] 08 de diciembre de 2008. https://www.boe.es/doue/2008/345/L00075-00082.pdf.

Gobernación, Ministerio de. 2018. Ministerio de Gobernación . *Estrategia Nacional de Seguridad Cibernetica* . [En línea] 20 de Enero de 2018. [Citado el: 15 de Abril de 2022.] https://uip.mingob.gob.gt/wp-content/uploads/2019/03/Estrategia-Nacional-de-Seguridad-Cibern%C3%A9tica.pdf.

Guatemala, Congreso de la República de. 2008. Ministerio de Gobernació. *Ley Marco del Sistema Nacional de Seguridad.* [En línea] 2008. [Citado el: 5 de Abril de 2022.] https://mingob.gob.gt/wp-content/uploads/2020/10/8.2-LEY-MARCO-DEL-SISTEMA-NACIONAL-DE-SEGURIDAD.pdf.

INCIBE. 2020. INCIBE CERT. *GUÍA NACIONAL DE NOTIFICACIÓN Y.* [En línea] 21 de febrero de 2020. [Citado el: 1 de Junio de 2022.] https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf.

Jefatura del Estado . 2011. Agencia Estatal Boletín Oficial del Estado . *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la.* [En línea] 29 de abril de 2011. https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf.

LISA institute. 2019. LISA institute. *Infraestructuras críticas: definición, planes, riesgos, amenazas y legislación.* [En línea] 28 de octubre de 2019. https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas.

Logitek. 2014. Industrial Cybersecurity by Logitek. *Seguridad IT versus Ciberseguridad Industrial.* [En línea] 2014. [Citado el: 2 de abril de 2022.] https://www.ciberseguridadlogitek.com/seguridad-it-versus-ciberseguridad-industrial/.

Ministerio del Interior. 2011. Agencia Estatal Boletín Oficial del Estado. *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.* [En línea] 20 de mayo de 2011. https://www.boe.es/buscar/pdf/2011/BOE-A-2011-8849-consolidado.pdf.

Nacional, Centro Criptológico. 2012. CCN-CERT Noticas actuales. *Norma ISO/IEC 27032, nuevo estándar de ciberseguridad.* [En línea] 17 de octubre de 2012. [Citado el: 24 de Abril de 2022.] https://www.ccn-cert.cni.es/gl/gestion-de-incidentes/lucia/23-noticias/297-publicada-isoiec-27013.html#:~:text=M%C3%A1s%20concretamente%2C%20ISO%2FIEC%2027032,personas%20en%20todo%20el%20mundo..

Secretaría Tecnica del Consejo Nacional de Seguridad . 2021. Secretaría Tecnica del Consejo Nacional de Seguridad . *COMITÉ NACIONAL DE SEGURIDAD CIBERNÉTICA.* [En línea] 29 de octubre de 2021. https://stcns.gob.gt/comite-nacional-de-seguridad-cibernetica/.

Seguridad, Secretaria de Estado de. 2017. Ministerio del Interior. *Dosier de Alerta Antiterrrorista.* [En línea] 2017. https://www.interior.gob.es/opencms/pdf/prensa/nivel-de-alerta-antiterrorista/descargas/Dossier_NAA.pdf.

Sevillano, Fernando . 2021. *Ciberseguridad Industrial e Infraestructuras Críticas.* España : RA-MA, 2021. ISBN: 978-84-1855-136-9.

Technology, Department of Information Security and Communication. 2017. The Institute of Electrical and Electronic Engineers. *A framework for the information classification in ISO 27005 standard.* [En línea] 6 de febrero de 2017. [Citado el: 20 de Abril de 2022.] https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7987208.

Universida de Cantabria. 2015. Grupo Unican. *Fases de una investigación.* [En línea] 04 de Abril de 2015. [Citado el: 24 de Marzo de 2022.] https://grupos.unican.es/mide/masterinnova/materiales/Fases%20investigacion.pdf.

Vanaclocha, Francisco J. 2013. *MARCO LEGAL Y DE GESTIÓN DE LA PROTECCION DE LAS INFRAESTRUCTURAS CRÍTICAS* . Madrid : McGRAW-HILLI INTERAMERICANA DE ESPAÑA , 2013. 978-84-481-8593-0.

Velamanzán, Laura. 2021. QuestionPro. *Entre datos ¿Que es la Investigación Cualitativa?* [En línea] 2021. [Citado el: 24 de Marzo de 2022.] https://www.questionpro.com/es/investigacion-cualitativa.html#:~:text=La%20investigaci%C3%B3n%20cualitativa%20tiene%20como,de%20investigaci%C3%B3n%20flexible%20e%20interactiva..

