Universidad de Buenos Aires
Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final de Especialización

Tema: Infraestructuras Críticas

Título: El Quinto Dominio Sobre Infraestructuras Criticas

Autor: Simón ROBERTS

Tutor: Darío RIZZO

Cohorte: 2021

Presentación: 2022

Declaración jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO
Ricardo Simón ROBERTS
D.N.I. 24.589.091

Índice de Contenido

Índice de Figuras

ALCANCE

En estos últimos años la tecnología avanza vertiginosamente y en plena era del conocimiento, la información y los sistemas han tomado una importancia crítica para las naciones. Por ello es necesario que todos los países y sus fuerzas armadas sean conscientes de esta nueva forma de guerra, la denominada “Guerra Cibernética” o “Quinto Dominio”, así como las maneras de defenderse y la importancia de identificar la infraestructura critica relacionada a la mayoría de servicios esenciales de infraestructuras de gestión pública y privada; son consideradas críticas porque la interrupción o perturbación severa de su funcionamiento, ocasionaría graves efectos sobre el normal desarrollo de las actividades básicas de la sociedad.

El presente trabajo de investigación tiene como objeto describir las características de las Infraestructuras Críticas, contemplando las múltiples amenazas a las cuales está expuesta, su implicancia y cómo podemos defendernos y responder, con actividades de formación, entrenamiento, concienciación y adiestramiento.

También contempla un estudio de cómo este tema es considerado en otros países y el marco normativo argentino que las contempla.

INTRODUCCIÓN

Los avances en la tecnología digital han revolucionado completamente la forma en que las personas, las empresas y los estados interactúan. La prestación de servicios gubernamentales, así como el flujo general de bienes y servicios, se han transformado debido a la mayor conectividad a Internet y al advenimiento del comercio electrónico y las transacciones electrónicas. Sin embargo, las nuevas tecnologías traen consigo desafíos y amenazas propias.

La adopción de nuevas tecnologías digitales permite una gestión más eficiente de las Infraestructuras Críticas en términos de escala, distancia y tiempo, pero también introduce nuevas vulnerabilidades que hacen que la protección de las Infraestructuras Críticas de información sea una tarea importante y desafiante. La protección de los activos y sistemas de información que respaldan y forman infraestructuras críticas, es decir, las Infraestructuras de Información Críticas (CII) se ha convertido en una

preocupación importante para las políticas de seguridad nacional a medida que se adoptan nuevas tecnologías. La Protección de Infraestructuras Críticas de Información (CIIP) se puede definir como todas las actividades destinadas a garantizar la funcionalidad, continuidad e integridad de las CII para disuadir, mitigar y neutralizar una amenaza, riesgo o vulnerabilidad o minimizar el impacto de un incidente.

Si bien las Infraestructuras Críticas (CI) y las Infraestructuras de Información Críticas (CII) están interrelacionadas y ambas son cruciales para el buen funcionamiento de una sociedad y su seguridad, estos conceptos no se pueden utilizar indistintamente y requieren diferentes métodos de gestión, control y protección. A pesar que existen varias definiciones de infraestructura crítica, y las naciones difieren en qué sectores se incluyen en la clasificación, las infraestructuras comúnmente críticas se consideran aquellas infraestructuras que son esenciales para el mantenimiento de las funciones vitales de la sociedad, la salud, la seguridad, el bienestar económico o social de las personas y la interrupción o destrucción de las mismas presentaría graves consecuencias. Por lo tanto, la protección continua y la gestión de riesgos de esas infraestructuras son cruciales para su resiliencia y la seguridad de cada nación.

Las tecnologías digitales son cada vez más adoptadas para la gestión, el mantenimiento, el control y la protección de infraestructuras críticas, por ejemplo, con Sistemas de Control Industrial (ICS), o se utilizan como infraestructura en sí, como los servicios de telecomunicaciones o los puntos de intercambio de tráfico de Internet. Estas se denominan CII y comúnmente son definidas como Redes de Tecnologías de la Información y la Comunicación (TIC) y datos que respaldan, vinculan y permiten operaciones de infraestructuras críticas, y cuya interrupción, destrucción o explotación podría tener un impacto debilitante.

Finalmente, los planetas de Tecnología de Operación (TO) y de Tecnología Informática (TI) están cada vez más cerca uno del otro, lo cual requiere redoblar los esfuerzos y tender puentes para lograr de una vez la tan necesaria convergencia que nos permita proteger adecuadamente las CI.

PROBLEMÁTICA GENERAL

Infraestructuras Críticas

Se define como Infraestructura Critica (CI) de un país a los sistemas, tanto digitales como físicos, que brindan servicios esenciales para la sociedad y que en caso de ser afectados por un ciberataque podrían tener un impacto grave que afecte a la seguridad, economía, política, energía, salud, comunicaciones o transporte, entre otros. El sector de la salud, por ejemplo, ha sido un blanco de ataque recurrente en los últimos años. Durante la pandemia (2019) se atacaron hospitales u organismos de este sector, —como fue el ataque del *ransomware Conti* al sistema de salud público de Irlanda, entre otros tantos ataques a la salud—, muchas de estas organizaciones vieron socavada la posibilidad de brindar la debida atención a sus pacientes y se necesitaron semanas o meses en algunos casos para que su infraestructura tecnológica vuelva a operar en su totalidad. [9]

La Infraestructura Crítica de Información (CII) se refiere a la infraestructura de comunicaciones e información, pilar de la CI, que incluye tanto el sistema interno de información y comunicación utilizado en un sector en particular de CI. Si bien la definición de CII puede llegar a variar según el país, es parte fundamental de las políticas asociadas a una Ciberestrategia de Seguridad Nacional (CS); dado que están en el centro de esta y, por tanto, el cómo se construye este concepto y se definen las áreas que serán consideradas, tienen una importancia nacional. [9]

Identificación

Son amplios los desafíos en cuanto a CI, en primer lugar, definir y distinguir qué se entenderá por CI y CII, e identificar las dependencias entre CI y servicios, especialmente en los denominados puntos de falla. Esta identificación debe considerar las dependencias y tipos de usuarios afectados.

Al considerar una industria, empresa u organización, como crítica, tendrá impacto en cómo se relaciona con la sociedad. Este componente social y técnico, muestra que la CI debe ser tratado como un objeto Socio técnico. Es decir, objetos o procesos que requieren tanto de explicaciones sociales como técnicas, sin la imposición de una sobre

la otra, para comprender su conformación, estabilización o funcionamiento. En el siguiente cuadro se presenta una comparación con las definiciones de sectores de CI para 4 países [3]:

Sector	Chile	UK	EEUU	España	Colombia
Energía	X	X	X	X	X
Telecomunicaciones	X	X	X	X	X
Agua	X	X	X (y residuales)	X	X
Salud	X	X	X	X	X

Sector	Chile	UK	EEUU	España	Colombia
Servicios Financieros	X	X	X	X	X
Seguridad Pública	X	X		X	X
Transporte	X	X	X	X	X
Administración Pública	X	X	X	X	X
Protección civil	X				
Defensa	X	X	X	X	X
Alimentos			X (y Agricultura)	X	X (y Agricultura)
Espacio		X		X	
Nucleares		X	X (y Residuos)	X	
Químico		X	X	X	
Instalaciones Comerciales			X		
Crítico de Fabricación			X		X (Industrial, Comercio y Turismo)
Represas			X		
Tecnología de la Información			X		
Instalaciones de Investigación				X	
Educación					X
Minero - Energético					X
Ambiente					X
Servicios de Emergencia		X	X		

Figura 1 – Sectores de Infraestructura Critica [3]

Asimismo, La Agencia de Ciberseguridad e Infraestructura de los Estados Unidos (CISA) clasifica a los sistemas críticos de un país en 16 sectores de vital importancia.

Figura 2 – Infraestructura Criticas de un país, según CISA [9]

Una infraestructura requiere de tres elementos que interactúen entre sí para que el sistema funcione como un todo: un medio de comunicación, una fuente de energía y un mecanismo de logística. Así, se puede incluir sectores industriales como las telecomunicaciones, medios de comunicación o repetición (antenas) e industrias de transporte (por ejemplo, ferrocarriles o infraestructura de caminos). Luego, se hace necesario incluir los centros de cómputos (*data centers*), lugares donde se custodia la infraestructura tecnológica. Otro punto a considerar es, el concepto de bien privado/público ya que, por ejemplo EE.UU. establece el sector de Instalaciones comerciales como CI dado que las grandes tiendas comerciales pueden ser utilizadas como refugios o bodegas para obtener insumos de primera necesidad.

Es por ello que una Infraestructura Critica (CI) es aquella que su incapacitación o destrucción tendría un efecto debilitante en la seguridad, la económica nacional, la salud pública, o cualquier combinación de estos.

Relevancias para las Industrias

Las infraestructuras críticas en su mayoría están interconectadas con otras; es decir, que si una infraestructura es afectada por una amenaza es probable que la misma pueda propagarse hacia otras. Es por ello que se observan convenios entre gobiernos para capacitar y compartir conocimientos en ámbitos de CS y les permitan movilizar tecnologías (entendido para este caso una metodología) la cual no es automática ya que una tecnología exitosa no necesariamente tendrá el mismo resultado en otras localidades, las metodologías deben ser traducidas a las necesidades propias del país.

Un punto innovador, en algunos países, respecto a las metodologías observadas, es la clasificación de la CI en dos niveles de criticidad, donde las de nivel 1, de alta criticidad, deben mantener un conjunto de protocolos y procedimientos, para asegurar la confiabilidad de sus redes y servicios, la continuidad operacional e identificar la interdependencia de éstos con otros sectores que proveen servicios públicos y/o servicios básicos. Algunos utilizan el Modelo de Madures de UK, el cual señala 5 niveles de criticidad, desde un nivel con alto nivel de impacto (categoría 5), hasta un nivel bajo de impacto o interrupción del servicio. Para ello, se debe implementar una línea base de seguridad de la información, de CS y de gestión de riesgos, para ser adoptado en los sectores públicos y privados. Si bien estos son sólo ejemplos de los requerimientos a plantear en una industria o sector que sea considerado CI, estos requerimientos deben ser asociados al análisis de riesgos. Asimismo, es necesario incorporar a la opinión pública en la definición de estos requerimientos, para disminuir la incertidumbre y evitar la consolidación de asimetrías de poder. Si sólo deciden los expertos, no se considerarán todas las implicancias sociales, pudiendo las medidas ser insuficiente y no integrales. [3]

Relevancias para la Sociedad

Que una infraestructura crítica sea afectada por un ciberataque puede repercutir de forma directa en una sociedad y también en otras infraestructuras críticas. Si, por ejemplo, la infraestructura del sector abastecimiento de agua y saneamiento de una población es atacada, esto puede generar la falta de un recurso vital como es el agua y que va más allá del consumo personal de agua de la población. Por otra parte, se ha demostrado que los sistemas críticos son altamente vulnerables debido a que están conectados digitalmente para que sea más sencillo para los operadores controlar cualquier sistema critico (bancos, energía, trasporte, etc.). Es por ello que la definición de CI no puede dejar indiferente a la sociedad, ya que la elección de tecnologías (entendidas como tal, metodologías, conocimientos y/o artefactos) afectará la forma de relacionarnos y generará consecuencias políticas y sociales. Al disponer de niveles de criticidad, emergen requerimientos legales y organizacionales. Se puede identificar dos líneas reflejadas en esta política. La primera, en relación con la tecnología como un medio para alcanzar un fin. Por ejemplo, la elección entre código abierto y cerrado, lo que significará un impulso a ciertas industrias, que contribuye al desarrollo de una estrategia país; se genera una disyuntiva tecnológica con múltiples consecuencias. La segunda línea, en relación a que las tecnologías son inherentemente políticas,

compatibles con ciertos tipos de relaciones sociales, donde seleccionar tecnologías implica condiciones sociales y materiales. Como ejemplo, en Alemania las agencias reguladoras de CI, poseen facultades similares a la policía en ciertas áreas, han generado regulaciones técnicas para los operadores y fabricantes de tecnologías, quienes deben cumplir con estándares de seguridad industriales, regulaciones específicas de su sector y regulación asociada a CI. Así, por ejemplo, en Israel, surgió una controversia entre el sector financiero y las agencias de regulación en materia de CI, esto ya que en el desarrollo de los requerimientos no se habría considerado la opinión de la industria. En Chile, las asociaciones empresariales han tomado conciencia de la relación público-privado, es así como la Cámara Nacional de Comercio, creó la Alianza Chilena de CS, que considera dentro de sus objetivos cooperar con las autoridades para la definición e implementación de regulaciones. Estas alianzas público–privado. podrían generar configuraciones de límites (*boundary configuration*), las que compartirían un enfoque específico con definiciones y métodos propios, para generar elementos sociales y discursivos específicos. Estas tienden a excluir a actores o grupos disidentes y, si bien, dan la sensación de una gran experiencia para el desarrollo e implementación de la política pública, al excluir las voces disidentes pone en riesgo el éxito de esta implementación. [3]

Sectores Sensibles

La protección de las Infraestructuras Críticas es una preocupación de los Estados. El alto nivel de desarrollo de las sociedades actuales descansa en su mayor parte en una serie de servicios básicos y esenciales cuya prestación radica mayoritariamente en el sector privado. Nunca las infraestructuras han sido tan trascendentales para el normal funcionamiento de los servicios y de los principales sistemas de producción como lo son la administración, el agua, el sistema financiero y tributario, la energía, el espacio, la industria nuclear o el transporte, entre otros. Tal como mencionamos, aquellas instalaciones, redes, servicios y equipos cuya interrupción puede tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos, son las que entendemos como Infraestructuras Críticas. Garantizar la seguridad de los suministros de estos servicios básicos ante nuevas amenazas es una responsabilidad no sólo de las administraciones públicas, sino también de los operadores privados a nivel nacional e internacional. [6]

Características Técnicas

Las particularidades técnicas y la alta exposición de los datos que pueden ser robados, hacen que la protección de este tipo de redes sea especial. Estas nuevas intromisiones, dirigidas a los sistemas Ciberfísicos de los procesos industriales que se ejecutan en las Infraestructuras Críticas, hacen necesaria la adopción de nuevas estrategias capaces de detectarlos sin interferir en su funcionamiento normal. [6]

Figura 3 – Estrategias de Protección en Procesos Industriales [6]

Es relevante distinguir entre Tecnologías de Información (TI) y Tecnologías de Operación (TO), esta última asociada a procesos productivos o industriales, y que su arquitectura difiere y no posee los mismos procesos de actualización y de seguridad, lo que dificulta los requerimientos de seguridad para CI.

Amenazas, Vulnerabilidades y Riesgos

Conceptos Generales

Para comprender el problema general se deben definir una serie de conceptos fundamentales:

Amenazas: Se definen como aquellos elementos que son peligrosos al hombre y que están causados por fuerzas extrañas o no extrañas a él. [23]

Vulnerabilidades: Podríamos definirlas como el conjunto de condiciones y procesos que se generan por efecto de factores físicos, tecnológicos, sociales, económicos y ambientales que aumentan la posibilidad de que una persona, comunidad o instalación pueda ser susceptible de sufrir daños humanos y materiales frente al impacto de los peligros o amenazas. La magnitud de estos daños estará asociada con el grado de vulnerabilidad. Una forma resumida de definir también la vulnerabilidad puede ser la probabilidad de que, debido a la intensidad del evento y a la fragilidad de los elementos expuestos, ocurran daños en la economía, la vida humana y el ambiente. Este enfoque hacia la vulnerabilidad contempla factores físicos, sociales, políticos, tecnológicos, ideológicos, institucionales, culturales y educativos que, a su vez, se relacionan dentro de la propia realidad de la vulnerabilidad. [23]

En Tecnología Informática (TI), una vulnerabilidad se entiende como una debilidad o exposición derivada de fallas que pueden tener diversos orígenes. En general, se trata de errores o problemas documentados y disponibles al público en general, identificados mediante codificación normalizada como CVE, CWE, CVSS, etc. La explotación de una vulnerabilidad puede derivar en situaciones no deseadas: apagado de servidores, fuga de datos o eventos maliciosos varios. [18]

En Tecnología de Operación (TO), el aprovechamiento de una debilidad técnica tiene el potencial de afectar infraestructuras críticas y servicios esenciales. Ciertamente, existen planes de contingencia y operación manual como alternativas, aunque el avance de la digitalización y el automatismo suman complejidades e interdependencias en los sistemas. [18]

Riesgos: Podemos definir que es la probabilidad de que una amenaza se convierta en un desastre, con graves consecuencias económicas, sociales y ambientales. Los riesgos corresponden a un valor relativo probable de pérdidas de toda índole en un sitio específico vulnerable a una amenaza en particular, en el momento de la materialización de ésta y durante todo el período de recuperación y reconstrucción que le sigue. En este sentido existen distintos niveles de riesgo: Riesgo aceptable, razonable o factible. Consecuentemente, para la protección de las infraestructuras críticas, hay que desarrollar en profundidad los criterios para la evaluación de las amenazas por causas de la naturaleza, riesgos tecnológicos, antisociales y delictivos, e incluso, sociales y laborales. Todo ello, sin olvidar que las infraestructuras críticas son aquellas cuyo funcionamiento resulta indispensable y no permite soluciones alternativas, por lo que su destrucción o alteración tendría un grave impacto a consecuencia de estos tipos de riesgos y sus magnitudes o consecuencias. [23]

Problemática

El imparable desarrollo de las tecnologías de la información y la comunicación, y las nuevas oportunidades para cometer delitos mediante las mismas, representan una nueva amenaza para la Seguridad Nacional. Internet es un lugar accesible, fácil de usar y eficaz, del que cada vez dependemos en mayor medida para llevar a cabo un sinfín de actuaciones de nuestra vida cotidiana. Estas características hacen precisamente de la red, un lugar propicio para que para que los delincuentes salgan indemnes dadas las dificultades para rastrearlos a través de la red y localizarlos. Las principales modalidades de ataques a través del ciberespacio son las conocidas como:

- el ciberterrorismo,
- el ciberdelito,
- el ciberespionaje,
- el hacktivismo.

Algunos ejemplos de delitos cometidos a través del ciberespacio son la captación y reclutamiento para una organización terrorista y la inutilización de medios informáticos de las instituciones públicas, el robo de datos personales mediante *phising* y la intrusión de troyanos en los sistemas, que representan todo un reto para las Fuerzas y Cuerpos de Seguridad.

Es por ello que las Infraestructuras Críticas de todos los países estás expuestas a multitud de riesgos y amenazas fruto de sus vulnerabilidades. Las Infraestructuras Críticas son el objetivo más deseado de los atentados terroristas, los ataques cibernéticos de particulares e incluso ataques híbridos por parte de gobiernos y servicios de inteligencia, de ahí que necesiten una protección más avanzada. Ejemplos como la situación actual de Ucrania lleva a muchas organizaciones y países a mantenerse alertas ante el riesgo de un aumento de los ciberataques a otros países y pone en evidencia la problemática de la seguridad de entornos gubernamentales y su infraestructura critica. Ucrania, independientemente de los últimos ataques y de la situación de conflicto que se vive hoy, es un país que tiene cierta experiencia lidiando con ataques a sectores críticos, ya que durante los últimos años ha sido uno de los principales focos para este tipo de ataques. En 2015, por ejemplo, un ataque del troyano BlackEnergy a una planta de energía eléctrica provocó cortes en el suministro que afectaron a la mitad de los hogares en la región Ivano-Frankivsk. Un año después, Industroyer, un malware modular y personalizable que fue considerado la mayor amenaza para los sistemas de control industrial desde Stuxnet. Para sorpresa de muchos, Industroyer no solo afectaba la infraestructura critica de las redes de distribución de energía al poder apagar o encender a voluntad los interruptores de una subestación eléctrica, sino que podía ser utilizado para atacar cualquier Infraestructura Crítica. Pero es importante recordar también que en un país no solo existen las infraestructuras críticas industriales, sino que también se encuentran aquellas arraigadas a la producción de servicios digitales que son vitales para la población del país (infraestructuras criticas digitales). Por ejemplo, con el inicio de los ataques de Rusia a Ucrania, en los primeros días de marzo descubrieron una nueva amenaza, la cual tenía como objetivo borrar toda la información de cientos de equipos de entidades ucranianas.

