Universidad de Buenos Aires

Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Tesis de Maestría

Título:

"Marco de Referencia de Ciberseguridad para Infraestructuras Críticas"

Autor: Esp. Dario Osvaldo RIZZO
Director: Dr. Mariano MÉNDEZ

Año de Presentación: 2020
Cohorte: 2017

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
Esp. Dario Osvaldo RIZZO
D.N.I. 28.264.829

Resumen

La era digital en la vida de las personas ha cobrado un rol fundamental para el desarrollo de las actividades cotidianas y laborales, yendo desde las más sencillas a las más complejas. Cada día, mayor cantidad de personas realizan transacciones comerciales: desde aplicaciones móviles y portales bancarios, solicitar turnos médicos, encargar un almuerzo, etc. Esta evolución digital masificó el uso de las tecnologías de la información, las que, paralela e inevitablemente fomentan la proliferación de actores malintencionados, o ciberdelincuentes, que acechan a la vera del flujo de información que los particulares, las compañías u organismos de gobierno, alimentan de modo insoslayable dentro de la comunidad digital.

En efecto, el flujo de información se ve afectado en los tres preceptos que configuran el ejercicio de la seguridad informática. A la postre, veremos en profundidad que la finalidad de los ciberdelincuentes no se limita a un objetivo en particular, sino que responden a una diversidad de factores, como pueden ser, los técnicos (conocimiento), los culturales (étnico-religiosos), los políticos (bélico-territoriales), entre otros.

Este trabajo propone abarcar el tópico de la ciberseguridad y la ciberdefensa, analizando su aplicación en la Argentina y en los países más influyentes en la materia, examinando potenciales focos de conflicto que puedan poner en riesgo las *infraestructuras críticas* de las Naciones, proponiendo además el diseño de un Marco de Ciberseguridad para ser aplicado ante posibles escenarios; con el objeto de ser empleado por cualquier Organismo Gubernamental o compañía que se catalogue como Infraestructura Crítica.

Palabras Claves

Ciberseguridad | Ciberataque | Infraestructuras Críticas | Amenaza | Estrategia | Marco

Índice

Índice de figuras

Índice de tablas

Prólogo

Quiero agradecer en primera instancia a las mujeres de mi vida, mi señora esposa Verónica y a los soles que iluminan mis días, mis hijas Renata e Isabella, quienes fueron un pilar y brindaron su apoyo incondicional a este proyecto, desde el primer día, hasta la finalización de la cursada, haciéndolo extensivo a mis Padres, que siempre me incentivan a capacitarme para afrontar los retos que nos pone nuestra vida laboral.

En segunda instancia, agradecer a mis compañeros, en los cuales encontré un excelente grupo de colegas y amigos. A la totalidad de los profesores de esta excelentísima casa de estudios, como es la Universidad de Buenos Aires, que, con su incansable esfuerzo y vasto conocimiento, hicieron de esta Maestría, una experiencia muy enriquecedora. No puedo olvidarme del Ministerio de SEGURIDAD de la Nación, quien me otorgo una beca para poder realizar la Maestría.

A mis amigos y colegas, el Lic. Diego A. RABALO quien se desempeña profesionalmente en el Departamento CIBERSEGURIDAD de la Policía Federal Argentina y el Lic. Rubén D. AYBAR futuro Magister en la materia y reconocido profesional, por su colaboración y perspectiva, quienes dieron sus constantes recomendaciones en el proceso de la confección del presente.

Y por último a mi director el Dr. Mariano MENDEZ, quien brindó su mayor esfuerzo, proporcionando su punto de vista y conocimiento en todo momento cuando lo requerí. Este trabajo hubiera sido imposible terminarlo y darle un sentido académico, sin su asistencia y guía.

Introducción

Este Trabajo Final de Maestría complementa al trabajo Final de la Especialización en Seguridad Informática, donde en este último se desarrolló y explicó en forma detallada el Marco de Trabajo de Ciberseguridad impulsado por el NIST [1]. En esta oportunidad, se ha efectuado una investigación descripto-explicativa adoptando, como referencia bibliográfica, documentos de Organismos y Corporaciones que están a la vanguardia de la Ciberseguridad y protección de Infraestructuras Críticas, se concluye el presente trabajo con el desarrollo de un Marco para ser propuesto a los altos mandos de las Organizaciones Gubernamentales relacionadas con la Seguridad Nacional donde se requiera, proponiendo su utilización para la futura Gestión de Riesgos de Ciberseguridad a nivel Nacional.