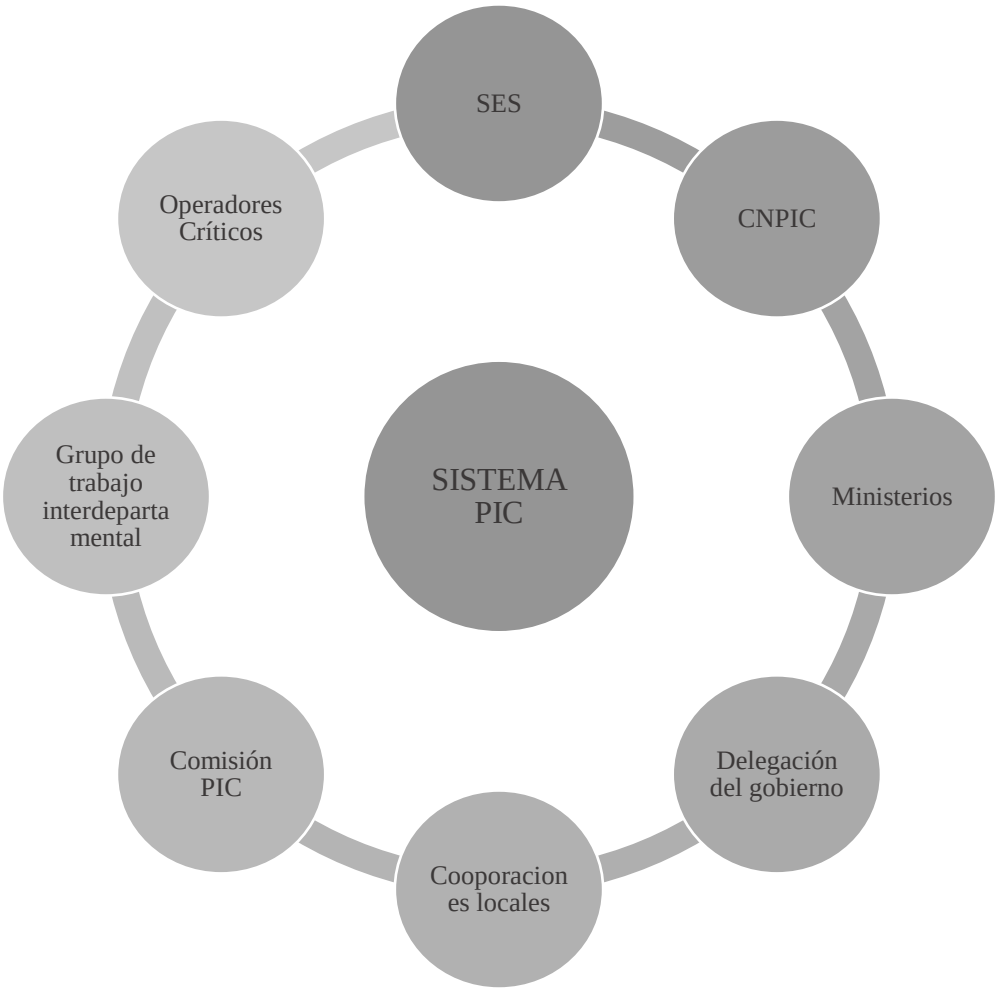
ANEXOS

Anexo 1. Tabla general de Impacto

Categoría	Clasificación de la infraestructura	Daños a las personas	Impacto económico y/o medioambiental	Incidencia sobre el servicio
5	CRÍTICA	MUY GRAVE – pérdida de vidas y/o daños a la salud (>X víctimas mortales y/	MUY GRAVES daños sobre la economía nacional de X millones de euros (>millones)	Pérdida o interrupción MUY GRAVE de los servicios básicos a la población
4		GRAVE – pérdida de vidas y/o daños a la salud (>víctimas mortales y/o heridos)	GRAVES daños en la economía nacional, de millones de euros (>millones)	Pérdida o interrupción GRAVE de los servicios básicos a la población
3	ESENCIAL	MUY IMPORTANTES pérdidas de vidas y/o daños a la salud (>víctimas mortales y/o heridos)	DAÑOS MUY IMPORTANTES sobre la economía nacional de millones de euros (>millones)	Perdida o interrupción MUY IMPORTANTE de los servicios básicos a la población
2		IMPORTANTE pérdida de vidas y/o daños a la salud (>víctimas mortales y/o heridos)	DAÑOS IMPORTANTES sobre la economía nacional, de más de millones de euros (>millones)	Pérdida o interrupción IMPORATE de los servicios básicos a la población
1	COMPLEMENTARIA	MODERADA pérdida de vidas y/o (>víctimas mortales y/o heridos)	DAÑOS MODERADOS sobre la economía nacional, de más de millones de euros (>millones)	Perdida o interrupción MODERADA de los servicios básicos a la población
0	NO SE CONSIDERA	NULA pérdida de vidas y/o daños a la salud.	DAÑOS ESCASOS sobre la economía nacional, de hasta millones de euros (>millones)	Perdida o interrupción ESCASA de los servicios básicos a la población