El conflicto geopolítico marcó un hito en cuanto a la revisión de la infraestructura critica de los países en materia de la ciberseguridad. Estados Unidos, por ejemplo, rápidamente comenzó a tomar medidas para fortalecer la seguridad de la infraestructura critica de su país, mientras que otros países como Noruega lanzaron recientemente una convocatoria internacional en busca de investigadores para trabajar en la seguridad y resiliencia de infraestructuras críticas. [9]

Tipos de Amenazas

Las amenazas que pueden poner en riesgo los intereses vitales y estratégicos se han visto incrementadas en los últimos años. Tanto es así que los funcionarios de seguridad y del gobierno están preocupados por las amenazas y las vulnerabilidades a las que están expuestas las infraestructuras críticas, las mismas se pueden agrupar en [17]:

1. Terrorismo: Cada vez tiene mayores dimensiones, fundamentalmente el yihadista (*neo ideología oriental que hace referencia a un tipo de ideología caracterizada por la frecuente utilización del terrorismo, en nombre de una pretendida yihad, a la cual sus seguidores llaman una «guerra santa» en el nombre de Alá*), el cual actúa a nivel global realizando execrables atentados terroristas. En la actualidad, el Daesh / ISIS es el principal protagonista por su modo de operar, su proyección mediática y su rápida expansión, pero cada vez están surgiendo otros movimientos terroristas con diferente ideología.

2. Crimen organizado: Es una amenaza de carácter transnacional, flexible y opaca. Tiene una gran capacidad desestabilizadora, cuyo fin es el ánimo de lucro, pero debilitando el Estado y minando la buena gobernanza económica. Una parte del Crimen Organizado es el llevado a cabo por los Grupos Violentos que son los responsables de gran parte de las conductas violentas en las grandes ciudades.

3. Proliferación de armas de destrucción masiva: Supone una gran amenaza para la paz y la seguridad internacional, afectando de manera directa a la Seguridad Nacional.

4. Espionaje: Es una amenaza de primer orden para la seguridad tanto por el espionaje de otros países como por el realizado por empresas extranjeras. La Inteligencia en el ciberespacio recibe el nombre de ciberinteligencia siendo su objetivo obtener cantidades ingentes de información y datos confidenciales entre los que puedan estar los de Infraestructuras Críticas.

5. Vulnerabilidad del ciberespacio: Las amenazas en el ciberespacio han adquirido una dimensión global que va mucho más allá de la tecnología. El objetivo es conseguir diferentes propósitos como, por ejemplo, la expansión de determinados intereses geopolíticos por parte de Estados, organizaciones terroristas y actores individuales.

6. Vulnerabilidad del espacio marítimo: Este espacio es de gran relevancia dado que reviste un gran valor estratégico. Los factores que desafían la seguridad marítima se concentran en dos grupos:

- Amenazas derivadas de actos intencionados y de naturaleza delictiva (la piratería, el terrorismo, los tráficos ilícitos, etc.)

- Amenazas accidentales derivadas de las condiciones naturales del propio medio (accidentes marítimos y las catástrofes naturales).

7. Vulnerabilidad del espacio aéreo y ultraterrestre: El espacio aéreo puede ser comprometido por parte de actores estatales y no estatales. Algunos ejemplos son las acciones contra la aviación comercial, los sistemas de control de navegación y los tráficos ilícitos. Los drones generan nuevos riesgos y amenazas al facilitar el espionaje, la comisión de atentados y riesgos para la seguridad ciudadana, física y patrimonial.

8. Causas naturales: El impacto de las catástrofes perjudica la vida de las personas, así como a los bienes patrimoniales, al medioambiente y al desarrollo económico. Por otro lado, las epidemias y las pandemias han aumentado su número y las situaciones de riesgo. Y, finalmente, los efectos derivados del cambio climático tienen graves consecuencias. Por ejemplo, la subida de las temperaturas afecta a los niveles del mar, a la degradación del suelo y a la acidificación del océano, entre otros.

9. Otros: Cualquier tipo de perturbación en los servicios ofrecidos por estas infraestructuras de sectores estratégicos y esenciales podría conllevar riesgos en los flujos de suministros vitales o en el funcionamiento de los servicios esenciales, además de dar lugar a disfunciones en materia de seguridad.

Asimismo, hay que contemplar que existen una gran diversidad de infraestructuras críticas en un país. No es lo mismo hablar de un sistema critico financiero que de un sistema critico que accione sobre un sistema industrial (plantas químicas, sectores energéticos, entre otros). Sin embargo, lo que sí podemos mencionar a rasgos generales son los tipos de amenazas informáticas utilizadas para afectar estos sistemas críticos. [9]

A rasgos generales las podemos dividir en [9]:

- APT
- Worms (gusanos)
- Botnets
- Ataques de DDoS
- Troyanos
- Exploits Zero Day
- Phishing

Muchas de estas amenazas se utilizaron en conjunto para realizar ataques a gran escala. Tal caso fue el de Stuxnet, una amenaza que explotó una vulnerabilidad *zero*

day para permitir la ejecución de código malicioso alojado dentro de dispositivos USB con el objetivo de afectar los sistemas de control industrial de una instalación nuclear en Irán. Si bien no llego a tener implicancias mayores por errores del propio *malware*, ya que solamente logró ralentizar el proceso de enriquecimiento de uranio en Natanz, Stuxnet fue una gran combinación de amenazas. Además, es importante aclarar que fue el primer *malware* diseñado para afectar Sistemas de Control Industrial (ICS, por sus siglas en inglés) y abrió camino a otras amenazas, como fue Industroyer. [9]

A todo esto, debemos sumar que según un relevamiento reciente la cantidad de vulnerabilidad sobre los Sistemas de Control Industrial (ICS) en los sectores de infraestructura critica aumentó un 110% en los últimos años. [9]

Panorama de Amenazas Regionales

El Informe de Inteligencia de Seguridad de Microsoft es una publicación semestral que se basa en la experiencia interna de Microsoft para presentar el estado actual de las amenazas cibernéticas. La inteligencia que lo informa proviene de las señales relacionadas con la seguridad del consumidor y de los sistemas de negocios en las instalaciones y los servicios en la nube que Microsoft opera a escala global. Por ejemplo, cada mes se escanean 400 mil millones de correos electrónicos en busca de *phishing* y *malware*, se procesan 450 mil millones de autenticaciones y se ejecutan más de 18 mil millones de escaneos de páginas web. Esta información permite la observación de tendencias a través de las diversas plataformas de Microsoft, así como las regiones. [1]

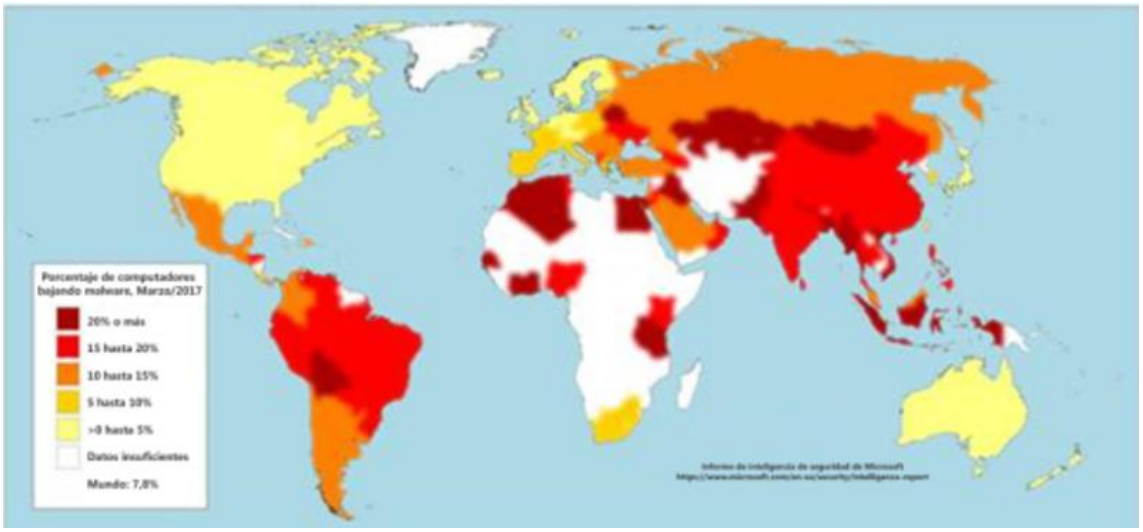


Figura 4 – Índice de amenazas cibernéticas por país/región [15]

Los resultados para América Latina y el Caribe en general siguen siendo más altos que el promedio mundial, aunque existen diferencias significativas entre los distintos países. Puerto Rico, Canadá y Estados Unidos rinden particularmente bien, superando al resto del mundo, mientras que Costa Rica y Panamá lo siguen de cerca. Los resultados del informe aclaran que todos los actores involucrados en la protección de infraestructuras críticas deben tomar en serio la ciberseguridad.

Es importante mencionar que la pandemia de 2019 ha generado, entre otras cosas, un incremento en el número, potencia y frecuencia de los ciberataques dirigidos a la región, en todas sus modalidades. Es algo que han señalado prácticamente todas las empresas analistas de seguridad. En América Latina se ha registrado un aumento del 24% en los ciberataques ocurridos durante los primeros ocho meses del año, en comparación con el mismo período de 2020.

El informe toma en cuenta los 20 programas maliciosos más populares, los cuales representan más de 728 millones de intentos de infección en la región con un promedio de 35 ataques por segundo. [19]

También detalla que, en este contexto de números de ciberataques del *Top20 de malware* encontramos que Brasil lidera la región con más de 1.390 intentos de infección por minuto, seguido de México, 299 por minuto, luego Perú con 96 por minuto, Ecuador con 89 por minuto, y finalmente Colombia con 87 por minuto.[20]

El Panorama de Amenazas en América Latina 2021 destaca también que la tendencia creciente de los ciberataques se verifica en todos los países, con la excepción de Costa Rica, que registró un leve aumento del 2%. [21]

En cuanto al crecimiento del número de ataques, podemos observar lo siguiente: [21]

- Ecuador (+75%)
- Perú (+71%)
- Panamá (+60%)
- Guatemala (+43%)
- Venezuela (+29%)

En tanto, el *phishing* o ataque de ingeniería social (mediante mensajes de correo fraudulentos) ha disminuido, aunque varios países de la región se encuentran aún entre los más atacados del mundo por esa modalidad.

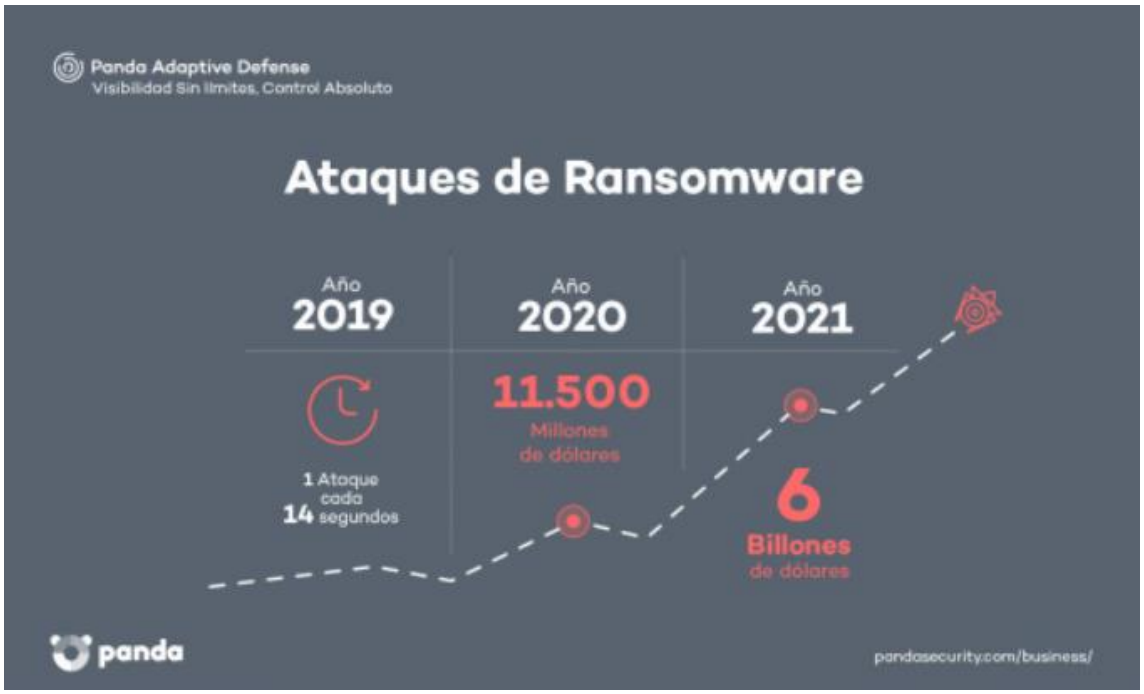


Figura 5 – Tendencia de Ataques de *Ransomware* [5]

Ataques a Infraestructuras Críticas en el Pasado

El gran público cree que, aunque puede haber riesgo, apenas han existido ciberataques a infraestructuras críticas. Desafortunadamente la realidad es otra y existen cientos de casos documentados alrededor de todo el mundo. Al pensar en ciberataques a infraestructuras críticas, nos tenemos que remontar mucho antes de que Internet existiera. Es por ello que recordar algunos incidentes que tuvieron lugar en el pasado reciente nos permiten tomar dimensión del impacto que podría un ciberataque a sectores críticos. A continuación, detallamos un análisis cronológico de los más representativos:

1982: Oleoducto Siberiano – Atacantes lograron instalar un troyano en el sistema SCADA que controlaba el oleoducto siberiano y provocó una enorme explosión en el mismo. [6]

1992: Chevron – Un trabajador fue despedido de la compañía y hackeo los ordenadores de Nueva York y San José que se encargaban del sistema de alertas y los reconfiguro para que dejaran de funcionar. Se descubrió el sabotaje cuando en Richmand, California, hubo un incidente en el que se liberó una sustancia nociva y el sistema no envió la alerta correspondiente, poniendo en riesgo a miles de personas durante las 10 horas en los que el sistema estuvo sin funcionar. [6]

1994: Salt River Project – Lane Jarret Davies logró ingresar a la red del Salt River Project a través de un modem, consiguiendo acceso a información y borrando ficheros de los sistemas responsables del control y entrega de agua y electricidad a sus consumidores. También accedió a información personal y financiera de los clientes y trabajadores. [6]

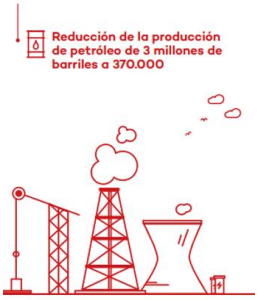
1997: Aeropuerto Worcester - un hacker ingresó en el sistema de control utilizado para las comunicaciones de tráfico aéreo en el aeropuerto de Worcester, Massachusetts, causando una falla que dejo inutilizado el sistema de telefonía durante 6 horas. Afecto los servicios de telefonía de la torre de control, del departamento de bomberos, del servicio meteorológico y de las compañías aéreas que estaban en el aeropuerto. [6]

1999: Gazprom – un hacker consiguió burlar los sistemas de seguridad de la compañía de gas natural rusa, con la ayuda de alguien que trabajaba en la empresa, y consiguió el control de los sistemas SCADA de la compañía que manejaban los flujos de gas. Para ello utilizó un troyano. [6]

2000: Maroochy System – un empleado hackeo con material robado a la empresa el sistema de control de aguas y provoco un vertido de un millón de litros de agua residuales en un rio cercano, inundando un hotel. [6]

2001: Planta de Gas – Un proveedor para encubrir un error que había provocado en uno de los ordenadores, creo una distracción hackeando 3 sistemas de la empresa y provocaron un corte de gas en hogares y empresas de un país europeo. [6]

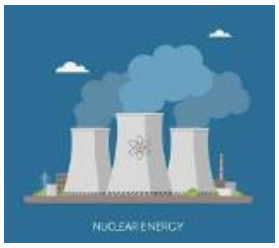
2002: PDVSA – la petrolera venezolana sufrió un ataque que bajo la producción de petróleo del país ese día - de 3 millones de barriles a 370.000 -. El ataque se llevó a cabo hackeando diferentes ordenadores dentro de la compañía. [6]



2006: Semáforos de los Ángeles – dos ingenieros de trafico de los Ángeles hackearon los semáforos de la ciudad durante una protesta laboral. Cambiaron la programación de alguno de ellos para que la luz roja estuviera mucho más tiempo activada, generando grandes atascos. [6]

2008: Tranvías de Lodz – un estudiante polaco de 14 años hackeo el sistema de tranvías de la ciudad de Lodz, en Polonia. El resultado 4 tranvías descarrilaron, causando 12 personas heridas. El estudiante construyo un mando infrarrojo similar a un mando de televisión con el que podía controlar los cruces de vías. [6]

2010: Stuxnet - un *malware* informático tomó el control de 1.000 máquinas que participaban en la producción de materiales nucleares y les dio instrucciones de autodestruirse. [22]



2011: Havex - es un *malware*, del tipo RAT (herramienta de control remoto) que permite obtener acceso a datos de las redes industriales y las máquinas. [25]

2012: Shamoon: es un *malware* con el objetivo de la destrucción de datos (y del sistema) de una red interna, se ha centrado en sitios de abastecimiento energético de determinados países, como Arabia Saudita. [26]

2012: Saudi Aramco – La mayor compañía petrolera del mundo fue víctima de un ataque dirigido a su cuartel general. Los atacantes habían conseguido acceso a la red a través de un ataque a uno de sus empleados, y desde ahí consiguieron acceso a 30.000 ordenadores de la compañía. Los atacantes borraron los contenidos de los ordenadores y en la pantalla se mostraba una bandera estadounidense en llamas. [6]

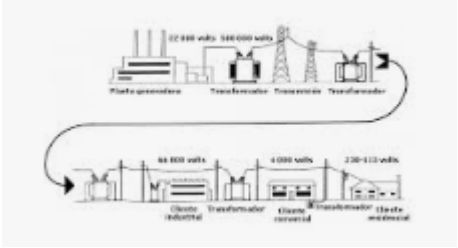
2012: RasGas – La empresa segunda mayor productora de gas natural licuado del mundo sufrió un ataque con el mismo *malware* utilizado en la petrolera saudi. Durante varios dias tanto la red interna como la pagina web de la empresa estuvieron inoperativas. [6]

2014: Planta Metalurgica Alemana – La planta fue victima de un ataque a traves de tecnica de ingenieria social, pudiendo acceder al ordenador de un empleado, y desde ahí consiguieron acceso a la red interna del sistema de control. Como consecuencia de esto, al apagar uno de los hornos, este no obedecio y se quedo encendido, lo que causo un daño masivo en las instalaciones. [6]

2015: Red Electrica Ucraniana – Ucrania sufrio un ciberataque en su red electrica que dejo sin energia a mas de 600.000 habitantes del pais. [6]

2015: BlackEnergy – un *malware* destructivo con un componente capaz de apagar sistemas críticos. afectó a una planta de energía eléctrica de Ucrania y dejo a miles de habitantes sin electricidad durante unas horas. [27]

2016: Industroyer - un *malware* modular y altamente personalizable que podría adaptarse a cualquier infraestructura crítica, como suministro de luz, agua y gas. El ataque a la red eléctrica de Ucrania, que dejó sin suministro una quinta parte de Kiev, capital de Ucrania, por una hora. [27]



2017: Triton - es un *malware* descubierto por primera vez en una planta petroquímica de Arabia Saudita. Puede desactivar los sistemas instrumentados de seguridad, que luego pueden contribuir a un desastre en la planta. Se le ha llamado "el malware más asesino del mundo. [28]

2017: WannaCry – es un *ransomware* que cifra los datos de la víctima y se solicita un rescate económico que debe ser pagado con la criptomoneda Bitcoin, para permitir de nuevo al acceso de los datos. Infecto más de 230.000 computadoras en más de 150 países. Los países más afectados fueron Rusia, Ucrania, India y Taiwán, así como partes del servicio nacional de salud de Gran Bretaña (NHS), Telefónica de España, FedEx, Deutsche Bahn, y las aerolíneas LATAM; junto con muchos otros blancos a nivel mundial. [29]

2017: Petya: *ransomware* NotPetya que afectó a la infraestructura critica de Banco Central de Ucrania y que luego se expandió a otros países. Además de los ataques a sectores como el de la salud, el energético o el de servicios financieros, los cibercriminales no temen en hasta incluso afectar los sistemas críticos de agua y saneamiento**.** [30]

2020: CPC Corp. - la compañía estatal de petróleo y gas natural de Taiwán vio su sistema de pago paralizado por un ataque de *ransomware*. Los actores de la amenaza utilizaron una unidad flash USB para infectar la red informática de la empresa. [31]

2021: Colonial Pipeline - un ataque de *ransomware* en los Estados Unidos cerró por completo la instalación durante unos días. Esto provocó una grave escasez de combustible y los precios se dispararon. Los piratas informáticos ingresaron a la red de la empresa a través de una cuenta de red privada virtual (VPN) inactiva que tenía acceso remoto a la red informática de la empresa. La empresa tuvo que

pagar un rescate de 4,4 millones de dólares a cambio de la herramienta de descifrado para restaurar su red informática. [31]

2022: Conflicto Rusa/Ucrania – se identificaron una nueva variedad de malware (programa maligno que realiza acciones dañinas en un sistema informático) y ataques de denegación de servicio distribuido (DDoS) que puede causar grandes pérdidas económicas a empresas al hacer que puedan estar horas sin funcionar.
Se informó haber detectado nuevo malware de borrado de datos que se ha utilizado contra organizaciones ucranianas. El objetivo es claro: eliminar todo tipo de datos e información y generar así caos y daño. [32]

La lista de ataques que se registraron en los últimos años apuntando a sectores críticos de un país es larga. Lo importante es comprender el impacto que pueden tener y más en un contexto como el actual de tensión geopolítica.