La tecnología es uno de los elementos más valiosos que apuntan las organizaciones terroristas y sus adeptos mediante la utilización de Internet con un amplio abanico de posibilidades, como ser [1]:

- ✓ El reclutamiento,
- ✓ el financiamiento,
- ✓ la propaganda,
- ✓ el adiestramiento,
- ✓ la motivación con una finalidad de comisión de actos terroristas,
- ✓ y/o simplemente, la transmisión de información con idénticos fines;

Dado esto, es que se necesitan conocimientos técnicos específicos para poder analizar y detectar de una manera eficaz a estos tipos de delitos.

Se han materializado varios ciberataques perpetrados con finalidades que superan la simplicidad de un logro personal por un sujeto, observándose el trabajo de una red o grupo de personas alineados por una ideología o con

[1] National Institute of Standards and Thecnology U.S. Department of Commerce (Instituto Nacional de Estándares y Tecnología de los Estados Unidos de Norteamérica NIST, por sus siglas en inglés)

fines económicos, por ejemplo, en 1982 vulneraron un sistema SCADA[2] de un oleoducto siberiano, en 2006 hackearon por varias horas los semáforos de la ciudad de Los Ángeles, y en 2015 Ucrania recibió un ciberataque a su red eléctrica, por solo mencionar algunos de ellos [2].

Las infraestructuras críticas, son una fortaleza y al mismo tiempo una debilidad de los Estados, por lo que han tomado una importancia vital para el funcionamiento y desarrollo de las económicas de los mismo, como así también, mejoran la calidad de vida de sus habitantes. En este sentido, se han convertido en objetivos con alta probabilidad de ser atacados a través de medios informáticos, como hemos ejemplificado anteriormente. Entre los diferentes factores que promueven estos escenarios, alimentados por la globalización, el creciente y permanente conflicto entre los estados, como consecuencia de las diferencias de intereses entre ellos, supone un desafío y la necesidad de implementar un marco estratégico de gestión de incidentes producto de las brechas de seguridad [2].

En este contexto, el objetivo principal de esta investigación será el diseño y creación de una propuesta para el Departamento de CIBERSEGURIDAD de la Policía Federal Argentina, cuya aplicación sea posible ante diferentes metodologías y vectores de ataques. En suma, las acciones definidas en el marco propuesto podrán ser adaptadas a cualquier organismo o compañía que sea catalogada como infraestructura crítica.

Actualmente desde la óptica Jurídica/Normativa en la República Argentina, existen intentos por establecer la temática en el ámbito Gubernamental mediante el dictado de plexos legales específicos como son: El Decreto Nro. 577/2017 publicado el 31 de Julio del 2017 en el que se crea un Comité de Ciberseguridad, el Decreto Nro. 480/2019 de fecha 12 de Julio del 2019 en el cual se amplía la composición de dicho Comité, la Resolución 1523/2019 de fecha 18 de septiembre del 2019 en la que se definen las Infraestructuras Críticas e Infraestructuras Críticas de Información, se observa con claridad, que no hay un plan interdisciplinario que abarque a todas las

[2] Supervisory Control And Data Acquisition (Adquisición de datos y supervisión de control, por sus siglas en inglés).

organizaciones alcanzadas por dicha definición, y la más reciente, la Resolución 1380/2019 de fecha 25 de octubre del 2019 en la que se define el concepto de Ciberdefensa, creándose el Centro Nacional de Ciberdefensa en el ámbito de la SUBSECRETARÍA DE CIBERDEFENSA, como así también, se define la Política Nacional.

Marco Normativo en la República Argentina

Como antecedentes locales, si bien este país posee normativa vigente y actual, se debe destacar el Decreto Nro. 577/2017 publicado en el Boletín Oficial de la República Argentina en su edición de fecha 31 de Julio de 2017 [3], por el cual se crea el comité de ciberseguridad, detallado de la siguiente manera:

ARTÍCULO 1°. - Créase el COMITÉ DE CIBERSEGURIDAD en la órbita del MINISTERIO DE MODERNIZACIÓN, que estará integrado por representantes del citado Ministerio, del MINISTERIO DE DEFENSA y del MINISTERIO DE SEGURIDAD, el cual tendrá por objetivo la elaboración de la Estrategia Nacional de Ciberseguridad.