Categoría	Clasificación de la infraestructura	Daños a las personas
5	CRÍTICA	Falta o interrupción Muy Grave del suministro de ……. >X de persona y duran más de Y días o bien Fatal de suministro que afecte a la mayor parte del país – Varias CC. AA – durante cualquier periodo de tiempo
4		Falta o interrupción GRAVE del suministro de ……. > X de personas y durante más de Z horas
3	ESENCIAL	Falta o interrupción MUY IMPORTANTE del suministro de …… > de personas y durante más de horas
2		Falta o interrupción IMPORTANTE del suministro …… >de personas durante más de horas
1	COMPLEMENTARIA	Falta o interrupción MODERADA del suministro de …… >de personas y durante más de horas
0	NO SE CONSIDERA	Pérdida o interrupción ESCASA de los servicios Básicos a la población <de personas y durante más 0de horas

Anexo 3. Figura de composición del sistema PIC español.



GLOSARIO

Antivirus: tipo de software que se utiliza para evitar, buscar, detectar y eliminar virus de un ordenador.

Análisis de Riesgo: el estudio de las hipótesis de amenazas posibles necesario para determinar y evaluar las vulnerabilidades existentes en los diferentes sectores estratégicos y las posibles repercusiones de la perturbación o destrucción de las infraestructuras que le dan apoyo.

Ciberamenazas: cualquier conducta dolosa de individuos u organizaciones, conocidos o no, desarrollada a través del ciberespacio contra sistemas de información, con el propósito de sustraer, alterar, abusar, desestabilizar, inutilizar, destruir o eliminar activos.

Ciberataques: amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste.

Cibercrimen: Delito cometido mediante el uso de técnicas, métodos y aparatos informáticos a través de internet o redes virtuales.

Ciberespacio: dominio global y dinámico compuesto por infraestructuras de tecnología de la información -incluyendo internet-, redes de telecomunicaciones y sistemas de información que configura un ámbito virtual.

Ciberespionaje: Práctica que se ejecuta con el fin de obtener secretos sin el permiso del poseedor, se emplean tecnologías de la información y la comunicación por parte de personas o empresas para obtener algún beneficio económico o personal.

Ciberseguridad: capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

Ciberterrorismo: forma de terrorismo por la que grupos emplean medios informáticos para atacar, ordenadores, empresas e infraestructura entre otros con el objetivo de intimidar o coaccionar a un gobierno o población.

Gestión de Incidentes: procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante éste.

Gestión de Riesgos: actividades coordinadas para dirigir y controlar a una organización con respecto a los riesgos.

Hackers: Persona con grandes conocimientos de informática que se dedica a detectar fallos de seguridad en sistemas informáticos.

Incidente: suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información.

Industria 4.0: revolución industrial que llega a tener su enfoque en gran medida por la interconectividad, la automatización, el aprendizaje automatizado y los datos en tiempo real.

Infraestructura Crítica: las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

Infraestructura Crítica Europea: aquellas infraestructuras críticas situadas en algún Estado miembro de la Unión Europea, cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros.

Infraestructura Estratégica: las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.

Interdependencia: los efectos que una perturbación en el funcionamiento de la instalación o servicio produciría en otras instalaciones o servicios, distinguiéndose las repercusiones en el propio sector y en otros sectores, y las repercusiones de ámbito local, autonómico, nacional o internacional.

Malware: Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial.

Operadores Críticos: las entidades u organismos responsables de las inversiones o del funcionamiento diario de una instalación, red, sistema, o equipo físico o de tecnología de la información designada como infraestructura crítica.

Operadores de Servicios Esenciales: organización pública o privada que presta un servicio necesario para el mantenimiento de las funciones sociales básicas tales como la salud, la seguridad, el bienestar social y económico de los ciudadanos.

Parches: Los parches son recursos de tecnología informática que ayudan a corregir ciertos errores.

Proveedor de Servicios Digitales: Persona jurídica que presta un servicio de la sociedad de la información.

Sectores Estratégicos: cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva, que proporciona un servicio esencial o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país.

Servicio Esencial: el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

Sistemas de Información: conjunto de componentes interrelacionados para trabajar, recopilar, almacenar, difundir y procesar información.

Soft law: Conjunto de normas que sin tener fuerza vinculante obligatoria contienen las pautas inspiradoras de una futura regulación de una materia, abriendo paso a un posterior proceso de formación normativa.

Subsector estratégico: cada uno de los ámbitos en los que se dividen los distintos sectores estratégicos, conforme a la distribución que contenga, a propuesta de los Ministerios y organismos afectados, el documento técnico que se apruebe por el Centro Nacional de Protección de las Infraestructuras Críticas.

Tecnologías de la Información IT: Plataforma de tecnologías que logra realizar la comunicación de usuarios, servicios, dispositivos y aplicaciones.

Tecnologías de la operación OT: Se fundamenta en la operación del perfeccionamiento, para la obtención de un mismo resultado de una forma más eficiente y eficaz.