Impactos

Vivimos en un mundo globalizado, en el que los riesgos y amenazas a la seguridad son también globales, por lo que es necesario poder afrontarlos en estrecha colaboración con los países de nuestro entorno para así garantizar la seguridad con éxito.
Vivimos igualmente en una sociedad acelerada, en la que se producen muchos cambios en muy poco tiempo, lo que dificulta que los poderes públicos puedan dar una respuesta eficaz a los problemas que surgen en el marco de la seguridad. Es por ello que en el ámbito de la seguridad nacional resulta esencial contar con una normativa que, de acuerdo con el principio de optimización, establezca mecanismos y procedimientos que proporcionen a los poderes públicos la capacidad de responder con eficacia a todo tipo de vulnerabilidades tanto presentes como futuras, evitando así caer en la improvisación, que supondría una respuesta ineficaz e, incluso, incorrecta, ya sea por exceso o por defecto en el uso de los correspondientes instrumentos. Es más, no sólo ha de desterrarse la improvisación, sino que ha de fomentarse la anticipación y, consiguiente, prevención, para lo que es necesario la mejora de los sistemas de información, pues la obtención de información y su posterior análisis permite tener una visión aproximada de

posibles riesgos y amenazas a la seguridad nacional y prevenir, cuando sea posible, su materialización. Sólo sobre la base de unos mecanismos y procedimientos legalmente preestablecidos, que permitan un mejor análisis de cada situación, podrá darse una respuesta óptima a las amenazas a la seguridad nacional. Los estados modernos se enfrentan a multitud de desafíos que afectan a su seguridad nacional. Dentro de las prioridades estratégicas de la seguridad nacional se encuentran las infraestructuras, expuestas a una serie de amenazas. Para brindarles seguridad es imprescindible catalogarlas y diseñar un plan de prevención y protección contra las posibles amenazas. Tanto en el plano de la seguridad física, como tecnológicas y las comunicaciones. [6]

Sistemas de Protección de CI de Otros Países

A lo largo de estos años ha habido acontecimientos clave que han marcado un antes y un después en el escenario de la seguridad mundial, como fue en su momento el 11 de septiembre de 2001 (11S) para Estados Unidos, la del 11 de marzo de 2004 (11M) para Europa y bien el actual conflicto bélico entre Rusia y Ucrania. Situaciones que nos permiten ver como la destrucción de ciertos objetivos puede afectar la vida, salud y bienestar tanto de los ciudadanos como de los Estados. Es por ello que el tratamiento tradicional de la seguridad con relación a estos objetivos ha cambiado completamente. Las infraestructuras críticas están en su mayoría en el sector privado, y este sector tiene también una responsabilidad en este ámbito. Estas fechas generaron diversas iniciativas para mejorar la prevención, preparación y respuesta frente a ataques mejorando la protección de infraestructuras críticas. [8]

A continuación, detallamos las medidas que tomaron algunos países para hacer frente a esta situación [2]:

Australia

En Australia los órganos encargados de la protección de las CI son el *Critical Infrastructure Advisory Council* (en adelante CIAC) perteneciente al *Attorney General´s Department* del Gobierno de Australia. El CIAC es un órgano consultivo del gobierno cuya misión es el liderazgo de la protección de las CI, que además de estar presidido por el *Attorney General´s Department*, realiza labores de secretaría y asesoría en materias de recuperación de las CI. [2]

Este sistema se vale de las siguientes herramientas para llevar a cabo sus objetivos [2]:

- ***Trusted Information Sharing Network*** (en adelante TISN) Es uno de los instrumentos utilizados por Australia para la comunicación e intercambio de información entre los propietarios y los operadores con el Gobierno. Este se conforma como un espacio seguro en el que además de comunicarse, cooperan para hacer frente a los problemas de seguridad que pueden surgir en las CI. Por otro lado, Australia también cuenta con un CERT como ocurre en la mayoría de países estudiados a continuación.
- ***Critical Infrastructure Resilience*** (en adelante CIR). Es un sitio web cuya función es el asesoramiento en materias de recuperación y de acciones a realizar en caso de ataque a las CI. El objetivo es que los operadores principalmente y los propietarios de una CI sepan gestionar mejor los riesgos y amenazas, proporcionando continuidad a los servicios que realizan y así evitar la interrupción de la actividad, que podría tener graves consecuencias para la sociedad.
- ***National Terrorism Threat Advisory System***. Mediante esta herramienta se informa de la probabilidad de actos terroristas, para realizar las labores de protección y prevención de la nación. Presenta una escala de cinco niveles: *"Not expected", "possible", "probable", "expected" y "certain"*.

Japón

El sistema de protección de las CI en Japón se conforma mediante *The Second National Strategy on Information Security, Second Action Plan on Information Security Measures for Critical Information Infrastructure* y *The Basic Policy of Critical Information Infrastructure Protection.* El sistema japonés es un sistema complejo, bastante desarrollado y que atiende a todo tipo de riesgos y amenazas, en el que una vez más vuelve a destacar la colaboración público-privada. El sistema japonés hace hincapié en la prevención de ataques cibernéticos a sus infraestructuras de interés nacional como principal amenaza. El *Cabinet Secretariat* es el órgano de mayor rango encargado de la protección de las CI bajo el que se encuentran el *Information Security Policy Council* (ISPC) y el *National Information Security Center* (NISC) cuya función principal es el desarrollo de la política de protección de las CI. Por otro lado, cobra vital importancia la colaboración internacional, en este caso con Estados Unidos, Europa, la región Asia-Pacífico y la Asociación de Naciones del Sudeste Asiático (ASEAN). [2]

Otros centros, órganos y organizaciones que participan en el sistema son [2]:

- ***National Incident Response Team (NIRT).*** Su misión principal es analizar las amenazas, la realización de estrategias técnicas para prevenir incidentes y ayudar a otras organizaciones gubernamentales en materia de seguridad de la información proporcionando conocimiento en la materia.
- ***Japan Computer Emergency Response Team Coordination Center*** (JPCERT/cc). Es un CERT japonés cuyo objetivo es proporcionar productos y servicios en materia de seguridad a las agencias gubernamentales y a las asociaciones de industria y comercio.
- ***Telecom Information Sharing and Analysis Center*** (Telecom-ISAC). Es un centro cuyo objetivo consiste en intercambiar información entre el gobierno y los agentes participantes, del sector de las telecomunicaciones, en el sistema de protección de las CI, además del almacenamiento y análisis de la información.
- ***Cyber Force***. Se encarga de vigilar internet con el objetivo de proteger la seguridad de la red y en caso de tener constancia de un ataque ciberterrorista informar a los operadores críticos del mismo para que puedan reaccionar al mismo.
- ***Portal Site of National Police Agency***. Este sitio web se encarga de proporcionar información sobre la seguridad en las redes al gobierno para prevenir emergencias a gran escala en la red.
- ***Capability for Engineering of Protection, Technical Operation, Analysis and Response*** (CEPTOAR). Se encarga de intercambiar y analizar la seguridad de la información y las comunicaciones entre las entidades privadas y públicas.

Estados Unidos

El *National Infrastructure Protection Plan 2013 (NIPP): Partening for Critical Infrastructure Security and Resilience* se desarrolló con la colaboración entre los sectores públicos y privados, siendo los participantes en el sistema de protección los propietarios y operadores de las CI, las agencias gubernamentales a nivel territorial, estatal y local, las agencias no gubernamentales, las agencias específicas de cada sector y otros agentes y departamentos Federales. El *Department of Homeland Security (DHS)* bajo mando del Secretario de este departamento, es el órgano encargado de guiar, promover y coordinar los esfuerzos de todos los integrantes de la comunidad de infraestructuras críticas para promover la seguridad y la resiliencia de las mismas. El plan estadounidense es bastante complejo y consta de numerosos agentes que

participan y realizan una actividad específica en la protección de las CI. Algunos de ellos se agrupan por sectores, agencias de coordinación entre diferentes sectores y a nivel estatal, local y territorial. *Sector Coordinating Structures* es el título bajo el que se agrupan aquellos agentes mencionados anteriormente referidos a un solo sector y el *Cross-Sector Coordinating Structures* es la agrupación de aquellos que se refieren a la coordinación entre sectores diferentes. [2]

La siguiente figura refleja algunos de los elementos que componen la comunidad de CI:

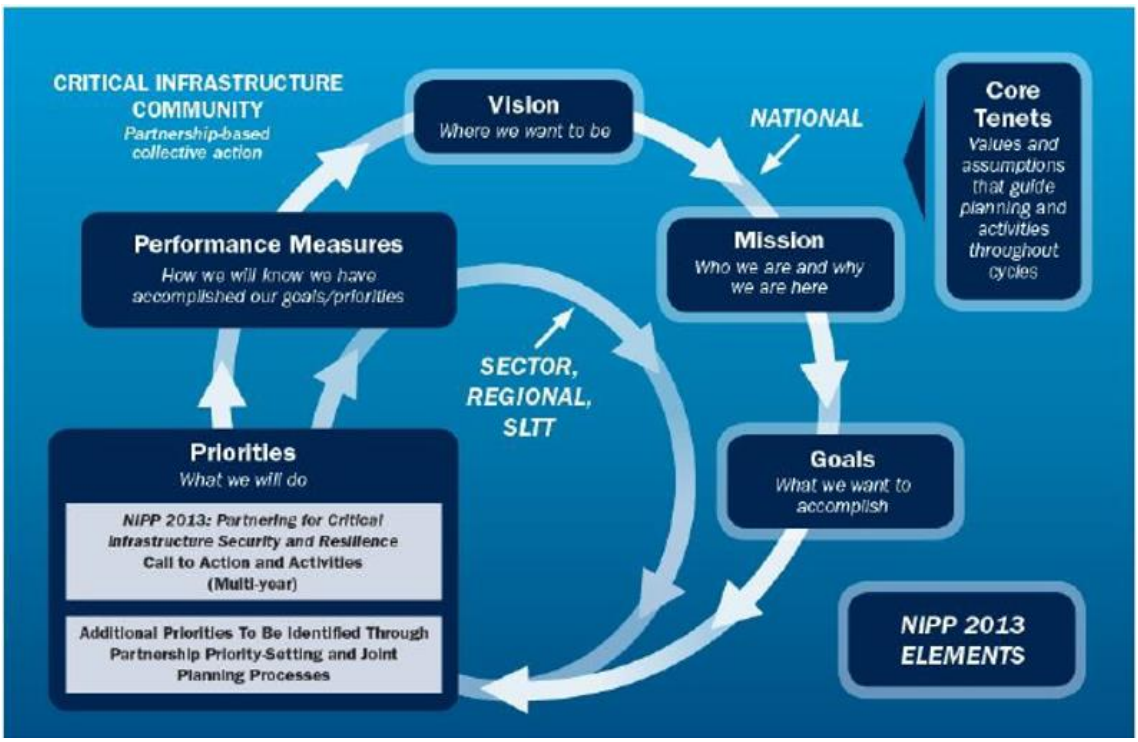


Figura 6 – Elementos que Componen la Comunidad de Infraestructuras Criticas [16]

Otros centros, agencias y organismos que participan de forma activa en este sistema, aportando diferentes funciones a la misma, son [2]:

1. ***Information Sharing and Analysis Centers*** (ISACs). Existe un centro para cada sector cuyo objetivo consiste en proporcionar análisis sectoriales profundos de amenazas y riesgos que ponen en peligro sus CI y coordinar las acciones llevados a cabo por el sector durante los incidentes, intercambiando además información con otros agentes de este sistema.

2. Critical Infrastructure Patnership Advisory Council (CIPAC). Los objetivos principales de este órgano son: la planificación, la coordinación y el intercambio de información entre sectores; el asesoramiento en materia de actividades operativas y de recuperación de las CI; proporcionar asesoramiento al Gobierno Federal en la creación y aplicación de políticas relacionadas con las CI.

3. National Infrastructure Coordinating Center (NICC). Es uno de los dos centros nacionales de CI del *Department of Homeland Security* junto con el *National Cybersecurity and Communications Integration Center* (NCCIC), que mencionaremos a continuación. Este centro tiene como objetivo proporcionar información previamente obtenida de las CI, para que los órganos encargados de tomar decisiones lo hagan eficazmente sobre cualquier tipo y nivel de amenaza.

4. National Cybersecurity and Communications Integration Center (NCCIC). Es el otro centro nacional de CI del *Department of Homeland Security* y tiene objetivos similares al NICC, con la diferencia de que sus actividades se centran sobre la parte lógica de las infraestructuras. Junto con el NICC tratan de reducir los tiempos de respuesta a la hora de tomar decisiones gracias a la información que aportan.

5. National Operations Center (NOC). Este órgano proporciona información y un marco de actuación común para el Gobierno Federal y los Gobiernos locales, estatales y territoriales, en caso de un incidente.

6. National Cyber Investigative Joint Task Force (NCIJTF). El FBI es el responsable de esta agencia y su función principal es desarrollar y compartir información sobre amenazas a través de la red y coordinar e integrar las actividades operacionales para hacer frente a los riesgos y amenazas, inclusive las que puedan afectar a las CI.

7. La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) es una agencia federal independiente de los Estados Unidos , un componente operativo bajo la supervisión del Departamento de Seguridad Nacional (DHS). Sus actividades son una continuación de la Dirección Nacional de Programas y Protección (NPPD). CISA se estableció el 16 de noviembre 2018, cuando el presidente Donald Trump firmó la Ley de Ley de Ciberseguridad e Infraestructura Agencia de Seguridad de 2018**.**

Estados Unidos, a pesar de usar instrumentos personalizados para cada órgano, también posee un CERT como ocurre en la gran mayoría de países. Uno de esos instrumentos es el *Protected Critical Infrastructure Information Program* (PCII) que establece los requisitos y pasos a seguir para el acceso y protección de la información de las CI. La comunidad en caso de incidente utiliza los sistemas establecidos en el *National Prevention Framework, National Response Framework, National Disaster Recovery Framework* y el *National Cyber-Incident Response Plan* cuyo objetivo principal es la prevención, la protección, la reducción de daños, la reacción y recuperación. [2]

Canadá

El sistema canadiense de protección de las CI se desarrolla en la *National Strategy for Critical Infrastructure* y el *Action Plan for Critical Infrastructure* que establecen una colaboración a nivel federal, provincial, territorial y de los sectores de las CI para el fortalecer la capacidad de recuperación de las mismas. El primero establece los principios básicos del funcionamiento de este sistema y el segundo profundiza en ellos desarrollando las actividades y mecanismos de los participantes en el mismo. La protección de las CI se enmarca dentro del *Department of Public Safety and Emergency Preparedness*, más conocido como *Public Safety Canadá*. [2]
La Estrategia Nacional para la Infraestructura Crítica de Canadá tiene como objetivo mejorar la resiliencia de las CI y definir las competencias de los Gobiernos provinciales, territoriales y federales y del sector privado. Para lograr la coordinación de las actividades a diferentes niveles de gobierno y sectores se crea el:

- ***National Cross Sector Forum***. Está formado por 10 representantes de cada uno de los diez sectores de CI. Se reúne anualmente y es presidida por el Viceministro de Seguridad Pública Canadá y un representante provincial o territorial. [2]
- ***Federal-Provincial-Territorial Critical Infrastructure (FPT-CI) Working Group***. Es el foro permanente en el que colaboran los Gobiernos, provinciales, territoriales y Federal en materia de CI. Las reuniones están copresididas por un representante del *Public Safety Canadá* y un representante provincial o territorial. [2]

Por su parte, el *National Risk Profile of Critical Infrastructure* proporciona información sobre los riesgos y amenazas para las CI, identificando dependencias e interdependencias entre las CI y sus sectores. El análisis de dicha información permite alcanzar una comprensión de las tendencias de los riesgos y amenazas. Estas actividades permiten llevar a cabo de una manera eficaz las actividades de gestión de riesgos de las CI. Este sistema tiene previsto que se comparta información multidireccional entre propietarios, operadores, gobiernos y organizaciones de seguridad e inteligencia como son *Royal Canadian Mounted Police* (RCMP), *Canadian Security Intelligence Service* (CSIS), *Canada Border Services Agency* (CBSA), *Canadian Cyber Incident Response Centre* (CCIRC) que ayudan, proporcionando información sobre los riesgos y amenazas, a la realización de actividades de gestión de riesgos. [2]

Canadá *utiliza Canadian Critical Infrastructure Gateway*, que consiste en una plataforma de trabajo de información no clasificada en el que los participantes en el sistema de protección pueden colaborar e intercambiar información con el objetivo de mejorar la capacidad de recuperación y hacer más seguras las CI canadienses. Por otro lado, el intercambio y la divulgación de información protegida o clasificada se rigen por las leyes y políticas federales, provinciales y territoriales. [2]

El *Regional Resilience Assessment Program* (RRAP) es un programa mediante el cual se realizan actividades de formación y evaluaciones de las CI, que podrán ser llevadas a cabo *"in situ"*, con el objetivo de analizar la capacidad de recuperación y la interdependencia entre ellas mismas. En estas evaluaciones se implican todos los agentes participantes en el sistema canadiense. [2]