Y dentro de la misma normativa, se expresa la voluntad de una pronta implementación, debido a la importancia que esta temática toma dentro de la Administración Pública Nacional, ilustrándose de la siguiente manera en el artículo 5° de la misma Ley:

ARTÍCULO 5°. - Encomiéndese al MINISTRO DE MODERNIZACIÓN, o a quien ese designe, impulsar los actos administrativos y demás acciones necesarias para la implementación de la Estrategia Nacional de Ciberseguridad que apruebe el COMITÉ DE CIBERSEGURIDAD, así como de los objetivos en ella contenidos.

Finalmente, con fecha 28 de mayo del 2019, mediante la resolución 829/2019 [4], de la Jefatura de Gabinete de Ministros de la *SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN,* se publica y aprueba la ESTRATEGIA NACIONAL DE CIBERSEGURIDAD de la República Argentina, la que consta de 5 principios rectores de la Ciberseguridad, que se mencionan a continuación:

- RESPETO POR LOS DERECHOS Y LIBERTADES INDIVIDUALES,

- LIDERAZGO, CONSTRUCCIÓN DE CAPACIDADES Y FORTALECIMIENTO FEDERAL,
- INTEGRACIÓN INTERNACIONAL,
- CULTURA DE CIBERSEGURIDAD Y RESPONSABILIDAD COMPARTIDA,
- FORTALECIMIENTO DEL DESARROLLO SOCIOECONÓMICO.

Si bien posteriormente, con fecha 12 de Julio del 2019, mediante el decreto Nro. 480/2019 [5], se realiza una modificación a la integración de dicho comité, sustituyendo el artículo 1° del mencionado decreto del párrafo anterior, quedando redactado de la siguiente manera:

ARTÍCULO 1°. - Créase el COMITÉ DE CIBERSEGURIDAD en la órbita de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS, el que estará integrado por representantes de la citada Secretaría de Gobierno, de la SECRETARÍA DE ASUNTOS ESTRATÉGICOS de la JEFATURA DE GABINETE DE MINISTROS, del MINISTERIO DE DEFENSA, del MINISTERIO DE SEGURIDAD, del MINISTERIO DE RELACIONES EXTERIORES Y CULTO y del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, el cual tendrá por objetivo la elaboración de la Estrategia Nacional de Ciberseguridad.

El COMITÉ DE CIBERSEGURIDAD, será presidido por el Secretario de Gobierno de Modernización, en su carácter de Vicejefe de Gabinete de la JEFATURA DE GABINETE DE MINISTROS".

Un antecedente previo al mencionado decreto, en el cual ya se observa la preocupación y a raíz de los sucesos a nivel global en el escenario de la ciberseguridad, se introduce como temática de importancia en la agenda de Gobierno, mediante la creación de una Subsecretaria de Tecnología y Ciberseguridad dependiente del Ministerio de Modernización, lo que se detalla en el decreto Nro. 898/2016 [6].

Otro hito para tener en cuenta y no menos importante, por medio de una decisión administrativa Nro. 669/2004, emitida por la SUBSECRETARIA

DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS [7], les indica a todos los organismos dependientes de la Administración Pública Nacional, dicten o adecuen sus políticas de seguridad de la información creando en cada una de las reparticiones un comité de seguridad de la Información que deberá desarrollar la normativa interna, detalla de la siguiente manera en sus artículos 1° y 2°:

ARTÍCULO 1°. - POLITICA DE SEGURIDAD DE LA INFORMACION Estableése que los organismos del Sector Público Nacional comprendidos en el artículo 7° de la presente medida, deberán dictar o bien adecuar sus políticas de seguridad de la información conforme a la Política de Seguridad Modelo a dictarse de conformidad con el artículo 8°, dentro del plazo de CIENTO OCHENTA (180) días de aprobada dicha Política de Seguridad Modelo.

ARTÍCULO 2°. - COMITE DE SEGURIDAD DE LA INFORMACION las máximas autoridades de los organismos comprendidos en el artículo 7° de la presente medida, deberán conformar en sus ámbitos un Comité de Seguridad de la Información integrado por representantes de las Direcciones Nacionales o Generales o equivalentes del organismo.

Recientemente se ha publicado la resolución Nº 1523/2019, emitida por SUBSECRETARIA DE GOBIERNO DE MODERNIZACION de la JEFATURA DE GABINETE DE MINISTROS [8], mediante la cual se busca una integración en lo concerniente a la ciberseguridad, con el fin de poder identificar y agrupar los sectores determinados tanto como infraestructura críticas como de operación, determinados de la siguiente manera en sus artículos 1º, 2º y 3º:

ARTÍCULO 1°.- Apruébese la definición de Infraestructuras Críticas y de Infraestructuras Críticas de Información, la enumeración de los criterios de identificación y la determinación de los sectores alcanzados, que como Anexo I (IF-2019-78452510-APN-SGM#JGM) forma parte de la presente medida.

ARTICULO 2°.- Apruébese el Glosario de Términos de Ciberseguridad, que como Anexo II (IF-2019-78455467-APN-SGM#JGM) forma parte de la presente medida.

ARTICULO 3°.- Delegase en el Director Nacional de Ciberseguridad de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS, la revisión y actualización periódica del Glosario aprobado en el artículo 2° de la presente medida.

Como se desprende de la Resolución 1380/2019 de fecha 25 de octubre del 2019 [9], en la que se define el concepto de Ciberdefensa y se crea el Centro Nacional de Ciberdefensa en el ámbito de la SUBSECRETARÍA DE CIBERDEFENSA, como también, se crea la Política de Ciberdefensa Nacional, según lo expresado en los artículos 1º, 2º, 3º y 4º:

ARTÍCULO 1°.- Sustituyese el Artículo 2° de la Resolución del Ministro de Defensa N° 59 del 23 de enero de 2017 por el siguiente:

"Entiéndase por CIBERDEFENSA a las acciones y capacidades desarrolladas por el MINISTERIO DE DEFENSA, EL ESTADO MAYOR CONJUNTO y las FUERZAS ARMADAS para anticipar y prevenir ciberataques y ciberexplotación de las redes nacionales que puedan afectar al Ministerio de Defensa y al Instrumento Militar de la Defensa Nacional, como así también a las Infraestructuras Críticas operacionales soporte de los Servicios Esenciales de interés para la Defensa o a Infraestructuras operacionales soporte de procesos industriales de fabricación de bienes sensibles para la Defensa o que posibiliten el acceso a los activos digitales estratégicos adjudicados a su custodia."

ARTÍCULO 2°.- Créase el Centro Nacional de Ciberdefensa en el ámbito de la SUBSECRETARÍA DE CIBERDEFENSA, donde funcionarán el CENTRO DE RESPUESTA ANTE EMERGENCIAS INFORMÁTICAS DEL MINISTERIO DE DEFENSA (CSIRT de DEFENSA), el CENTRO INTELIGENTE DE OPERACIONES DE SEGURIDAD (¡SOC) del COMANDO CONJUNTO DE CIBERDEFENSA del ESTADO MAYOR CONJUNTO DE

LAS FUERZAS ARMADAS que centraliza la operación de los CENTROS DE OPERACIONES DE SEGURIDAD (iSOC) remotos de cada una de las Fuerzas Armadas y el LABORATORIO DE ANÁLISIS CIBERNÉTICO (CyberLab), entre otras plataformas y sistemas, cuyas actividades y mecanismos de implementación serán definidos por el SUBSECRETARIO DE CIBERDEFENSA a través de los actos pertinentes.

ARTÍCULO 3°.- Apruébese la Política de Ciberdefensa consistente en CUATRO (4) Líneas de Acción principales que se desarrollarán conjugando TRES (3) ejes de políticas y cuya implementación se realiza a través de DOS (2) planes en orden de cumplimentar los objetivos aprobados por el artículo 2º del Decreto Nº 684 del 3 de octubre de 2019, descriptos en los Anexos I (IF-2019-96170351-APN-SSC#MD), II (IF-2019-96170945-APN-SSC#MD), III (IF-2019-96171204-APN-SSC#MD), IV (IF-2019-96172220-APN-SSC#MD) y V (IF-2019-96171563-APN-SSC#MD), los que se acompañan a la presente Resolución.