Reino Unido

En Reino Unido la protección de las infraestructuras críticas se ha concretado en la *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards* de marzo de 2010; otros documentos que describen su sistema de protección de CI son: el *United Kingdom National Security Strategy* (NSS), *la Strategic Defence and Security Review* (SDSR) y la *UK's Cyber Security Strategy*, cada uno de ellos prevé, en su respectivo ámbito, la creación de un marco sobre la protección de las CI. El terrorismo y la ciberseguridad son los asuntos más relevantes a la hora de protegerse, además vuelve a ponerse de manifiesto la importancia de la colaboración público-privada y la agrupación por sectores para una mejor protección. Igualmente se hace hincapié en la prevención y en la capacidad de resiliencia de las CI. [2]

La *UK Government's counter terrorism strategy* (CONTEST) también hace referencia a las CI y divide su estrategia en cuatro aspectos [2]:

- *Prevent*
- *Pursue*
- *Protect*
- *Prepare*

El CPNI es el centro encargado de la protección de las CI en Reino Unido y está formado por el Centro de Coordinación de Seguridad de la Infraestructura Nacional (NISCC,

National Infrastructure Security Coordination Centre) y el NSAC (*National Security Advice Centre*), dependiente este a su vez del MI5 británico, y los centros WARP (*Warning, Advice and Reporting Point*). [2]

La *Office of Cyber Security & Information Assurance* (OCSIA) es un órgano cuya misión es asumir la dirección y coordinar el programa de ciberseguridad en Reino Unido con el objetivo de mejorar la seguridad en la red y la seguridad de la información, además proporciona asesoramiento al *Cabinet Office Ministers* y al *National Security Council.* Este órgano trabaja con el *Communications-Electronics Security Department* (CESG) que pertenece al *Government Communications Headquarters* y es la autoridad nacional para el aseguramiento de la información que, además, proporciona asesoramiento sobre cómo proteger la información y sistemas de información contra las amenazas actuales. Otros órganos importantes en la protección de las CI son el *National Cyber Security Centre y el Cyber Security Operations Centre* (CSOC). Este conglomerado de estrategias y de órganos componen el sistema de protección de las CI de Reino Unido, que como ocurre en la mayoría de los países también posee un CERT. [2]

Francia

En relación a la protección de las CI, Francia cuenta con la *Stratégie Nationale pour* la *sécurité du numérique* y el *Livre blanc sur la défense et la sécurité nationale*.
La principal regulación de la protección de las CI se realiza en la *Instruction générale interministérielle relative* la *sécurité des activités d'importance vitale Nº6600/SGDSN/PSE/PSN du 7 janvier 201453*, que sustituye la tradicional denominación de infraestructura crítica por la de *points d'importance vitale* (PIV) o *activités d'importance vitale*. Esta *Instruction générale crea el Dispositif de sécurité des activités d'importance vitale* (SAIV) que es descrito como el cuadro legislativo y reglamentario que permite asociar a los operadores de vital importancia (OIV), públicos o privados, al sistema nacional de protección contra el terrorismo, el sabotaje y los actos de mala fe y analizar los riesgos y aplicar las medidas de su nivel en coherencia con las decisiones de los poderes públicos. [2]

Además, la *Instruction générale interministérielle* crea tres planes de protección [2]:

- *Plans de sécurité d'opérateur (PSO).*
- *Plans particuliers de protection des points d'importance vitale (PPP).*
- *Plans de protection externe (PPE).*

El órgano responsable del sistema de protección de las CI en Francia es la *Secrétariat General de la Défense Nationale* (SGDSN) y el principal objetivo del sistema es protegerse especialmente de los ataques terroristas sobre infraestructuras físicas, aunque también adquiere importancia la protección de ataques a través de la red. El SAIV se coordina con otros planes como son el *Plan Vigipirate* y los planes complementarios del anterior llamado *Plans Pirate*. El *Plan Vigipirate* es un dispositivo de vigilancia, prevención y de protección en la lucha contra el terrorismo. Por su parte, los *Plans Pirate* son una serie de planes de intervención que se adaptan a un tipo de riesgo particular. Estos planes contemplan la utilización de medios específicos tales como armas biológicas, químicas y nucleares, en lugares igualmente específicos como pueden ser medios de transporte colectivos como aviones o el metro. Para cada caso existen unos mecanismos y respuestas específicos de reacción. [2]

Por último señalar que en Francia se han creado reglamentariamente órganos implicados en la protección de CI como es el *Conseil de politique nucléaire* o la *Agence nationale de la sécurité des systèmes d'information*, implementándose una regulación más exhaustiva mediante circulares e instrucciones como la *Circulaire relative à la doctrine nationale d'emploi des moyens de secours et de soins face à une action terroriste mettant en oeuvre des matières radioactives*, 18/02/2011 (800/SGDSN/PSE/PPS) u otras relativas a la protección de información clasificada. [2]

Bélgica

El sistema de protección de CI belga se configura principalmente en la Loi 01/07/2011 - *Sécurité et protection des infrastructures critiques*, buena parte de cuyo articulado coincide con los mandatos de la Directiva 114/2008/CE. La citada Ley ha sido posteriormente desarrollada reglamentariamente a través de las siguientes normas [2]:

- **Subsector del transporte aéreo**: AR 02/12/2011 - *Les infrastructures critiques dans le sous-secteur du transport aérien*.
- **Sector de la energía**: AR 11/03/2013 - La *sécurité et la protection des infrastructures critiques pour le secteur de l'Energie*.
- **Subsector de los puertos**: AR 29/01/2014 - La *sécurité et la protection des infrastructures critiques dans le sous-secteur des ports.*
- **Sector de telecomunicaciones**: AR 27/05/2014 - *Arrêté royal portant exécution dans le secteur des communications électroniques de l'article 13 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.*

- **Sector de transporte y subsector de transporte ferroviario**: AR 19/02/2016 - *Sécurité et prévention des infrastructures critiques, pour le secteur du transport, sous-secteur du transport ferroviaire.*

En cuanto a los centros y órganos que participan directa o indirectamente en la protección de las CI belgas son los siguientes [2]:

- ***Direction générale Centre de Crise du Service public fédéral Intérieur*** (DGCC): *Le Centre de Crise* es el agente más importante en la protección de las CI que no tiene centro propio, sino que forma parte de las muchas tareas de las que se encarga este centro. Éste se encarga de la protección de los bienes y personas y de la coordinación nacional en materia de orden público.
- ***Organe de Coordination pour l'Analyse de la Menace*** (OCAM) que se encarga de analizar las amenazas a nivel nacional.

Cultura Global de Ciberseguridad

Las consecuencias que generan las fallas en las Infraestructuras Críticas provocan daños de un impacto incalculable y ya hemos mencionado como los países han tomado medidas de prevención, entendiendo la gravedad que las vulnerabilidades existentes pueden provocar en los sistemas críticos, tratando así de proteger tanto a éstas como a la sociedad. [4]

Es necesario que se promueva una cultura global de Ciberseguridad y de prevención en las TIC, de modo que puedan desarrollarse e implementarse prácticas tratando de identificar los temas comunes y especialmente los problemas y las fallas más comunes, contando con la colaboración y cooperación de equipos internacionales expertos, analistas e investigadores, que deriven de orígenes académicos, del sector privado o del sector gubernamental. Es por ello que han surgido diversas iniciativas a nivel mundial, las cuales han servido y continúan actualmente siendo utilizados como bases de proyectos, entre las cuales podemos mencionar:

ITU (Unión de Telecomunicación Internacional)

La Unión de Telecomunicación Internacional o "ITU", siglas en inglés de *International Telecommunications Union*, es el organismo especializado de la Organización de las Naciones Unidas (ONU), encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras. Miembros de

la ITU han tenido un rol importante en materia de Ciberseguridad, a través de varias resoluciones, decisiones, programas y recomendaciones junto a los representantes del gobierno, la industria, el sector académico e instituciones de investigación, regional e internacional. La ITU proporciona un foro donde se exponen los diversos puntos de vista en los temas de Ciberseguridad y Ciberdelincuencia, con el objetivo de llegar a un entendimiento común entre los países participantes sobre la forma en que estos inconvenientes pueden ser abordados. [4]

La sede de esta organización se encuentra en Ginebra (Suiza).

La ITU está compuesta por tres sectores:

- ITU-T: Sector de Normalización de las Telecomunicaciones
- ITU-R: Sector de Normalización de las Radiocomunicaciones
- ITU-D: Sector de Desarrollo de las Telecomunicaciones de la ITU

En general, la normativa generada por la ITU está contenida en un amplio conjunto de documentos denominados Recomendaciones, agrupados por Series. Cada Serie está compuesta por las Recomendaciones correspondientes a un mismo tema. Aunque en las Recomendaciones nunca se "ordena", solo se "recomienda", su contenido, a nivel de relaciones internacionales, es considerado como mandatario por las Administraciones y Empresas Operadoras. [4]

La Agenda sobre Ciberseguridad Global (GCA) es un marco de la ITU para la cooperación internacional a fin de proponer soluciones para mejorar la confianza y la seguridad en la sociedad de la información. Se basa en las iniciativas nacionales y regionales para evitar la duplicación de trabajo y fomentar la colaboración con todos los interlocutores. [4]

En la agenda se definieron cinco temas:

- Medidas legales
- Medidas técnicas y de procedimientos
- Las estructuras orgánicas
- Capacidad de construcción
- Cooperación Internacional

Estos cinco temas constituyen el informe estratégico global internacional, a partir del cual se elaborarán las siguientes estrategias [4]:

- El desarrollo de un modelo legislativo del cibercrimen
- La creación de estructuras políticas nacionales y regionales sobre cibercrimen
- Establecer criterios de seguridad y esquemas de acreditación para aplicaciones de sistemas de software.
- La creación de un marco legal para observar, prevenir y responder a un incidente.
- La creación de un sistema genérico universal de identidad digital
- La facilidad de construir capacidades humanas e institucionales
- La cooperación internacional, dialogo y coordinación

Es fundamental que cada país incluya el desarrollo de [4]:

- Entender el cibercrimen desde una perspectiva global
- Definir una estrategia de Ciberseguridad a nivel nacional
- Desarrollar el conocimiento público de los desafíos ante el cibercrimen y la Ciberseguridad (los problemas económicos, políticos, sociales, técnicos y legales)
- Promover una cultura en Ciberseguridad (información sobre riesgos, propagación de simples recomendaciones como ser; usar sistemas seguros, reducir las vulnerabilidades evitando situaciones peligrosas)
- Entrenar e informar sobre tecnologías de comunicaciones y problemas de seguridad y proveer de normas legales pertinentes.
- Desarrollar la educación en Ciberseguridad
- Proponer un marco de trabajo unificado el cual incluya una muestra humana, regulatorio, organizacional, económica, técnica y operacional acerca de la Ciberseguridad.
- Colocar estructuras organizacionales como soporte estratégico en distintos puntos del país.
- Crear puntos de alertas regionales que provean de información técnica y asistencia con al cibercrimen y a los riesgos en seguridad.
- Crear leyes efectivas a nivel nacional e internacional.
- Desarrollar prácticas aceptables de protección y reacción
- Establecer cooperación efectiva y promover la cooperación y coordinación a nivel nacional e internacional.
- Forzar a los proveedores de tecnologías a mejorar la seguridad de sus productos y servicios.

G8

Se denomina G8 o “Grupo de los ocho” a un grupo de países industrializados del mundo cuyo peso político, económico y militar es muy relevante a escala global. Está formado por 8 países del mundo, Estados Unidos de América, Reino Unido, Canadá, Francia, Alemania, Italia, Japón y Rusia. Fue creado en 1975 como el G7, en ése momento eran siete los países que lo conformaban. Anualmente los representantes de estos países se reúnen en las llamadas Cumbres del G8. La finalidad de las reuniones es la de analizar el estado de la política y las economías internacionales e intentar aunar posiciones respecto a las decisiones que se toman en torno al sistema económico y político mundial y a las relaciones con los países en desarrollo. A partir de esta base inicial en la agenda de las cumbres realizadas, se ha ampliado considerablemente los temas a tratar incluyendo los micro-económicos tales como el empleo y la autopista de la información, los problemas internacionales como el medio ambiente, la delincuencia y las drogas, y una serie de temas políticos y de seguridad que van desde derechos humanos a través de la seguridad regional hasta el control de armas, enfocándose en el estado actual del terrorismo en el mundo. En Julio del 2000, en Okinawa, se realizó el *Okinawa Charter on Global Information Society* o la llamada Carta constitucional, GIS o siglas en inglés de *Global Information Society*, en la cual se enumeran importantes principios para el desarrollo de una información global, acompañada por acciones para prevenir el cibercrimen y crear un ciberespacio seguro en la sociedad mundial. En este aspecto, la carta constitucional de Okinawa se refiere a las Pautas de la Organización para la Cooperación y el Desarrollo Económico u “OECD”, siglas en inglés de *Organisation for Economic Co-operation and Development*, en lo que se refiere a la Seguridad de Sistemas de Información. En esta Carta constitucional, el G8 pidió al sector público y al privado a realizar los mayores esfuerzos para unir la información internacional. En el documento “G8 Principios para proteger las Infraestructuras de Información Crítica”, del 2003, se da información esencial acerca de las infraestructuras críticas, como protegerlas efectivamente, y como los países deben protegerlas de daños y posibles ataques. Además de poder identificar las causas y el origen de los mismos, sugiriendo una apropiada intercomunicación, coordinación y cooperación entre los distintos países. Son once los puntos que se enumeran, incentivando a los países a considerarlos en el desarrollo de sus estrategias para reducir los riesgos de Infraestructuras Críticas. [4]

OECD (Organización para la Cooperación y el Desarrollo Económico)

La OECD es una organización de cooperación internacional, compuesta por 34 estados, cuyo objetivo es coordinar sus políticas económicas y sociales. Fue fundada en 1960 y su sede central se encuentra en el *Château* de la *Muette*, en la ciudad de París, Francia. En la OECD, los representantes de los países miembros se reúnen para intercambiar información y armonizar políticas con el objetivo de maximizar su crecimiento económico y ayudar a su desarrollo y al de los países no miembros. Se considera que la OECD agrupa a los países más avanzados y desarrollados del planeta, siendo apodada como el club de países ricos. Los 34 países miembros que lo conforman son: Australia, Austria, Bélgica, Canadá, Chile, República Checa, Dinamarca, Estonia, Finlandia, Francia, Alemania, Grecia, Hungría, Islandia, Irlanda, Israel, Italia, Japón, Corea, Luxemburgo, México, Países Bajos, Nueva Zelanda, Noruega, Polonia, Portugal, República Eslovaca, Eslovenia, España, Suecia, Suiza, Turquía, Reino Unido y Estados Unidos. [4]

Los principales objetivos de la OECD son [4]:

- Contribuir a una sana expansión económica en los países miembros, así como no miembros, en vías de desarrollo económico.
- Favorecer la expansión del comercio mundial sobre una base multilateral y no discriminatoria conforme a las obligaciones internacionales.
- Realizar la mayor expansión posible de la economía y el empleo y un progreso en el nivel de vida dentro de los países miembros, manteniendo la estabilidad financiera y contribuyendo así al desarrollo de la economía mundial.

La OECD, ha desarrollado artículos sobre los temas de seguridad de sistemas de información y redes, incluyendo a las infraestructuras de información crítica. Actualmente la organización está comprometida a dar lucha contra el cibercrimen y contra el uso de software malicioso. Produce constantemente informes analíticos, estadísticas, y guía de políticas, declaraciones y recomendaciones para ayudar al sector gubernamental y al empresarial a desarrollar políticas consistentes en seguridad de la información, relevando el conocimiento público de mayor importancia, para desarrollar una cultura de seguridad en la sociedad. [4]

Las Pautas de la OECD incluyen los siguientes principios complementarios a la política y a los niveles operacionales [4]:

1. Conocimiento: Los partícipes deben ser consciente de la necesidad de segurizar los sistemas de información y redes y de las opciones para reforzar la seguridad;

2. Responsabilidad: Todos los partícipes son responsables sobre la seguridad de los sistemas de información y redes;

3. Respuesta: Los partícipes deben actuar oportunamente previniendo y respondiendo ante diferentes incidentes;

4. Ética: Los partícipes deben respetar los intereses legítimos de los otros;

5. Democracia: La seguridad de sistemas de información y redes debe ser compatible con los valores esenciales de una sociedad democrática;

6. Valoración de riesgo: Los partícipes deben dirigir la valoración de riesgo;

7. Plan de Seguridad y aplicación: Los partícipes deben incorporar la seguridad como un elemento esencial en los sistemas de información y redes;

8. Dirección de la Seguridad: Los partícipes deben adoptar un acercamiento comprensivo en la dirección de seguridad;

9. Re-evaluación: Los partícipes deben repasar y deben imponer la seguridad en los sistemas de información y redes, y realizar las modificaciones apropiadas a las políticas de seguridad, prácticas, medidas, y procedimientos.

Acuerdo entre EE. UU y Canadá.

Canada-United States Action Plan for Critical Infrastructure (en adelante Canadá-U.S. *Action Plan*) es un Plan que pretende fortalecer la protección y la capacidad de resiliencia de las infraestructuras críticas mediante la colaboración entre Canadá y Estados Unidos. El citado Plan es fruto del *Agreement Between the Government of Canada and the Government of the United States on Emergency Management Cooperation*, acuerdo formalizado entre Estado Unidos y Canadá en diciembre de 2008, por el que ambos Estados se comprometieron a colaborar en situaciones de emergencia que involucrasen a los dos países. El Plan prevé el intercambio y protección de información entre ambos países, además de la colaboración entre los diferentes sectores de ambos, la colaboración en la identificación de CI y sectores de riesgo y la intervención conjunta mediante los planes de gestión de riesgos. [2]

Los objetivos del *Canadá-U.S. Action Plan* serían básicamente [2]:

- La naturaleza interconectada de las infraestructuras críticas exige un enfoque coordinado entre Canadá- EE.UU.
- El enfoque regional para la colaboración a través de la frontera debe ser guiada por un marco global para la infraestructura crítica entre Canadá-EE.UU.
- La fuerte colaboración del sector privado a través de la frontera debe ser respaldado por un enfoque integrado entre Canadá-EE.UU.
- La descoordinación aumenta la probabilidad de la duplicación de costes y esfuerzos que pueden ser evitados a través del desarrollo de la colaboración y el intercambio de mejores prácticas.
- La comunicación entre las partes implicadas en las infraestructuras críticas (tanto nacional como transfronteriza) necesitan ser coordinadas de forma precisa y oportuna.

Programa Europeo de Protección de Infraestructuras Críticas (PEPIC).

El Programa Europeo de Protección de Infraestructuras Críticas (PEPIC) tiene como objetivo la mejora de la protección de las CI en la UE frente a las amenazas a las mismas, especialmente contra el terrorismo. Su punto de partida es la identificación y designación de las Infraestructuras Críticas Europeas (en adelante ICE), tal y como ordena la Directiva 2008/114/CE. Su ejecución requiere la adopción de "medidas diseñadas para facilitar la aplicación del PEPIC, lo que incluye un Plan de acción del PEPIC, la Red de información sobre alertas en infraestructuras críticas (CIWIN), el uso de grupos de expertos en PIC a nivel de la UE, los procedimientos para compartir la información sobre PIC y la identificación y análisis de interdependencias". Por lo tanto, se deben llevar a cabo planes de intervención en caso de incidente que afecte a alguna ICE y además se le debe prestar apoyo a las CI de los Estados miembros. Este programa sitúa su plan de acción en 3 líneas de actividad que son las siguientes [2]:

- **Línea de actividad 1**: se ocupará de los aspectos estratégicos del PEPIC y del desarrollo de medidas aplicables horizontalmente a todas las acciones de protección de CI.
- **Línea de actividad 2**: se ocupará de las infraestructuras críticas europeas y se ejecutará a nivel sectorial.
- **Línea de actividad 3**: se ocupará de apoyar a los Estados miembros en sus actividades relacionadas con infraestructuras críticas nacionales.

Los Estados miembros usan para el intercambio de información de sus ICE y de alertas rápidas, la Red de Información sobre Alertas en Infraestructuras Críticas (CIWIN), complementando los sistemas y plataformas que tengan los países establecidos para sus CI. El Sistema Europeo de Alerta Rápida (ARGUS por sus siglas en inglés) permite la conexión de todos los sistemas de emergencia en Europa mandando la información a los mismos para que lleven a cabo las medidas pertinentes en caso de amenaza [2].

Los Planes de Intervención se realizan en caso de incidente, su finalidad es reducir los daños e impedir la destrucción de la CI, intentando evitar que interrumpan sus servicios, tanto en el país en el que se produce el incidente como en los Estados miembros a los que proporcione servicios o se interconecten con las correspondientes CI. En su ejecución intervienen todos los agentes implicados en la protección de las ICE tanto nacionales como comunitarios. El PEPIC marcó las pautas que debían seguir los Estados miembros en sus desarrollos legislativos sobre las CI, explicando la similitud entre los sistemas de protección de las CI de la mayoría de los Estados miembros de la UE [2].

Protección de Infraestructura de Información Crítica

La CIIP contempla al conjunto de subsistemas destinados a garantizar la seguridad de los diferentes recursos y procesos vinculados a la CII. La CIIP se basa en un conjunto de personas, recursos físicos, sistemas de comunicación e información, normas y procedimientos, de carácter indispensables para la nación, en base a los cuales se logra garantizar la continuidad de las operaciones de los sistemas vinculados a la CII. Las CII pueden ser sujeto de errores involuntarios, de desastres naturales (huracanes, tornados, terremotos, inundaciones, etc.), de accidentes (interrupciones nucleares, radiológicas, biológicas o sustancias químicas), o de ataques deliberados causados por personas o naciones (terroristas, criminales, hackers) con intereses contrapuestos. La CII es considerada un recurso invaluable para la sociedad moderna por lo que la CIIP permite establecer un esquema de seguridad adecuado por medio del cual enfrentar las diferentes amenazas en base al concepto de tratamiento de riesgos de seguridad.

Desde el punto de vista estratégico, la CIIP cumple sus objetivos en base a los siguientes principios [4]:

Principio 1 “Seguridad Física”: proteger los activos físicos de carácter crítico vinculados a los diferentes sistemas en el contexto de CII.

Principio 2 "Seguridad Lógica": proteger los diferentes activos de información vinculados a los sistemas en el contexto de CII.
Principio 3 "Colaboración": establecer recursos y procesos que permitan abordar la problemática vinculada a la CII desde una perspectiva global e integradora, que utilice diferentes recursos de los sectores público y privado por medio de los cuales poder abordar al problema con un frente unificado. La Colaboración implica la generación de recursos que permitan agilizar las comunicaciones y compartirlas (herramientas y datos).
Principio 4 "Aprendizaje": todas las operaciones desarrolladas en el contexto de CIIP deben aportar el conocimiento sobre el tratamiento de la problemática. El aprendizaje deberá poder se traducido en una estrategia.

En toda situación que comprometa la seguridad de la CII, las consecuencias de la misma seguramente serán sentidas por la sociedad provocando en algunos casos situaciones de pánico y temor por los daños causados. Debido a su carácter crítico, es de esperar que los recursos vinculados a las CIIP no estén aislados entre sí, de tal modo que pueda garantizarse su continuidad en situaciones de desastre. Para esto, deben contemplarse arquitecturas de interconexión a escala nacional y multinacional, dependiendo de otras infraestructuras. Debido a esto, cualquier accidente a escala nacional, requerirá de esfuerzos a escala mundial, ya sea por los gobiernos o por el sector privado en el que todos resulten beneficiados. Las operaciones de protección de una CI emplean metodologías analíticas por medio de las cuales es posible detectar e identificar las vulnerabilidades y realizar un análisis que derive en estrategias adecuadas de mitigación del riesgo. Por ejemplo, pueden realizarse pruebas de penetración sobre la infraestructura ya que es un método relativamente sencillo, rápido y económico para detectar brechas de seguridad en los diferentes sistemas. Este tipo de técnicas es útil especialmente en aplicaciones web que den soporte a las CII. Una cuestión importante que debe ser tenida en cuenta es que las metodologías de evaluación del riesgo deben ser consideradas independientemente del modelo de negocio del que se trate, alcanzando tanto al sector privado como al público. La finalidad de las actividades vinculadas a la CIIP consiste en garantizar que ningún perjuicio pueda poner en peligro la vida de una organización la cuál sea parte de la CII. En términos prácticos esto equivale a reducir la probabilidad de materialización de las amenazas, limitar las consecuencias de los ataques y los problemas de funcionamiento inducidos y permitir la normalidad y funcionamiento de un sistema tras un siniestro a un costo aceptable y

en un plazo razonable. Las TIC son por sí mismas Infraestructuras de Información Crítica [4].

PLAN DE ACCIÓN

Objetivo

El objetivo prioritario debe concentrarse en la protección de las infraestructuras con dimensión transnacional. Para ello es necesario desarrollar un Programa para la Protección de las Infraestructuras Críticas, con el fin de definir las mismas, analizar sus vulnerabilidades y su interdependencia, así como presentar soluciones que prevengan y protejan ante todo tipo de peligros. Dicho programa debe ayudar a las empresas a integrar las variables de la amenaza y sus consecuencias en sus evaluaciones del riesgo; esta última no debe ser solo la confidencialidad o la integridad de la información, sino la tolerancia a fallos, con el objetivo de evitar consecuencias impredecibles, especialmente, la pérdida de vidas humanas. Es por ello fundamental que se tomen medidas en la línea de desplegar una estrategia de seguridad que cuente con múltiples filtros de protección.

Responsabilidad

Como ya hemos comentado con anterioridad, gran parte de los suministros y servicios esenciales de los países son ofrecidos, facilitados y garantizados por las infraestructuras críticas. Debido al carácter interdependiente, complejo y privado de la gran mayoría de las infraestructuras críticas es de suma relevancia su protección. De esta manera, los principales responsables de la protección de las infraestructuras críticas son [17]:

1. Gobiernos – Son los principales interesados en la generación e implantación de iniciativas de Protección de Infraestructuras Críticas para garantizar que los servicios esenciales funcionen de manera adecuada.

2. Organismos competentes – Es muy común que los gobiernos deleguen las tareas de difusión, elaboración y gestión de iniciativas de Protección de Infraestructuras Críticas (CIP) en organismos públicos, privados o combinación de ambos. Se encargan de garantizar que la industria adopte las medidas de seguridad establecidas por las leyes de protección. Para ello, fomentan y difunden las iniciativas de concienciación y

de facilitación del cumplimiento legislativo. Los organismos competentes son los siguientes:

- La Secretaría de Estado de Seguridad del Ministerio del Interior.
- El Centro Nacional para la Protección de las Infraestructuras Críticas.
- Los Ministerios y organismos integrados en el Sistema.
- Las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía.
- Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía.
- Las Corporaciones Locales mediante la asociación de Entidades Locales de mayor implantación a nivel nacional.
- La Comisión Nacional para la Protección de las Infraestructuras Críticas.
- El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

3. Operadores de infraestructuras críticas – Son los que tienen más interés en que sus infraestructuras sean seguras, funcionen de manera adecuada y no sufran daños, interrupciones ni ataques. No obstante, en ocasiones, los requerimientos de las normativas pueden entrar en conflicto con sus estrategias empresariales. Las principales funciones de los operadores críticos en materia de seguridad son:

- Analizar sus organizaciones para comprobar si hay algún tipo de problema en ellas.
- Diseñar nuevas políticas de seguridad y un marco de gobierno desde el punto de vista de la seguridad integral.
- Establecer nuevas estructuras organizativas para converger la seguridad física con la cibernética bajo un mismo responsable.
- Hacer reuniones para gestionar todos temas relacionados con la seguridad que fueran transversales a la organización.
- Analizar los de riesgos y las amenazas no previstos con anterioridad y que han ayudado a mejorar la planificación de la seguridad.
- Llevar a cabo estudios de las consecuencias y el impacto que supondría la interrupción y no disponibilidad de los servicios esenciales prestados por el operador.
- Concienciar al personal sobre la importancia del cumplimiento de los procedimientos y recomendaciones de seguridad en su operativa diaria.

4. Terceras partes – No se ven afectadas de manera directa por las exigencias legales, pero sí manera indirecta. Un ejemplo de ello son las empresas en que los operadores de las infraestructuras hayan delegado la gestión de las mismas. La forma en que se

verán afectadas variará en función de los acuerdos establecidos con el operador de la infraestructura. Así pues, podrán ir desde la asunción de nuevas responsabilidades dentro del marco de trabajo existente o a la contratación de nuevos servicios.

Figura 7 – Principales Responsables de la Protección de las Infraestructuras Criticas [17]

Plan Completo de Seguridad Integral

Las infraestructuras críticas necesitan incrementar sus niveles de seguridad, monitoreo, respuesta ante incidentes, resiliencia y comunicación en tiempo y forma de los incidentes, integrando la seguridad en los procesos de negocio y creando un entorno de trabajo más seguro para todos. Para lograr estos objetivos, las organizaciones necesitarán una estrategia de ciberseguridad innovadora basada en principios de buena gestión de riesgos, considerando sus activos más críticos y los escenarios que plantea un evento de riesgo de estas características. La ciberseguridad tiene que ser parte integrante de todo el proceso de transformación digital, de ninguna manera debe ser pensada como adicional o paralela sino como transversal a toda la organización.

El programa de protección para la CI (Información Crítica) establecerá, en primer lugar, la base para facilitar el intercambio de información entre los operadores de infraestructura crítica a través de políticas y directrices. En segundo lugar, permitirá una focalización sistemática, mejoras a través de mediciones más claras de gobernanza,

madurez y ciberseguridad de las redes. Tercero, requerirá operadores para fomentar una cultura de alfabetización en riesgos cibernéticos en todos los niveles de las organizaciones.
El objetivo es que todos los sectores críticos establezcan un sistema robusto y efectivo contra las ciberamenazas en evolución.

Estrategia Nacional

La realidad analizada y en la que vivimos hace necesario regular la Protección de las Infraestructuras Críticas para poder aportar un mayor grado de protección frente a amenazas de todo tipo. [6] Para mejorar la prevención y respuesta frente a ataques lógicos, los gobiernos deben llevar a cabo distintas medidas a nivel global. Medidas orientadas a la creación de centros de coordinación que registren todo tipo de información relevante para aumentar la protección de las infraestructuras críticas.

Cooperación y Proyectos Comunes

La ciberseguridad no debe ser tratada como un tema político partidista, la ciberseguridad es transversal. Todas las personas pueden ser potenciales víctimas de fraudes y todas las instituciones y empresas pueden ser blanco de ataques. Se debe ir en busca de alcanzar el mismo objetivo. El éxito está en los países que logran establecer la cooperación, intercambian información y desarrollan proyectos comunes.

Entre las mejores prácticas está la de identificar la infraestructura crítica que debe ser resguardada para su operación integral, los protocolos necesarios para la prevención, atención y respuesta ante riesgos y desastres; y la creación de una instancia capaz de coordinar los esfuerzos. Existen sectores que por sus características son especialmente sensibles, como, por ejemplo, el eléctrico, el agua, el gas, el transporte, el químico, las comunicaciones, el sistema financiero, el sanitario, etc.

Un elemento adicional a entender en el caso del resguardo de la infraestructura crítica de un país, es el hecho de la interconectividad existente en el mundo digital. Ello potencia efectos de contagios y de multiplicación de consecuencias que pueden rebasar a los propios países, como es el caso de los virus. También significan oportunidades, pues se pueden obtener economías de escala en el uso y aprovechamiento de la infraestructura tecnológica, como ocurre en la Unión Europea, que trabaja en el

concepto de Espacio Económico Común Europeo. Cabe señalar que el tema de la infraestructura tecnológica crítica no es exclusivo de los gobiernos, también es aplicable a todas las empresas y organizaciones que dependen de sistemas y servicios informáticos: solo cambian los riegos y la complejidad en su atención.

Colaboración entre Entidades

La gravedad del incremento de riesgos cibernéticos ha suscitado una oleada de reacciones, en las que las autoridades han ejercido muchas veces de director de orquesta, coordinando las actividades entre el sector público y el privado, puesto que la realidad indica que, muchas de las infraestructuras críticas de una nación se encuentran en manos de operadores que, desconocen por sí solos, en mayor o menor grado, cuál es la mejor manera de identificar, diseñar y ejecutar las mejores estrategias en materia de ciberseguridad. [23]

Una de las claves para llevar a cabo estas acciones –además de la necesaria coordinación entre instituciones y empresas- es la disposición de la información exhaustiva y actualizada sobre las nuevas amenazas que desafían la integridad de las infraestructuras críticas. Para ello son necesarios el diálogo, la asociación y la colaboración entre entidades y empresas especializadas y dedicadas, ya sea a nivel nacional como internacional, así como participación de especialistas y expertos en la materia. En este sentido, una de las medidas con mayor éxito para hacer frente a los delitos cibernéticos es la creación de CERTs. Un CERT, como es sabido, está constituido por un equipo de expertos muy cualificados cuyo objetivo es asumir y centralizar los planes directores de las empresas y entidades en materia de seguridad. El primero apareció a finales de los 80, en EEUU, y aunque sus siglas en inglés - *Computer Emergency Response Team* - lo definan como un equipo de respuesta ante incidentes de seguridad, un CERT desempeña en la actualidad todas las funciones requeridas para implementar un servicio integral de seguridad. El éxito de estas estructuras y las recomendaciones internacionales de organismos vinculados con la seguridad de las redes de telecomunicaciones, han hecho que la implantación de CERTs se haya multiplicado por cinco en la última década. [23]

Por lo que se refiere a la gestión de la seguridad, hay que recordar que no es posible proteger todas las infraestructuras contra las distintas amenazas, ni siquiera ante la amenaza de atentados terroristas. Sin embargo, mediante técnicas de gestión de riesgos se puede focalizar la atención en los puntos de máximo riesgo permanente o

prioritario. En relación con la gestión de la ciberseguridad, conviene destacar también que es un proceso deliberado de análisis de los riesgos y amenazas, y de decisión y ejecución de acciones, con objeto de reducir el riesgo a un nivel definido y aceptable, a un coste razonable, teniendo en cuenta, igualmente, las vulnerabilidades del sistema y actividad. En consecuencia, se acuña el término de ciberseguridad como esa connotación sistémica y sistemática que deben desarrollar los Gobiernos para ampliar ahora sus responsabilidades de Estado, en el contexto de la protección de personas y patrimonios en sus fronteras nacionales electrónicas o digitales. Un concepto estratégico de los Gobiernos en el que hemos de ratificar que se requiere la comprensión y abordaje de las distintas variables, principalmente, las vulnerabilidades de las infraestructuras críticas de la nación, las garantías y derechos de los ciudadanos en el mundo online, la renovación de la Administración de Justicia en el entorno digital y la evolución de la inseguridad de la información en el contexto tecnológico y operacional. Por tanto, al hablar de ciberseguridad, hemos de hablar de la convergencia con la interconexión de los sistemas internos, la interdependencia con sistemas externos y la consolidación hacia estándares abiertos (IP). En este sentido, es absolutamente necesaria la convergencia de las seguridades que, aunque tradicionalmente se ha separado la seguridad física clásica de la seguridad lógica de las TIC, en el contexto actual no es posible trabajar con aproximaciones estancas. Una infraestructura crítica puede presentar vulnerabilidades frente a amenazas físicas y lógicas, no pudiendo considerar las salvaguardas de uno y otro tipo dentro de planes separados. Aunque las seguridades se clasifiquen como físicas o lógicas, la amplitud del concepto de infraestructura crítica, y la multiplicidad de sectores afectados, exige la necesidad de afrontar su protección desde un punto de vista integral y multidisciplinar. [23]

Es por ello que resulta imprescindible disponer de un Plan Director que integre todas las seguridades ya que, actualmente, los operadores de infraestructuras críticas han de seguir muchos planes de seguridad: estratégicos sectoriales, seguridad integral, seguridad del operador, protección de específicos, emergencia, continuidad de negocio, autoprotección, seguridad industrial, etcétera. Y todo ello, sin olvidar la dependencia que hay entre sectores en caso de un incidente, que implica la necesidad de coordinar e interrelacionar la respuesta de diferentes operadores ante los incidentes. [23]

Estrategia de Ciberseguridad

Construcción de la Resiliencia

El objetivo de cualquier estrategia de ciberseguridad es proteger la mayor cantidad posible de activos y, sin duda, los activos más importantes. Dado que no es factible protegerlo todo en igual medida, es importante identificar lo que es valioso y necesita una mayor protección, identificar las vulnerabilidades y, a continuación, priorizar y crear una arquitectura de defensa en profundidad que garantice la continuidad del negocio. Lograr la resiliencia consiste en gran medida en comprender y mitigar los riesgos para aplicar la protección adecuada en los puntos apropiados del sistema. Es esencial que este proceso esté estrechamente alineado con los objetivos de la organización porque las decisiones de mitigación pueden tener una grave repercusión en las operaciones. Idealmente, debería basarse en un enfoque de sistemas que involucre a las partes interesadas de toda la organización. [24]

Un concepto clave de la defensa en profundidad es que la seguridad requiere un conjunto de medidas coordinadas. Existen cuatro pasos imprescindibles para hacer frente al riesgo y las consecuencias de un ciberataque [24]:

- Comprender el sistema, lo que es valioso y lo que necesita más protección.
- Comprender las amenazas conocidas a través del modelado de amenazas y la evaluación de riesgos.
- Abordar los riesgos e implementar la protección con la ayuda de normas internacionales, que se basan en las buenas prácticas globales.
- Aplicar el nivel apropiado de evaluación de conformidad (ensayos y certificación) frente a los requisitos.

Enfoque Basado en Riesgo

Un enfoque de sistemas basado en el riesgo aumenta la confianza de todas las partes interesadas al demostrar no solo el uso de medidas de seguridad basadas en las buenas prácticas, sino también que una organización ha implementado las medidas de manera eficiente y efectiva. Esto significa combinar las normas correctas con el nivel correcto de evaluación de conformidad, en lugar de tratarlos como áreas distintas. El objetivo de la evaluación de la conformidad es evaluar los componentes del sistema, las competencias de las personas que lo diseñan, lo operan y lo mantienen, y los procesos y procedimientos utilizados para ejecutarlo. Esto puede significar el uso de diferentes tipos de evaluación de conformidad, que van desde la autoevaluación corporativa o la

confianza en las declaraciones de un proveedor hasta la evaluación y pruebas independientes de terceros, y la selección de la que sea más adecuada de acuerdo con los diferentes niveles de riesgo. En un mundo donde las amenazas cibernéticas son cada vez más habituales, ser capaz de aplicar un conjunto específico de normas internacionales combinado con un programa de certificación específico y mundial es un enfoque comprobado y altamente efectivo para desarrollar la resiliencia cibernética a largo plazo. Sin embargo, las normas y la evaluación de conformidad solo pueden tener un impacto máximo como parte de un enfoque basado en el riesgo basado en una evaluación integral de las amenazas y las vulnerabilidades. Este enfoque incorpora no solo la tecnología y los procesos, sino también las personas, lo que reconoce la función esencial de la formación. [24]

Muchas organizaciones basan sus estrategias de ciberseguridad en el cumplimiento de las normas y regulaciones obligatorias. Esto puede conducir a una mejor seguridad, pero no puede abordar las necesidades de las organizaciones individuales de manera integral. Las defensas más robustas se basan tanto en las normas “horizontales” como “verticales”. Las normas horizontales son genéricas y flexibles, mientras que las normas verticales satisfacen necesidades muy específicas.