ARTÍCULO 4°.- Créase, en el ámbito de la SECRETARÍA DE ESTRATEGIA Y ASUNTOS MILITARES, el Comité Consultivo de Ciberdefensa que estará integrado por la SUBSECRETARÍA DE PLANEAMIENTO ESTRATÉGICO Y POLÍTICA MILITAR, la SUBSECRETARÍA DE CIBERDEFENSA y el ESTADO MAYOR CONJUNTO DE LAS FUERZAS ARMADAS, cuyo cometido será la realización de estudios para la definición del Plan de adecuación de las Organizaciones Militares y la preparación de la propuesta de la DIRECTIVA PARA LA ELABORACIÓN DEL PLANEAMIENTO ESTRATÉGICO MILITAR (DEPEM) en materias de Tecnologías de la Información y Comunicaciones y ciberespacio en el término de treinta días desde el dictado de la presente.

Infraestructuras Críticas

Definiciones

Como modelo comparativo a futuro, y por cuestiones que se abarcaran más adelante, resulta interesante la clasificación que le atribuye Estonia a las Infraestructuras Críticas (país ubicado al noroeste del continente europeo), esta nación es considerada la más digitalizada del mundo. Particularmente, ha creado un organismo específico llamado RIA [3] y que además ha desarrollado una definición propia para la expresión **"*Infraestructura de información crítica*"**, asignándole la responsabilidad de proteger estas infraestructuras, siendo la autoridad máxima del Sistema de Información de Estonia. En tal sentido, las cataloga como "*Sistemas de información y comunicación cuyo mantenimiento, fiabilidad y seguridad son esenciales para el buen funcionamiento de un país. La infraestructura de información crítica es parte de la infraestructura crítica"* [10].

El NIST, quien dentro de sus funciones tiene un área específica en lo que refiere a la Ciberseguridad, las define como: *"Sistemas y activos, ya sean físicos o virtuales, tan importantes para un País que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitante en la seguridad cibernética, seguridad económica nacional, seguridad o salud pública nacional o cualquier combinación de esos asuntos"* [11].

En la República Argentina, mediante el ANEXO I de la Resolución 1523/2019, mencionada en el apartado anterior, se han definido de la siguiente manera [8]:

"Las Infraestructuras Críticas son aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el

[3] Riigi Infosüsteemi Amet (Estonian Information System Authority, Autoridad de Sistemas de Información de Estonia, por sus siglas en estonio)

funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente."

Además, hace la distinción de las Infraestructuras Críticas y las Infraestructuras Críticas de Información [8]:

"Las Infraestructuras Críticas de Información son las tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas."

De la comparación entre las diferentes definiciones efectuadas por entidades de Gobierno y Tecnología, se deduce la existencia de un núcleo conductor de los objetivos críticas a ser protegidos en un País para reducir las vulnerabilidades ante ciberataques.

En términos más generales, pueden considerarse como Infraestructuras Críticas, por ejemplo, las **plantas de generación de energía**, los **sistemas de transporte públicos**, los **sistemas de producción**; entre otros. Todas ellas controladas y monitoreadas, en su mayoría, por **Sistemas de Control Industria**l (ICS) y **sistemas SCADA** (Control de Supervisión y Adquisición de Datos).

Actualmente, los productos ICS se basan principalmente en plataformas de sistemas estándares embebidos y a menudo, utilizan software comercial de similares características. La aplicación de estas Plataformas reduce los tiempos de los procesos, abaratan costos operativos y ofrecen una mayor facilidad de uso, pero al mismo tiempo, aumentan la exposición a potenciales ciberataques [12].

El Organismo ENISA [4] [13], en la guía *"Metodologías para la identificación de activos y servicios de Infraestructuras Críticas"*, expone la necesidad de arbitrar una colaboración efectiva entre el sector público

[4] European Union Agency for Cybersecurity (Agencia de Ciberseguridad de la Unión Europea, por sus siglas en inglés)

(Gobierno y Agencias) y el sector privado (Compañías de servicios), ya que, a menudo, controlan numerosas infraestructuras críticas que son accesorias a las de Gobierno. Esto último, se debe a la complejidad de las interdependencias, el rol de los propietarios de los activos y los mecanismos para hacer, que estas, sean seguras y resistentes.

Por estas razones, en la guía en cuestión expresa que, debe haber una colaboración fluida entre los actores involucrados, que tienen la función de realizar la administración de los activos y servicios críticos utilizados en las redes de comunicación, como pueden ser:

- Operadores de infraestructura crítica.
- Proveedores de comunicación electrónica.
- Autoridades nacionales de regulación de las telecomunicaciones.
- Agencias de ciberseguridad.