Normas horizontales y verticales

La normativa horizontal es aquella que se aplica a un conjunto o familia de productos o a un sector en particular, a partir de definiciones de principios de carácter amplio; mientras que la normativa “vertical” tiene alcance para un producto específico.

Dentro de ellas podemos mencionar las normas que forman la serie ISO/IEC-27000, que son un conjunto de estándares creados y gestionados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrónica Internacional (IEC). Ambas organizaciones internacionales están participadas por multitud de países, lo que garantiza su amplia difusión, implantación y reconocimiento en todo el mundo. Las series 27000 están orientadas al establecimiento de buenas prácticas en relación con la implantación, mantenimiento y gestión del Sistema de Gestión de Seguridad de la Información (SGSI) o por su denominación en inglés *Information Security Management System* (ISMS). Estas guías tienen como objetivo establecer las mejores prácticas en relación con diferentes aspectos vinculados a la gestión de la seguridad de la información, con una fuerte orientación a la mejora continua y la mitigación de riesgos.

[12] Cada norma tiene reservado un número dentro de una serie que van desde 27000 hasta 27019 y de 27030 a 27044. [13]

La IEC 62443 es otra norma horizontal cuyo objetivo principal es facilitar el tratamiento de las vulnerabilidades de los IACS (*Industrial Automation and Control System*) frente a ataques informáticos y la aplicación de medidas que las mitiguen. Desde sus inicios, su propósito ha sido establecer un nexo entre la ciberseguridad y los IACS, definiendo una serie de requisitos mínimos para lograr niveles de seguridad cada vez más rigurosos que ayuden a mejorar la seguridad en entornos industriales. [14]

Tal como mencionamos, las normas horizontales se pueden complementar con las normas verticales para brindar soluciones a sectores específicos; como ser del sector nuclear, las redes de comunicaciones industriales, la automatización industrial y la industria marítima, entre otros.

Tratamiento de Riesgos

La gestión de riesgo se ha convertido en una práctica crítica en ciberseguridad. Consiste típicamente en dos sistemas de prácticas: una centrada en la evaluación de riesgos (identificación, análisis, evaluación del riesgo) y otra centrada en la gestión (aceptación, transferencia, tratamiento de riesgos).

El objetivo de la gestión de riesgos de ciberseguridad es avanzar y mantener un excelente estado de ciberseguridad basado en las necesidades, consideraciones y mejores prácticas únicas de la industria de la organización. Con una comprensión de la tolerancia al riesgo, las organizaciones pueden priorizar las actividades de ciberseguridad, permitiendo a las organizaciones tomar decisiones informadas sobre los gastos de ciberseguridad.

La implementación de programas de gestión de riesgos permite conocer los peligros que pueden afectar a la organización a nivel informático y como tratar los mismos según su probabilidad de ocurrencia e impacto. Para ello se deben contemplar lo siguiente:

1. Identificación de activos.
2. Identificación de amenazas y vulnerabilidades.
3. Identificar la probabilidad de ocurrencia y su impacto.

4. Definición del riesgo asociado en base a la disponibilidad, integridad y confidencialidad deseada.
5. Tratamiento del riesgo:
    - Aceptar el riesgo hasta un cierto umbral.
    - Mitigar el riesgo en base a la implementación de medidas detectivas, preventivas y/o correctivas.
    - Transferir el riesgo a un tercero (Seguro).
    - Anular el riesgo.

Este programa le permite a la organización conocer todos los activos relacionados con la información, identificando amenazas y vulnerabilidades que permitan definir los riesgos reales a los que se expone la información y los sistemas.

No disponer de las medidas apropiadas de seguridad expone a las organizaciones a sufrir situaciones graves que ocasionen pérdidas importantes (como periodos de inactividad o pérdida de datos sensibles).

Marco de Ciberseguridad

Este enfoque de la gestión del riesgo de ciberseguridad necesita garantizar que se implementen medidas de protección basadas en la integración de información de amenazas, vulnerabilidades identificadas y una estrategia de reducción de riesgos, promoviendo prácticas organizacionales sólidas que incluyen la planificación, los procedimientos, la priorización presupuestaria y la asignación de recursos clave (humanos, monetarios y técnicos). [1]

Para el desarrollo de una política o marco de CIIP sostenible se deben considerar [1]:
1. Asegurar una división clara de las responsabilidades: Dado que CIIP involucra a múltiples partes interesadas, con diferentes intereses y puntos de vista con respecto a ella, se requiere un fuerte liderazgo del gobierno para coordinar las múltiples agencias que deben participar en el proceso de desarrollo de una estrategia CIIP, así como en su implementación. La estrategia también debe determinar claramente las diversas responsabilidades de las CIIP, tanto en operadores públicos como privados, así como en los diferentes sectores. También deberían asignarse plazos y presupuestos. El "Plan Nacional para la Protección de Infraestructuras Críticas de Información"', así como la Recomendación del Consejo de la Organización para la Cooperación y el Desarrollo

Económicos (OCDE) sobre la Protección de Infraestructuras Críticas de Información son guías útiles para lograrlo.

2. Participar en un enfoque holístico: Una política eficaz de CIIP debe adoptar un enfoque holístico que considere aspectos y puntos de vista técnicos, económicos, organizacionales, de cumplimiento de la ley y de políticas de seguridad. La razón de esto es que la operación y protección de CIIP implica una sección representativa de actores con diferentes roles. Por ejemplo, en el caso de un incidente cibernético, se puede llamar al equipo de respuesta para contener el evento; sin embargo, si el incidente se identifica como un ataque intencional, se puede llamar a la policía u otro personal de seguridad para investigar. Por lo tanto, la política debe delinear roles claros de responsabilidad y canales de comunicación para todos los actores involucrados para asegurar la coordinación y una respuesta estratégica.

3. Desarrollar marcos, pautas y procedimientos: Los gobiernos deberían, mediante un proceso consultivo abierto, elaborar procedimientos y directrices claros para los procesos y aspectos clave de la CIIP. Los marcos deben estar integrados en la gestión de riesgos, al tiempo que se asegure que los operadores CII puedan adoptar la última tecnología, como la computación en la nube, para lograr las eficiencias necesarias. Un marco de gestión de riesgo recomendado, por ejemplo, incluye el marco de gestión de NIST, que enfatiza que la gestión del riesgo organizacional es un elemento clave en el programa de seguridad de la información de la organización y proporciona un marco efectivo para seleccionar los controles de seguridad apropiados para un sistema que permita proteger a las personas, las operaciones y los activos de la organización.

4. Establecer líneas de base de seguridad: Las líneas de base de seguridad son un conjunto fundamental de políticas, resultados, actividades, prácticas y controles destinados a ayudar a gestionar el riesgo de seguridad cibernética. Las líneas de base de seguridad son particularmente útiles para mejorar la ciberseguridad, ya que deben abarcar una serie de riesgos que suelen aplicarse en ciertos entornos. La mayoría de los riesgos que enfrentan los gobiernos y las empresas son similares, por lo que la mayoría de las actividades "básicas" o de gestión de riesgos también son similares. Por ejemplo, todas las organizaciones deben pensar en revisar y actualizar regularmente las evaluaciones de riesgos, administrar cómo se accede a los recursos para evitar usuarios o comportamientos no autorizados, y planificar y mitigar el impacto de los incidentes.

5. Soporte de soluciones dinámicas: Debido a la continua evolución del panorama cibernético, cualquier solución y enfoque CIIP debe ser dinámica y de naturaleza flexible.

La situación regular y frecuente y las reevaluaciones de riesgos son importantes para mantener soluciones actualizadas y garantizar mejoras constantes. Un ejemplo de cómo garantizar ese enfoque es el Programa Voluntario Cibernético Comunitario de Infraestructura Crítica (C3 - pronunciado 'C-Cubed'), que fue establecido por el Departamento de Seguridad Nacional de los Estados Unidos. El Programa C3 se estableció para ayudar a los propietarios y operadores de infraestructuras críticas a utilizar el Marco NIST para gestionar sus riesgos cibernéticos.

6. Fomentar la confianza: Como se ha señalado anteriormente, las alianzas público-privadas entre las CII y el gobierno son esenciales para la CIIP y deben basarse en un intercambio abierto de información y experiencia. Para facilitar dicho intercambio, la confianza entre las partes es esencial. La generación de confianza puede ser particularmente desafiante cuando las alianzas implican empresas competidoras que tienen un interés particular en mantener sus activos y posibles problemas de seguridad de los competidores. Es fundamental que los gobiernos ayuden a facilitar estos intercambios y ayuden a proteger sectores enteros en lugar de solo empresas individuales.

7. Crear proyectos que demuestren beneficios mutuos: Las alianzas público-privadas, así como las redes nacionales e internacionales, deben tener como objetivo el intercambio de información y el apoyo mutuo con respecto a las amenazas cibernéticas. Sin embargo, estos son difíciles de despegar. De hecho, para que el intercambio de información sea exitoso a largo plazo, sus beneficios deben ser claros para todas las partes involucradas. Por lo tanto, es importante que todos los participantes, ya sean públicos o privados, compartan cualquier información de inteligencia y descubran que podrían tener que habilitar la seguridad del grupo en su conjunto.

8. Desarrollar mecanismos de alerta temprana: Los sistemas de alerta temprana desempeñan un papel clave en la prevención de la propagación de ataques cibernéticos y en la minimización del impacto de las amenazas cibernéticas. Por lo tanto, tanto el sector público como el privado deberían priorizar las funciones que permiten mecanismos de alerta temprana. El intercambio de información entre las diferentes CII, así como con el gobierno, por ejemplo, aumentaría la conciencia situacional de los operadores de las CII, les permitiría detectar un ataque potencial y frustrarlo o mitigar su impacto.

9. Invertir en recursos humanos y técnicos: La CIIP requiere empleados con habilidades particulares. La identificación, el reclutamiento y la retención de expertos en ciberseguridad es crucial para garantizar un alto nivel de seguridad y protección continua. Además, es importante que las organizaciones entiendan que las habilidades

de ciberseguridad no son un término monolítico y que pueden necesitar diferentes expertos para ayudarles con la gestión de riesgos y la seguridad informática tradicional, por ejemplo Además, las organizaciones deberían proporcionar capacitación periódica de seguridad para todo el personal, ya que la falta de higiene en materia de seguridad cibernética en toda la organización a menudo es donde las entidades son más vulnerables. Además, garantizar que los empleados estén equipados con los recursos técnicos necesarios para llevar a cabo su trabajo de manera efectiva es igualmente importante. Como resultado, se recomienda una asignación presupuestaria suficiente para productos y servicios de ciberseguridad técnica.

10. Mejorar la resiliencia cibernética: Los estados y las empresas deberían implementar una estrategia de resiliencia cibernética para garantizar la continuidad del negocio y del servicio en caso de un incidente de seguridad. Es fundamental que vayan más allá de centrarse en la ciberseguridad, pero se aseguren de que estén preparados para que cuando ocurra una crisis, sean receptivos a ella y sean capaces de reinventar su estructura de TIC frente al estrés sostenido y las interrupciones agudas. En otras palabras, ser ciberresilientes asegurará que las empresas o los servicios puedan continuar estando disponibles y operar a pesar del impacto de las amenazas cibernéticas o de los desastres naturales y causados por el hombre.

11. Participar en una red internacional: Como las amenazas cibernéticas no tienen fronteras físicas, la cooperación entre organizaciones y países es esencial para la prevención, identificación, respuesta y recuperación efectivas. Identificar y participar en estructuras y marcos internacionales existentes, por ejemplo, a través de la OEA, Meridian o FIRST19, puede ayudar a los gobiernos a comprender el entorno de amenazas y mantenerlos al tanto de las últimas tendencias de ciberseguridad y mejores prácticas.

Framework para Infraestructuras Criticas según NIST

En 2018 el NIST público un *framework* de trabajo estratégico para mejorar la ciberseguridad de las infraestructuras críticas de los Estados Unidos, específicamente denominado CSF (*NIST Cybersecurity Framewok*). De manera resumida, este marco posee los siguientes objetivos [9]:

- Describir el estado de la ciberseguridad y resultados deseados.
- Marco que sea comprensible para todos.
- Abarca tanto la prevención como la respuesta a un incidente.

El *framework* de CSF está estructurado sobre la base de otros tres *framework* [9]:

- Marco básico (*Framework Core*),
- Niveles de implementación del marco (*Framework Implementation Tiers*).
- Perfiles del marco (*Framework Profiles*).

Figura 8 – Marco CSF de NIST [9]

Gestión de Incidentes de Seguridad (GIS)

La Gestión de Incidentes de Seguridad (GIS) conforma uno de los componentes clave vinculados a la CIIP, y como extensión del resto de los componentes de CI. La GIS requiere del establecimiento de una capacidad de respuesta basada en una serie de servicios globales que permitan responder a eventos e incidentes de seguridad de manera adecuada y eficiente, permitiendo sostener el nivel de calidad operativa deseado en base a los requerimientos de los diferentes sectores implicados y al riesgo de seguridad presente. La capacidad de la GIS hace uso de una serie de procesos para el tratamiento de eventos e incidentes de seguridad en una concepción extremo-a-extremo soportada por el contexto jurídico establecido y por las diferentes políticas de seguridad vinculadas a los sectores público y privado. La GIS requiere además de la presencia de esquemas claros de roles y responsabilidades, de herramientas adecuadas, de recursos de infraestructura y finalmente de un plantel de especialistas de seguridad dedicados a llevar adelante todos los procesos involucrados de tal manera que todas las actividades desarrolladas resulten repetibles en el tiempo. [4]

Modelo

A continuación, se presenta una síntesis de los cinco procesos fundamentales que hacen al modelo de GIS [4]:

- **Preparación**: Establecimiento, sostenimiento e implementación de un esquema de trabajo y de mejora continua sobre el grupo de respuesta a incidentes de seguridad, o sobre las áreas afines.
- **Protección**: Implementación de planes de acción y de mejora en cuanto a protección de la infraestructura con el fin de mitigar los riesgos de seguridad.
- **Detección**: Identificación y reporte de eventos de seguridad en el momento de ocurrencia, tratando en cada caso de inferir la posibilidad de futuros eventos relacionados.
- **Clasificación** (*Triage*): Categorización, priorización, correlación y finalmente asignación de cada evento a un analista para su posterior investigación e implementación de respuestas adecuadas.
- **Respuesta**: Consiste en la planificación, coordinación e implementación de los procedimientos de respuesta a incidentes.

La siguiente figura muestra un esquema general de los principales procesos asociados a la capacidad de la GIS.

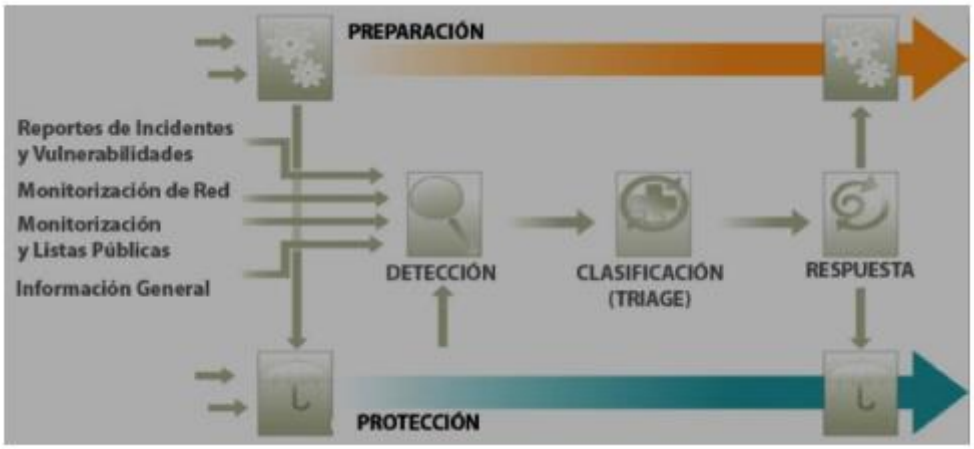


Figura 9 – Procesos Asociados a las Capacidades del GIS [4]

Los procesos del modelo pueden ser interpretados de la siguiente manera [4]:

- **Preparación y Protección**: procesos continuos en el tiempo, requieren de la puesta en escena de un conjunto grande de recursos tales como políticas, procedimientos, personal, tecnologías e infraestructura de tal manera que las

actividades de gestión de incidentes puedan llevarse adelante a tiempo, de forma coordinada y efectiva. Es interesante visualizar el hecho que los procesos de Preparación y Protección soportan la implementación y operación de los otros procesos del sistema.

- **Los procesos de Preparación y Protección** obedecen a requerimientos o políticas que establecen reglas a cumplir sobre la estructura y funcionalidad de dichos procesos.
- **El nexo presente entre los procesos Preparación y Protección** establece una realimentación de información por medio de recomendaciones de mejora destinada a optimizar la infraestructura de cómputo. La información realimentada es obtenida por medio de procedimientos de análisis *postmortem* en el proceso de Preparación.
- **Los procesos de Detección, Clasificación y Respuesta** son presentados en orden, según el flujo de información vinculado a incidentes es procesado. Los eventos que llegan al proceso de Detección deben ser sometidos a análisis para detectar si deben o no ser sujetos a más análisis y evaluaciones. Si en base a la información procesada en la etapa de Detección (reportes de vulnerabilidades o incidentes, un evento sospechoso, etc.) se determina que una respuesta es necesaria, la información es pasada al proceso de Respuesta.
- **Los procesos de Protección y Detección** deben interactuar bajo la premisa de que si un incidente o una vulnerabilidad es detectada como consecuencia de una evaluación sobre la infraestructura (parte de un proceso de Protección), ésta deberá ser informada al proceso de Detección para su posterior tratamiento.
- Finalmente, **el proceso de Respuesta** deberá interactuar con los procesos de Preparación y de Protección, según corresponda. En cuanto a la relación con el proceso de Preparación, la información pasada por el proceso de Respuesta tiene como objetivo la mejora de procesos mediante la adopción de análisis *postmortem*. Por otro lado, en cuanto a la relación con el proceso de Protección, la información pasada por el proceso de Respuesta tiene como objetivo generar las acciones de respuesta.

Resulta claro que la implementación de la GIS no solo requiere de la aplicación de tecnología para la resolución de incidentes de seguridad, sino que requiere del establecimiento de un plan de acción y de un conjunto de procesos que resulten consistentes, repetibles y de gran calidad.

Consideraciones sobre la GIS

Como capacidad global, la GIS deberá incorporar elementos de diferentes unidades operativas por lo que resultará imprescindible contar con un plan que defina las interacciones entre los componentes del sistema de tal manera de optimizar la forma en que los diferentes incidentes son manejados. Como mínimo, el plan para la GIS deberá contemplar [4]:

- Forma de integración de los procesos y estructuras existentes a la GIS,
- Fortalecimiento y mejora de las capacidades de cada uno de los componentes de tal manera que puedan manejarse adecuadamente los eventos de seguridad con el fin de garantizar la confidencialidad, la integridad y la disponibilidad de los activos de información vinculados a la CII,
- Soportar y complementar los planes existentes de continuidad del negocio o de recuperación de desastres siempre que resulte apropiado,
- Complementar y enriquecer las políticas de negocios y de TI vinculadas con aspectos de seguridad,
- Extender al máximo el alcance de los sistemas de comando y control, establecer roles y responsabilidades e incorporar facilidades de trazabilidad de actividades,
- Conformar la GIS como parte de la estrategia global de protección, y
- Contemplar el establecimiento de procesos para:
    - detectar y clasificar eventos,
    - categorizar y priorizar,
    - notificar y comunicar,
    - analizar y responder,
    - colaborar y coordinar, y finalmente
    - mantener y por trazar eventos e incidentes en base a registros.

Implementación de la GIS

Los procesos y las tareas desarrollados en la GIS en el marco de CIIP deben contemplar desde el inicio una perspectiva global que permita integrar a todos los actores independientemente del sector al que pertenezcan en base a conceptos de Ingeniería correspondientes a las áreas de Seguridad de la Información y Resiliencia de Sistemas. Desarrollar tal perspectiva requiere que se identifiquen perfectamente cada uno de los siguientes componentes del sistema [4]:

- Los objetivos de negocio de cada componente de las CII,

- Las áreas intervinientes en la capacidad de GIS,
- La forma de implementación de las comunicaciones entre áreas, contemplando siempre las singularidades por sector,
- Los mecanismos de interacción entre áreas,
- Los esquemas de ejecución de acciones en el marco de las diferentes áreas operativas,
- La forma en la que se relacionará cada uno de los procesos con el modelo global de la GIS,
- Los mecanismos de intercambio de información, y finalmente,
- Los métodos de coordinación de las diferentes acciones.

El primer paso en vías de la implementación de una capacidad la GIS consiste en identificar a las organizaciones, áreas y recursos humanos apropiados para cada tipo de procedimiento involucrado y hacerlas parte del sistema en base a un esquema de roles y responsabilidades perfectamente definido. La selección del personal idóneo para formar parte del GIS es quizás la tarea más desafiante del proyecto. El propósito de cada grupo operativo involucrado en la GIS debe ser cuidadosamente planeado y documentado. Es importante que todos los procesos que vayan a ser incorporados al sistema de GIS puedan ser modelados mediante diagramas de procesos con el fin de abstraer los componentes esenciales para su análisis. El proyecto de implementación para la GIS requiere de la definición de flujo de trabajo o *workflows* que especifiquen de manera simple y clara como un incidente fluye por el modelo, es decir; por cada uno de sus procesos de tal manera que pueda definirse claramente quién lleva adelante cada tarea del plan, de qué manera, en qué orden y con qué requerimientos de tiempo. Los flujos de trabajo evidencian las interacciones y las dependencias entre las tareas y las actividades de un proceso. Realizar un mapa del sistema de GIS en base a la modelización de su estructura permite obtener una visión de alto nivel de todas las actividades, de los roles y de las responsabilidades, de la tecnología, de las interfaces y de las dependencias que se dan en todo proceso de respuesta a incidentes; y como estos se relacionan y dependen unos de otros. Es esencial que se defina un sub proceso Forense a través del cual se genera análisis *postmortem* de todos los incidentes clave con el objetivo de mejorar las estrategias de protección de la infraestructura y las políticas y procedimientos de seguridad y respuesta. Es recomendable ejecutar ejercicios de simulación periódicamente para asegurar que todos los involucrados sepan cómo reportar los incidentes y finalmente, como responder, sobre todo en contextos de crisis. [4]

GIS como formador de valor para la CIIP

En síntesis, el modelo de GIS puede constituirse en un componente clave en la CIIP ya que permite desarrollar e implementar un conjunto de procesos de seguridad consistentes y confiables destinados a soportar la identificación, detección, análisis y respuesta a incidentes de seguridad en base a una serie de procesos de calidad soportados por personas, tecnologías de la información y las comunicaciones de manera eficiente y sostenible. Desde un punto de vista estratégico y funcional, la GIS ayuda a establecer las garantías necesarias que permiten asegurar que la CII seguirá operando de tal manera que pueda alcanzar su misión, incluso en presencia de riesgo operativo producto de fallas internas de los sistemas, de acciones accidentales o deliberadas de personas internas o externas, o de eventos externos. La misión final de la GIS consiste en garantizar "Resistencia Operacional" a la CII de la Nación en base a la colaboración entre los sectores público y privado, y a un adecuado marco de gestión del riesgo vinculado principalmente a tareas de Gestión de Seguridad (GS), de Continuidad del Negocio y Recuperación de Desastres (CN/RD), y finalmente de las operaciones asociadas a las áreas de TI. La GIS establece las bases sobre las cuales, independientemente del sector y del área del que se trate, se pueda trabajar en conjunto para sostener el concepto de resistencia operativa. [4]

Consejos para Proteger Infraestructura Critica

Los ataques cibernéticos pueden causar costosas interrupciones en las operaciones de infraestructura crítica y efectos en cadena desastrosos para la economía. A medida que las empresas avanzan y automatizan su infraestructura de TI, la brecha cada vez mayor entre los sistemas de tecnología de la información (TI) y tecnología operativa (TO) hace que sea importante que los proveedores de infraestructura crítica tomen medidas proactivas agresivas. Para que las organizaciones de infraestructura crítica se protejan a sí mismas y a sus clientes de manera eficaz, deben adoptar un enfoque múltiple.

Para ello, compartimos una serie de aspectos de seguridad para minimizar los riesgos de sectores críticos [5] [10]:

- **Higiene cibernética:** Una buena higiene cibernética tanto para la TO como para la TI.
    - Los controles de segmentación, parches de firmware / software, autenticación multifactor (MFA, por sus siglas en inglés), gestión de

contraseñas y gestión de activos son todos importantes para proteger los entornos de TO.

- Mantener la conciencia del problema y de las muchas formas en que su empresa podría ser vulnerable a un ataque. Evitar contraseñas simples, haciendo cumplir la autenticación de factores múltiples y aplicando métodos de autenticación alternativos (por ejemplo, gesto o PIN).
- Ser proactivos en la recopilación de información sobre los ataques recientes y en la comunicación de esa información.
- Mantener la infraestructura actualizada y libre de vulnerabilidades, tanto de hardware como de software.
- Diseñar planes de respuesta ante incidentes, que sean claros y objetivos.
- Implementar un modelo Zero Trust y seguridad en capas.
- Manejar medidas de protección reactivas para minimizar el impacto (backup de información o plan de recuperación de desastre).
- Revisar los sistemas en busca de vulnerabilidades, especialmente aquellos que tengan agujeros de seguridad reportados y conocidos desde hace tiempo.
- Controlar los medios extraíbles es esencial en una infraestructura.
- Controlar las redes utilizadas en estas infraestructuras y, en aquellos casos que lo requieran, aisladas del exterior.
- Controlar las PC al que están conectados los controladores lógicos programables (o PLC). Son estos dispositivos conectados a Internet los más sensibles, ya que pueden proporcionar acceso a un atacante.
- Imponer políticas de seguridad que controlen el acceso a datos confidenciales y limiten el acceso de la red corporativa a usuarios, ubicaciones, dispositivos y Sistemas operativos (SO) apropiados.
- No trabajar en zonas Wi-Fi públicas donde los atacantes puedan espiar sus comunicaciones, capturar inicios de sesión y contraseñas, y acceder a sus datos personales.

- **Colaboración: es clave para combatir el ciberdelito.**
  - Formar parte de comunidades que permitan compartir inteligencia sobre amenazas con pares, proveedores externos y las fuerzas del orden para que todos podamos estar mejor preparados para abordar los riesgos.
- **Educación:** el 88% de todas las filtraciones de datos son causadas por errores humanos.

  - Es fundamental que los empleados que manipulan o tienen acceso al sistema comprendan que la seguridad es una responsabilidad compartida y cómo pueden potencialmente poner a su empresa en riesgo.
  - Elaborar planes de capacitación sobre los riesgos que existen y el modo en que operan los ataques.
- **Tecnología:** Invertir en tecnología para anticipar, prevenir o minimizar los ataques; sus inversiones deben estar bien alineadas con las necesidades futuras de la empresa**.**
  - Anticipe hacia dónde se dirige la empresa, comprenda los riesgos e invierta en consecuencia. Se pronostica que el costo del daño global del *ransomware* superará los $265 mil millones para 2031, así que invierta sabiamente.
  - Disponga de medidas de protección tecnológicas, como soluciones de seguridad integrales que incluyan antivirus, antimalware, firewall y otros sistemas de detección proactiva.
  - Implemente no solo soluciones de *Threat Intelligence*, sino que además soluciones más proactivas, como *Threat Hunting*, para evitar caer en ataques que todavía no han sido detectados.
- **Eficiencias operativas:** A medida que realiza inversiones en tecnología, asegúrese de trabajar en estrecha colaboración con las partes interesadas para que comprenda el impacto de sus decisiones en las unidades de negocio y ellos comprendan la urgencia en torno a la protección de datos y aplicaciones.
  - La búsqueda proactiva de amenazas y la gestión de vulnerabilidades son operaciones de seguridad importantes para priorizar la mitigación de riesgos.

LEGISLACIÓN Y NORMATIVA. ANTECEDENTES

Consideraciones Generales sobre Legislación

A raíz de los problemas vinculados a la protección de la Infraestructura Crítica debe pensarse en la adopción de una legislación apropiada que permita garantizar la integridad, confidencialidad y disponibilidad de la misma. En el contexto de CIIP, los aspectos jurídicos deberán acompañar a la ciencia de la Seguridad de la Información con el objetivo común de lograr la seguridad de los ciudadanos y el bienestar económico

del país. Es necesario que los países comprendan la necesidad de crear una conciencia y una cultura asociados a la Seguridad de la Información, la cual será de ayuda para entender las implicancias relacionadas a las amenazas crecientes y poder ayudar a protegerlas legalmente, estableciendo funciones legislativas legítimas. Debido al carácter distribuido de muchas de los componentes vinculados a las CII, e incluso a la utilización de recursos de infraestructura compartidos con el resto del mundo como es el caso de Internet, se requiere la cooperación internacional para facilitar la creación de un marco legal para combatir el crimen. Las medidas legales, técnicas, procesales, estructurales y orgánicas, necesitan ser emprendidas a nivel nacional, regional y multinacional, por lo que cada nación deberá colaborar estrechamente con sus socios estratégicos en el abordaje del problema para identificar los actuales desafíos, considerando las amenazas futuras, y proponiendo estrategias globales. Esta responsabilidad compartida requiere de acciones coordinadas para la prevención, respuesta y recuperación de las funciones y actividades tras un incidente que afecte a los sectores público o privado, e incluso a los mismos ciudadanos. [4]

Un claro ejemplo es la “Cumbre Mundial sobre la Sociedad de la Información” (CMSI), allí se reconocieron los riesgos reales y significativos planteados por una seguridad inadecuada en CII. En esta cumbre, los líderes mundiales y los gobiernos allí reunidos designaron a la ITU (Unión de Telecomunicación Internacional) como el organismo dedicado a la creación de normas de seguridad en la utilización de las TIC. La ITU provee un conjunto de herramientas legislativas que ayudan a establecer normas legales en el mundo, relacionadas con la Ciberseguridad. La ITU lanzó la “Agenda sobre Ciberseguridad Global” (GCA de las siglas en Inglés de Global Cibersecurity Agency), con la colaboración de gobiernos, industrias, organizaciones regionales, instituciones académicas y de investigación. La GCA constituye un marco de alcance mundial con el fin de coordinar respuestas internacionales a los retos planteados por la seguridad en infraestructuras basadas en TIC, con el objetivo de proponer estrategias globales en base a trabajos e iniciativas existentes, generando mayor confianza y seguridad en la sociedad para la utilización de las TIC. [4]

La GCA tiene siete objetivos estratégicos principales basados en las cinco áreas de trabajo siguientes [4]:

1. Medidas Legales: Estrategias para desarrollar un marco legislativo del cibercrimen, el cual sea operable y aplicable internacionalmente.

2. Medidas Técnicas y de Procedimiento: Estrategias para desarrollar un marco de trabajo para protocolos de seguridad, estándares, esquemas aplicables a software y hardware.

3. Estructuras Institucionales: Estrategias globales para la creación de estructuras políticas e institucionales contra el cibercrimen. Los sistemas deberán predecir, detectar, responder y gestionar la crisis ante un incidente.
4. Construir Capacidades: Estrategias globales para crear mecanismos de creación de capacidades humanas e institucionales en los puntos I, II y III. Con el fin de aumentar la conciencia, transferir los conocimientos, y colocar a la Ciberseguridad en la agenda de los gobiernos.
5. Cooperación Internacional: Proponer un marco de trabajo para el diálogo internacional, la cooperación y la coordinación al momento de abordar las ciberamenazas.

A partir de estas áreas, los objetivos estratégicos para desarrollar el marco legal son [4]:
1. Elaborar estrategias para desarrollar un modelo legislativo del Cibercrimen, que sea aplicable en el mundo, y que interopere con medidas legislativas nacionales e internacionales.
2. Elaborar estrategias globales para la creación de estructuras organizacionales y políticas relacionadas con el cibercrimen.
3. Desarrollar una estrategia para establecer los mínimos criterios de seguridad y acreditar esquemas aplicados al hardware y software.
4. Desarrollar estrategias de creación para un marco global mirando, cuidando y respondiendo a incidentes, asegurando una correcta coordinación con las nuevas iniciativas y si hubiera, con las existentes.
5. Desarrollar una estrategia global para la creación de un sistema de identidad digital genérica y universal, necesitando estructuras organizacionales para asegurar el reconocimiento de credenciales digitales a través de distintas áreas geográficas.
6. Desarrollar una estrategia global para facilitar la construcción de capacidades humanas e institucionales reforzando el conocimiento y la habilidad en todos los sectores y áreas.
7. Proponer un marco global con múltiples colaboradores, teniendo como estrategia la cooperación internacional, el diálogo y la coordinación en todas las áreas participantes.

Desarrollar legislaciones adecuadas dentro de un marco jurídico resulta un factor esencial para combatir el ciberdelito. Se requiere la elaboración de leyes penales, ante actos criminales como el fraude informático, la denegación de servicios, acceso ilegal, violaciones del derecho de la propiedad intelectual, usurpación de identidad, pornografía infantil. En este sentido, en nuestro país la Ley 25.326 de Protección de Datos

Personales sancionada en el año 2000 ofrece un marco legal para la protección integral de los datos de las personas y aplica tanto al sector público como al privado. Se encarga de proteger aspectos de Privacidad. Por otro lado, la Ley 26.388 establece una reforma del Código Penal en materia de Delitos Informáticos por medio de la derogación y modificación de algunos incisos introducidos por el art. 32 de la Ley 25.326 al Código Penal. Dicha ley aplica penas a delitos como [4]:

- **La Pornografía y Exhibición Infantil**: Comercio, publicación, facilitación, divulgación o distribución, de actividades sexuales explícitas a menores de edad.
- **La Violación de Secretos y de la Privacidad**:
    - Acceso indebido, apoderación y publicación de una comunicación electrónica, cartas, documentos.
    - Acceso a un sistema o dato restringido sin el correspondiente permiso.
    - Violación y modificación a sistemas de confidencialidad y banco de datos personales.
    - Alteración del normal funcionamiento de un sistema informático o la transmisión de datos.

Si bien existen leyes aplicables a actos cometidos fuera de ambientes de las TIC, estas mismas leyes en muchas oportunidades no son aplicables al ámbito cibernético. Se necesitarán herramientas e instrumentos jurídicos necesarios para investigaciones en el ciberdelito. Como se especificó anteriormente, las amenazas pueden originarse en cualquier lugar del mundo, enmascarando la identidad del autor tras la red, por tal motivo, las herramientas de investigación no serán las mismas usadas en delitos comunes, y las leyes necesitarán asistencia jurídica mutua, para aplicarse en el lugar de origen del delito. No todos los sistemas jurídicos del mundo reconocen los potenciales abusos de las nuevas tecnologías, por lo tanto, no incluyen las modificaciones necesarias en las actuales leyes penales nacionales. En base a esto resulta fundamental comprender la creciente complejidad introducida por las TIC y trabajar para realizar los ajustes jurídicos pertinentes. El proceso de ajuste consta de tres etapas [4]:

- En la primera etapa se deberá reconocer la actividad delictiva asociada a las nuevas tecnologías. Se necesitará de autoridades nacionales competentes que cuenten con departamentos específicos calificados para investigar ciberdelitos, como por ejemplo el “CERT *Coordination Center*” (Equipo de respuesta de emergencias en sistemas computacionales y redes de EE: UU) que funciona en

la Universidad de Carnegie Mellon, Equipos de respuesta a incidentes informáticos en organismos privados, etc.

- La segunda etapa consiste en identificar los problemas en el Código Penal, necesarios para garantizar eficaces bases jurídicas. Se necesita comparar situaciones dispuestas jurídicamente, con los nuevos tipos de delitos. Las leyes existentes pueden cubrir delitos que no actúen sobre la cibernética.
- La tercera etapa consiste en redactar una nueva legislación. Tomando como punto de partida las experiencias anteriores, puede resultar difícil para las autoridades nacionales llevar a cabo este proceso de redacción relativo a los ciberdelitos sin la cooperación internacional.

Sin la armonización internacional de disposiciones jurídicas y penales, luchar contra el ciberdelito será de gran dificultad debido a la incompatibilidad de legislaciones propias de cada país. En consecuencia, el trabajo en conjunto sobre las leyes nacionales genera un beneficio enorme ya que permite reutilizar la experiencia de otros países y contar con asesoría jurídica de expertos internacionales.

Europa

De forma especial, el Consejo Europeo en el año 2004 pidió a la Comisión correspondiente que elaborase una estrategia global para una mayor protección de las infraestructuras críticas. En respuesta a dicha petición la Comisión publicó, el 22 de octubre de 2004, una Comunicación que describe las acciones que la Comisión adopta actualmente para proteger las infraestructuras críticas y propone medidas adicionales para consolidar los instrumentos existentes. Así el proyecto de la Comisión de proponer un Programa Europeo para la Protección de las Infraestructuras Críticas (PEPIC) y una Red de Alerta en relación con las Infraestructuras Críticas (CIWIN) fue finalmente aceptado en el Consejo Europeo de 16 y 17 de diciembre de 2004, tanto en las conclusiones del Consejo relativas a la prevención, preparación y respuesta ante ataques terroristas, como en el programa de solidaridad que el Consejo aprobó el 2 de diciembre de 2004. Como principal prioridad, el 15 de septiembre de 2005 fue aprobada la Decisión C/2005/3179 sobre financiación de un proyecto piloto relativo a acciones preparatorias para reforzar la lucha contra el terrorismo, puesto que el riesgo de ataques terroristas catastróficos contra infraestructuras críticas se considera en aumento y, como las consecuencias de un ataque contra los sistemas industriales de control de las infraestructuras críticas podrían ser muy variadas, aunque se da por supuesto que un

ciberataque podría no causar víctimas, pero provocaría la pérdida de servicios de infraestructura vitales. Por todo ello, los estados miembros deberán, por tanto, determinar sus respectivas infraestructuras críticas, según una fórmula armonizada a escala de la UE, conjuntamente con los organismos o personas responsables de su seguridad. España en el año 2007 creó el plan para proteger las principales infraestructuras críticas (más de 3.500) de los sectores de las telecomunicaciones, energía, transportes, agua y sanidad, principalmente. De su coordinación se encarga el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC). [4]

Las principales competencias del CNPIC son las siguientes [17]:

- Recolectar, analizar, integrar y evaluar la información aportada por las instituciones públicas, los servicios policiales, y sectores estratégicos.
- Evaluar las amenazas y analizar los riesgos sobre las instalaciones estratégicas.
- Diseñar y establecer la información, la comunicación y los mecanismos de alerta.
- Coordinar las administraciones españolas con los respectivos programas de la Unión Europea.