Clasificación

Como compendio, es interesante nuevamente la valoración que ofrece la ENISA, donde describe una lista orientativa de sectores críticos y subsectores y servicios asociados. Además, considera el total de la cadena de valor como un servicio crítico. La siguiente lista debe ser considerada como de referencia (tomándola como punto de partida), para evaluar los sectores y los servicios que, se clasificarán como críticos, acorde a la función que cumplan para la Sociedad [13].

Sector crítico	Subsector crítico	Servicios críticos
1. Energía	Electricidad	○ Generación (todas las formas). ○ Transmisión / Distribución. ○ Mercado de electricidad.
	Petróleo	○ Extracción. ○ Refinamiento. ○ Transporte. ○ Almacenamiento.

	Gas Natural	○ Extracción. ○ Transporte / Distribución. ○ Almacenamiento.
2. Tecnologías de la información y la comunicación (TIC)	Tecnologías de la información	○ Servicios web. ○ Centro de datos / servicios en la nube. ○ Software como servicio.
	Comunicaciones	○ Comunicación de voz / datos. ○ Conectividad a internet.
3. Agua	Agua potable	○ Almacenamiento de agua. ○ Distribución de agua. ○ Aseguramiento de la calidad del agua.
	Aguas residuales	○ Recolección y tratamiento de aguas residuales.
4. Alimentos		○ Agricultura / producción de alimentos. ○ Suministro de alimentos. ○ Distribución de alimentos. ○ Calidad / inocuidad de los alimentos.
5. Salud		○ Atención médica de emergencia. ○ Atención hospitalaria (pacientes hospitalizados y ambulatorios). ○ Suministro de productos farmacéuticos, vacunas, sangre, suministros médicos. ○ Infección / control de epidemias.
6. Servicios Financieros		○ Bancos. ○ Transacciones de pago.

		○ Bolsa de valores.
7. Orden Público y Seguridad		○ Mantenimiento del orden público y la seguridad. ○ Sistema judicial y penal.
8. Transporte	Aviación	○ Servicios de navegación aérea. ○ Operación aeroportuaria.
	Transporte terrestre	○ Servicios de autobús / tranvía. ○ Mantenimiento de la red vial.
	Transporte en tren	○ Gestión del ferrocarril público. ○ Servicios de transporte ferroviario.
	Transporte marítimo	○ Seguimiento y gestión del tráfico marítimo. ○ Operaciones para romper el hielo.
	Postal / envío	
9. Industria	Industrias críticas	○ Empleo.
	Industria química / nuclear	○ Almacenamiento y eliminación de materiales peligrosos. ○ Seguridad de las unidades industriales de alto riesgo.
10. Administración Civil		○ Funciones del gobierno.
11. Espacio		○ Protección de sistemas espaciales.
12. Protección civil		○ Servicios de emergencia y rescate.
13. Ambiente		○ Control de la contaminación del aire y alerta temprana. ○ Vigilancia meteorológica y alerta temprana.

	○ Monitoreo de agua subterránea (lago / río) y alerta temprana. ○ Monitoreo y control de la contaminación marina.
14. Defensa	○ Defensa Nacional.

TABLA 1. *LISTA DE SECTORES Y SERVICIOS CRÍTICOS RELACIONADOS* [13]

En el mismo orden de ideas, la Agencia Europea, evalúa al impacto con relación a tres características principales [13]:

I. **El alcance o distribución espacial:** el área geográfica que podría verse afectada por la pérdida o falta de disponibilidad de una infraestructura crítica;
II. **La severidad o intensidad o magnitud:** las consecuencias de la interrupción temporal o destrucción de una infraestructura crítica particular;
III. **Los efectos del tiempo o la distribución temporal:** el punto de que la pérdida de un elemento podría tener un impacto grave (de inmediato, en uno o dos días, o una semana).

Criterio	Explicación
Población afectada	El porcentaje de la población del País afectado por la interrupción del servicio.
Concentración	La densidad de la población en el área geográfica que afecta el servicio.
Impacto Económico	La interrupción del costo del servicio en términos de porcentaje del PBI
Confianza pública	El efecto que el buen funcionamiento de este servicio tiene en la confianza pública hacia el gobierno.
Relaciones Internacionales	El efecto que tendrá una interrupción del servicio en las relaciones entre el País, con sus pares.
Orden Público	El efecto que una interrupción del servicio puede causar al orden público.

Operaciones públicas obstaculizadas	Las operaciones diarias de la sociedad, como ir a trabajar en transporte público, se detienen o se paralizan.
Los servicios de otro País se ve afectado	Las interdependencias con servicios críticos de otros Estados deben tenerse en cuenta.

TABLA 2. ***LISTA DE CRITERIOS PARA LA DEFINICIÓN DE SECTORES Y SERVICIOS CRÍTICOS*** **[13]**

Ciberseguridad

Considerando lo desarrollado hasta ahora, se puede concluir que la ciberseguridad tiene como objetivo capital la protección de la Infraestructura Computacional, haciendo principal énfasis en evitar la pérdida o robo de datos críticos -o sensibles- y garantizar su acceso a la Organización, buscando el cumplimiento de los tres preceptos fundamentales para la protección de la información. Estos últimos, se encuentran netamente vinculados y conforman las bases de la Seguridad Informática. A continuación, se observa la tríada CIA (Confidentiality Integrity Availability, por sus siglas en Ingles) representada gráficamente en la *figura 1.*

FIGURA 1. ***REPRESENTACIÓN PROPIA, SEGÚN LA TEORÍA DE LA TRÍADA CIA***

El instituto NIST explica los tres preceptos de la siguiente manera [11]:

- **Confidencialidad:** es el modo de prevenir la divulgación de información, a personas o sistemas informáticos, que no cuenten con la debida autorización para acceder a la misma.

- **Integridad:** es la propiedad con la cual los datos confidenciales se mantienen intactos, es decir, sin modificaciones o eliminaciones de manera no autorizada y sin detecciones.

- **Disponibilidad:** es el sostén fundamental, motivo por el cual representa la base de la tríada -triangular-, definiéndose como la capacidad de garantizar la accesibilidad oportuna y confiable de la información.

Significado etimológico del término *"ciber"*

Para comenzar un análisis más profundo de los conceptos que desarrollaremos en este trabajo, es necesario conocer el origen y significado etimológico de las palabras.

De origen griego, el término *"cyber" (kyber)*, significa *"control, timón, espacio virtual creado por medios informáticos"* [14]. En este sentido, se podría tomar como lógica la definición compuesta de CIBERESPACIO, ofrecida por la Real Academia Española (R.A.E.) como *"un ámbito virtual creado por medios informáticos".* Más allá de cualquier consideración, o definición más profunda que se pudiera encontrar en la materia, se estima a esta última como la más sintética y acertada para un posterior análisis de la cuestión de la seguridad informática.

En esta inteligencia, conociendo la multiplicidad de construcciones que se pueden crear a partir de la palabra "CIBER", se trata particularmente de identificar y acotar la definición de "CIBERESPACIO" a tan solo "CIBER" como adjetivo, y que puede ser conjugado al acompañarse con verbos que definan una determinada acción dentro del ámbito creado por los medios informáticos.

Partiendo de esto, es posible desarrollar múltiples conceptos y términos que abarcan la cuestión de la seguridad informática (ciberseguirdad, ciberataque, ciberterrorismo, ciberespionaje, etc.). En suma, si bien más adelante se tratara en profundidad a cada uno de ellos, se debe tener claro que la cuestión CIBER, se refiera a las TIC's, puede ser utilizada como medio u objetivo por parte del enemigo o la competencia.

En el siguiente gráfico, se representa la utilización de las tecnologías de la información como una doble dimensión para ser considerada al momento de analizar las potenciales amenazas en el desarrollo de las estrategias de ciberseguridad.