Legislación Europea

Directiva 2008/114/CE DEL CONSEJO de 8 de diciembre de 2008 sobre [17]:

- Identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.
- Constituye un importante paso en la cooperación en esta materia en el seno de la Unión.
- Se establece que la responsabilidad principal y última de proteger las infraestructuras críticas europeas corresponde a los Estados miembros y a los operadores de las mismas.
- Se determina el desarrollo de una serie de obligaciones y de actuaciones por dichos Estados, que deben incorporarse a las legislaciones nacionales.

Legislación Española y Otros Documentos de Utilidad

Ley 8/2011 de 28 de abril por la que se establecen medidas para la protección de las infraestructuras críticas [17]:

- La finalidad de esta norma es establecer las medidas de protección de las infraestructuras críticas.
- Estas medidas deben proporcionar una base adecuada sobre la que se asiente una eficaz coordinación de las Administraciones Públicas y de las entidades y organismos gestores o propietarios de infraestructuras que presten servicios esenciales para la sociedad con el fin de lograr una mejor seguridad para aquellas.

Real Decreto 704/201 de 20 de mayo por el que se aprueba el Reglamento de protección de las infraestructuras críticas. [17]

La finalidad de este decreto es desarrollar, concretar y ampliar los aspectos contemplados en la Ley 8/2011 de 28 de abril. Está dividido en cuatro grandes apartados:

- Título I que contiene las cuestiones generales relativas a su objeto y ámbito de aplicación.
- Título II que está plenamente dedicado al Sistema de Protección de Infraestructuras Críticas y desarrolla las previsiones legales relativas a los órganos creados por la Ley.
- Título III que se encarga de la regulación de los instrumentos de planificación.
- Título IV que consagra la seguridad de las comunicaciones y a las figuras del Responsable de Seguridad y Enlace y del Delegado de Seguridad de la infraestructura crítica.

Plan de seguridad del operador (PSO). Con este documento se pretende que el Operador designado como crítico o estratégico cumpla el Real Decreto 704/2011 [17]:

- Estableciendo los contenidos mínimos sobre los que se debe de apoyar un operador crítico a la hora del diseño y elaboración de su PSO.
- Además, pretende orientar a aquellos operadores que hayan sido o vayan a ser designados como críticos en el diseño y elaboración de su respectivo Plan, con el fin de que éstos puedan definir el contenido de su política general y el marco organizativo de seguridad.

- En otras palabras, el PSO definirá la política general del operador para garantizar la seguridad integral del conjunto de instalaciones o sistemas de su propiedad o gestión.

Guía de Buenas Prácticas para la elaboración de los Contenidos Mínimos de los Planes de Seguridad del Operador [17]:

- Con este documento se pretende orientar a aquellos operadores designados como críticos en la elaboración de su PSO, sirviendo como complemento a las Resoluciones del Secretario de Estado de Seguridad sobre Contenidos Mínimos del PSO.
- Se trata de un documento de carácter voluntario que no incluye requisitos adicionales a los establecidos por la legislación vigente o por la Resolución mencionada previamente.
- En esta guía se incluyen una serie de Anexos (ejemplos, relación de estándares y buenas prácticas, etc.) que podrán ser de ayuda a los operadores críticos para la confección de alguno de los puntos de los contenidos mínimos del Plan de Seguridad del Operador.

Plan de protección específico (PPE). Con este documento se pretende que el Operador designado como crítico o estratégico cumpla el Real Decreto 704/2011 [17]:

- Estableciendo los contenidos mínimos sobre los que se debe apoyar el operador crítico a la hora de elaborar su respectivo PPE en las instalaciones catalogadas como críticas.
- Los PPE son los documentos operativos donde se definen las medidas concretas a poner en marcha por los operadores críticos para garantizar la seguridad integral (seguridad física y ciberseguridad) de sus infraestructuras críticas.

Guía de Buenas Prácticas para la elaboración de los Contenidos Mínimos de los Planes de Protección Específicos. [17]:

- Con este documento se pretende orientar a aquellos operadores designados como críticos en la elaboración de sus PPEs, sirviendo como complemento a las Resoluciones del Secretario de Estado de Seguridad sobre Contenidos Mínimos del PPE.

- Se trata de un documento de carácter voluntario que no incluye requisitos adicionales a los establecidos por la legislación vigente o por la Resolución mencionada previamente.
- En esta guía se incluyen una serie de Anexos (detalle de medidas organizativas o gestión, operacionales o procedimentales, protección o técnicas, etc.) que podrán ser referentes de ayuda a los operadores críticos para la confección de alguno de los puntos de los contenidos mínimos del PPE.

Argentina

En el año 2011, en base a una serie de consideraciones como ser “que la seguridad de la infraestructura digital se encuentra expuesta a constantes amenazas, que en caso de materializarse pueden ocasionar graves incidentes en los sistemas de información y comunicaciones, por lo que resulta imprescindible adoptar las medidas necesarias para garantizar el adecuado funcionamiento de las infraestructuras críticas”, a través de la resolución JGM Nº 580/2011 se crea en Argentina el “Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad”. Este programa tiene entre otros objetivos, la elaboración de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas necesarias para el correcto funcionamiento del Sector Público Nacional, las organizaciones de jurisdicción provincial, la sociedad civil y las organizaciones privadas, sin embargo, no se define explícitamente a la ciberseguridad, solo se introduce la noción de Infraestructura crítica.
Tal como consigna el Art. 7º, “La OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION, en su carácter de autoridad de aplicación, brindará el apoyo técnico y administrativo necesario para la implementación del “PROGRAMA NACIONAL DE INFRAESTRUCTURAS CRITICAS DE INFORMACION Y CIBERSEGURIDAD”.
Ese mismo año, la ONTI través de la disposición Nº 3/2011 aprueba el "Formulario de adhesión al Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad”, mediante el cual las entidades y jurisdicciones definidas en el artículo 8º de la Ley Nº24.156 y sus modificatorias, los organismos inter jurisdiccionales, y las organizaciones civiles y del sector privado podrán adherir al “Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad”. [4]

Leyes relacionadas a la ciberseguridad:

- Ley 26.388 de Delito informático [11]
- Ley 25.326 de Protección de Datos Personales [11]
- Decreto Reglamentario N° 1558/2001 [11]
- Ley 25.506 de Firma Digital [11]
- Decreto Reglamentario N° 2628/2002 [11]
- Ley 26.904 de Grooming [11]

Normativa vinculada a las funciones de la Dirección Nacional de Infraestructuras críticas de la información y ciberseguridad

- Decisión Administrativa 641/2021. Establece los requisitos mínimos de seguridad de la información para organismos públicos. [11]
- Disposición 6/2021. Creación del Comité Asesor para el Desarrollo e Implementación de aplicaciones seguras. [11]
- Disposición 1/2021. Centro Nacional de Respuestas a Incidentes Informáticos (CERT.ar) en el ámbito de la Dirección Nacional de Ciberseguridad. [11]
- Resolución 580/2011. Creación del Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad. [11]
- Disposición ONTI 3/2013. Aprobación de la Política Modelo de Seguridad de la Información. [11]
- Resolución 1523/2019. Definición de Infraestructuras Críticas. [11]

Otras normativas relacionadas a la ciberseguridad

- Decreto 577/2017. Creación del Comité de Ciberseguridad. [11]
- Decreto 480/2019. Modificación del Decreto 577/2017. [11]
- Resolución 829/2019. Aprobación de la Estrategia Nacional de Ciberseguridad. [11]
- Resolución 141/2019. Presidencia del Comité de Ciberseguridad. [11]
- Disposición 6/2021. Creación del Comité Asesor para el Desarrollo e Implementación de aplicaciones seguras. [11]
- Decisión Administrativa N° 532/2021: relacionada con la implementación de acciones relativas a la ciberseguridad y a la protección de las infraestructuras críticas de información, así como también a la generación de capacidades de

prevención, detección, respuesta y recupero ante incidentes de seguridad informática del Sector Público Nacional y de los servicios de información y comunicaciones definidos en el artículo primero de la Ley Nº 27.078. [11]

- Infraestructura critica Decreto N° 802 de la JEFATURA DE GABINETE DE MINISTROS, la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN (Contempla todas esas actividades esenciales que dependen de las Infraestructuras Críticas: centrales eléctricas o nucleares, sistema de aguas, transporte ferroviario, sistema bancario, tecnología de satélite, sistemas de telecomunicaciones o de la Administración). [11]

CONCLUSION

Las infraestructuras críticas son aquellos sistemas y servicios que soportan infraestructuras esenciales para el desarrollo de la sociedad y garantizan el normal servicio prestado por los estados. Todos tienen la particularidad de que su disponibilidad impacta directamente en la sociedad. Asimismo, existe una interdependencia de las infraestructuras críticas entre ellas, al estar interconectados desde varios estados; motivo por el cual un incidente de seguridad en una infraestructura critica de un estado podría afectar a otros países. Dada la importancia que tienen las CI y el contexto geopolítico en el que nos encontramos, el empleo de ciberataques como elemento desestabilizador se ha convertido en realidad, y nos obliga a disponer de una serie de medidas de seguridad adicionales para protegerlas. En concordancia con lo anterior, debemos tener en cuenta la problemática específica de los sistemas industriales, ya que en su origen no han sido diseñados teniendo presente la implementación de medidas de seguridad por lo que nos encontramos con la falta de actualizaciones de seguridad por obsolescencia de los equipos, contraseñas por defecto, sistemas que carecen de medidas de seguridad, dispositivos conectados a redes no confiables, etc.

Para hacer frente a esta situación los gobiernos están realizando diferentes esfuerzos para hacer frente a esta problemática y afrontar estos nuevos retos. Se han desarrollado normativas para que estas infraestructuras dispongan de adecuadas medidas de seguridad y creados organismos específicos para coordinar las respuestas antes estos nuevos retos que varían según el país. No obstante, a ello, sugerimos contemplar los siguientes aspectos de seguridad para minimizar los riesgos asociados:

- **Higiene cibernética:** Cumplir con ciertos puntos básicos de seguridad para asegurar la resiliencia; basándose en algún modelo reconocido (CERT, IEC 62443, IECEE, etc.).
- **Colaboración:** es clave para combatir el ciberdelito.
- **Educación:** Es fundamental que los empleados que manipulan o tienen acceso al sistema comprendan que la seguridad es una responsabilidad compartida y cómo pueden potencialmente poner a su empresa en riesgo.
- **Tecnología:** Disponer de medidas de protección tecnológicas, como soluciones de seguridad integrales que incluyan antivirus, antimalware, firewall y otros sistemas de detección proactiva.
- **Eficiencias operativas:** A medida que realiza inversiones en tecnología, asegúrese de trabajar en estrecha colaboración con las partes interesadas para que comprenda el impacto de sus decisiones en las unidades de negocio y ellos comprendan la urgencia en torno a la protección de datos y aplicaciones.
- **Sistema de Gestión de Incidentes** que permita el control continuo de las redes y aplicaciones mediante alertas, basado en algún *framework* reconocido, por ejemplo, NIST.

Los incidentes surgen donde pueden surgir, es decir, la gente que te quiere hacer daño lo hace en aquel sitio donde puede y es posible que los sectores como un sector como la energía o dentro de la energía un sector como el sector eléctrico pueda ser más susceptible de tener esos ciberincidentes dado que está más expuesto. No todo son ataques, no todo es ciberataques en esto del mundo cibernético del mundo digital. De hecho, la mayoría de los problemas que hay, la mayoría de los incidentes que se dan son por obsolescencia de equipos, por fallos en los equipos, por supuesto, por negligencia de quienes los opera, etcétera.

Un factor interesante e importante es que los países se integren globalmente y posean una mutua y estrecha colaboración con organismos de escalas mundiales. No es bueno que los países se mantengan aislados y no intercambien información con el resto, es por ello que, si cada uno aporta sus experiencias, sus éxitos, sus inquietudes y sus formas de resolver cada uno de los problemas en materia de amenazas a Infraestructuras Críticas, consecuentemente se generará un sólido lazo para enfrentar los peligros existentes. De esta forma es posible combatir el cibercrimen y mantener el ciberespacio cubierto. Hoy en día, la seguridad es un bien que beneficia a todos, es por ello que actitudes mezquinas no integran el conjunto de las buenas prácticas.

Como ciudadanos, pero especialmente como profesionales, debemos conocer cómo y con qué criterios se protegen las Infraestructuras Criticas, dado que nos permitirá proteger nuestros propios sistemas u organización con la misma eficacia.

BIBLIOGRAFIA CONSULTADA

[1] Protección de la Infraestructura Critica en América Latina y el Caribe.
Luis Almargo- Secretario General de la Organización de los Estados Americanos (OEA).
Tom Burt - Vicepresidente y Director Jurídico Adjunto de Digital Trust Microsoft Corporation.
2018.

[2] Protección de infraestructuras críticas: un análisis de derecho comparado.
Francisco Javier Galindo Sierra.
2016.

[3] Infraestructura Crítica y Ciberseguridad en Chile, orientaciones para su consenso.
Felipe A. Lopez, David Ruete, Gustavo Gatica.
RISTI, N.º E43, 07/2021.

[4] Diseño de un Plan Estratégico para la Protección de la Infraestructura de Información Critica en la Argentina.
Marisa Verónica Voragini.
2011.

[5] Guía para prevenir ataques a infraestructura crítica.
Página web:
https://revistaitnow.com/guia-para-prevenir-ataques-a-infraestructura-critica/
Redacción enero 18, 2018.
(Consultada el 18/5/2022).

[6] Infraestructuras Criticas.
Página web:
https://www.pandasecurity.com/es/mediacenter/src/uploads/2018/10/1611-WP-InfraestructurasCriticas-ES.pdf
(Consultada el 13/5/2022).

[7] Las vulnerabilidades en infraestructuras críticas aumentaron un 14% en 2018.
Página web:
https://www.pandasecurity.com/es/mediacenter/seguridad/vulnerabilidades-en-infraestructuras-criticas/
Redacción MARZO 13, 2019.
(Consultada el 18/5/2022).

[8] Cómo evitar el hackeo a Infraestructuras Críticas.

Página web: https://www.pandasecurity.com/es/mediacenter/panda-security/whitepaper-infraestructuras-criticas/
Redacción 30 Nov 2016.
(Consultada el 18/5/2022).

[9] Ciberataques a la infraestructura crítica de un país y sus consecuencias.
Página Web: https://www.welivesecurity.com/la-es/2022/03/10/ciberataques-infraestructura-critica-pais-consecuencias/
Redacción 10 Mar 2022.
(Consultada el 18/5/2022).

[10] Mantener la infraestructura crítica a salvo de los ataques cibernéticos.
Página Web: https://neuronamagazine.com/mantener-la-infraestructura-critica-a-salvo-de-los-ataques-ciberneticos/
Redacción 29 Oct 2021.
(Consultada el 18/5/2022).

[11] Normativa – Ciberseguridad.
Página Web: https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad/normativa
(Consultada el 3/5/2022).

[12] ISO 27000 y el conjunto de estándares de Seguridad de la Información
Página Web: https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/
(Consultada el 17/5/2022).

[13] La familia de Norma ISO 27000.
Página Web: https://www.isotools.org/2015/01/21/familia-normas-iso-27000/
(Consultada el 17/5/2022).

[14] IEC 62443: ciberseguridad para soluciones industriales.
Página Web: https://itcl.es/blog/iec-62443-ciberseguridad-para-soluciones-industriales/
(Consultada el 17/5/2022).

[15] Informe de inteligencia de seguridad de Microsoft.
Página Web: https://www.microsoft.com/en-us/security/Intelligence-report
(Consultada el 17/3/2022).

[16] NIPP 2013 Partnering for Critical Infrastructure Security and Resilience.
Página Web: https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf
(Consultada el 24/5/2022).

[17] Infraestructuras críticas: definición, planes, riesgos, amenazas y legislación. Página Web: https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas (Consultada el 17/5/2022).

[18] Aportes para una urgente convergencia entre Tecnología Operativa y Tecnología Informática. Página Web: https://www.segurilatam.com/seguridad-por-sectores/infraestructuras-criticas/infraestructuras-criticas-aportes-para-una-urgente-convergencia-entre-tecnologia-operativa-y-tecnologia-informatica_20220109.html (Consultada el 17/5/2022).

[19] Los ataques *ransomware* crecieron más de 700% durante el 2021. Página Web: https://nextvision.com/los-ataques-ransomware-crecieron-mas-de-700-durante-el-2021/#:~:text=El%20informe%20creado%20por%20Kaspersky,de%2035%20ataques%20por%20segundo. (Consultada el 17/5/2022).

[20] Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021. Página Web: https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/#:~:text=En%20total%2C%20solo%20el%20Top20,Colombia%20(87%20por%20minuto). (Consultada el 17/5/2022)

[21] Ciberataques: crecen un 24% en América Latina. Página Web: https://prensariotila.com/35367-Ciberataques-crecen-un-24-en-America-Latina/ (Consultada el 17/5/2022).

[22] El virus que tomó control de mil máquinas y les ordenó autodestruirse. Página Web: https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet#:~:text=El%20%22gusano%22%20%2D%20ahora%20conocido,infraestructura%20del%20%22mundo%20real%22. (Consultada el 17/5/2022)

[23[Infraestructuras Críticas y Ciberseguridad. Página Web: https://manuelsanchez.com/2011/07/06/infraestructuras-criticas-y-ciberseguridad/

(Consultada el 17/5/2022).

[24] Ciberataques dirigidos a infraestructuras críticas.
Página Web: https://revista.une.org/15/ciberataques-dirigidos-a-infraestructuras-criticas.html
(Consultada el 17/5/2022).

[25] Malware Havex dirigido a los controles industriales y servidores OPC.
Página Web: https://www.infoplc.net/actualidad-industrial/item/102024-malware-havex-controles-industrialesservidores-opc
(Consultada el 24/5/2022).

[26] Arabia Saudita dice ser blanco de un ciberataque "avanzado".
Página Web: https://www.france24.com/es/20171120-arabia-saudita-dice-ser-blanco-de-un-ciberataque-avanzado
(Consultada el 24/5/2022).

[27] Rusia y Ucrania: los 3 ciberataques rusos que más teme Occidente.
Página Web: https://www.bbc.com/mundo/noticias-60850173
(Consultada el 24/5/2022).

[28] Tritón es el software malicioso más asesino y se está difundiendo.
Página Web:
https://gruporadical.com/ver_prensa/1#:~:text=Trit%C3%B3n%20es%20el%20software%20malicioso%20m%C3%A1s%20asesino%20y%20se%20est%C3%A1%20difundiendo&text=En%20el%20verano%20de%202017,de%20da%C3%B1ar%20a%20las%20personas.
(Consultada el 24/5/2022).

[29] ¿Qué es WannaCry?
Página Web: https://www.avast.com/es-es/c-wannacry#:~:text=El%20ataque%20de%20WannaCry%20explot%C3%B3,000%20equipos%20en%20150%20pa%C3%ADses.
(Consultada el 24/5/2022).

[30] Petya (malware).
Página Web: https://es.wikipedia.org/wiki/Petya_(malware)
(Consultada el 24/5/2022).

[31] 9 veces en las que los piratas informáticos atacaron cibernéticamente instalaciones industriales.
Página Web: https://www.d4k.org/9-veces-en-las-que-los-piratas-informaticos-atacaron-ciberneticamente-instalaciones-industriales/.
(Consultada el 8/5/2022).

[32] Rusia ataca con malware y ataques DDoS a cientos de webs de Ucrania.

Página Web: https://www.redeszone.net/noticias/seguridad/ataques-ddos-borrado-datos-ucrania/

(Consultada el 24/5/2022).