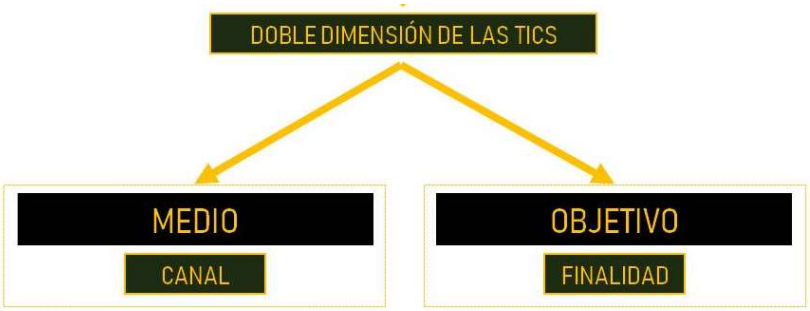

FIGURA 2. ***REPRESENTACIÓN PROPIA, REPRESENTACIÓN DEL ENFOQUE DE LA UTILIZACIÓN DE LAS TIC'S***

Se utilizará como ejemplo de la doble dimensión de las TIC's la amenaza ciberterrorista. En el primer caso podemos considerar como MEDIO al uso de internet a modo de instrumento del que se vale una organización terrorista para estructurar parte de sus actividades [15], algunas de ellas como se representan en el gráfico a página siguiente.

FIGURA 3. ***REPRESENTACIÓN PROPIA, REPRESENTACIÓN DE LA UTILIZACIÓN COMO MEDIO DE LAS TIC'S***

Considerando el mismo ejemplo (ciberterrorismo), la segunda hipótesis de utilización de las TIC's puede tratarse del perjuicio o daño de los activos informáticos como objetivo del ataque, desde la consideración que atacando

Internet puede llevar a conseguir parte de esos fines (ataques graves a través de medios electrónicos a las INFRAESTRUCTURAS CRÍTICAS de una Comunidad, Región, Estado o Nación) [15].

FIGURA 4. ***REPRESENTACIÓN PROPIA, REPRESENTACIÓN DE LOS OBJETIVOS DE LOS CIBERATAQUES***

Habiendo abarcado la definición y el significado del término "ciber", como *"un ámbito virtual creado por medios informáticos"* y que el mismo puede utilizarse como *"medio u objetivo",* con la potencialidad de causar graves perjuicios a la estabilidad de una Nación, es importante finalmente tratar, máxime, la cuestión de la seguridad en el ciberespacio o ciberseguridad.

¿Qué es la ciberseguridad?

Como punto de partida resulta acertado contemplar la clasificación desarrollada por el NIST, donde define a la ciberseguridad como "*la capacidad de proteger o defender el uso del ciberespacio de los ciberataques"*. De aquí se puede extraer dos elementos que son parte y conforman el todo, el ciberespacio y los ciberataques –concepto este último, del que se hablara más adelante–. En tal sentido, nuevamente el NIST, entiende al ciberespacio como "*un dominio global, dentro del entorno del ecosistema digital, el cual consiste*

en la red interdependiente de infraestructuras de sistemas de la información, en el que se incluyen Internet, redes de telecomunicaciones y datos, sistemas informáticos y procesadores y controladores integrados" [11].

Otra definición, desde la perspectiva Gobierno/Institucional, es la realizada por el ISO[5], quien, en su Norma ISO/IEC 27032:2012 "Gestión de la Ciberseguridad" -siendo un estándar en la materia-, propone combatir el cibercrimen mediante la *cooperación y coordinación*, plantea a la "Ciberseguridad" o "la seguridad del Ciberespacio", como el *resguardo de la confidencialidad, integridad y disponibilidad de la información dentro del Ciberespacio.* Este Organismo considera al "ciberespacio" como "*un entorno complejo -netamente lógico- en el que interactúan personas, software y servicios asociados a internet, mediante la utilización de dispositivos tecnológicos interconectados a él"* [16].

Asimismo, desde la óptica comercial, la firma Kaspersky Lab, empresa líder en la materia, la define como la práctica de proteger computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos de ataques maliciosos, además destaca que, se la conoce como seguridad de tecnología de la información o seguridad de la información electrónica [17].

Una vez abarcado y comprendido el concepto de ciberseguridad, se debe entender la acción del ciberataque:

Una definición muy interesante es la impulsada por la UNODC[6], que la determina de la siguiente manera: generalmente se refiere a la explotación deliberada de redes informáticas como medio para ejecutar un ataque. Estos ataques suelen estar destinados a desestabilizar el normal funcionamiento de los blancos escogidos, tales como los sistemas informáticos, servidores o la

[5] International Organization for Standardization (Organización Internacional de Normalización ISO, por sus siglas en inglés)
[6] United Nations Office on Drugs and Crime (Oficina de las Naciones Unidas contra la Droga y el Delito, por sus siglas en inglés)

infraestructura que le da soporte, mediante el uso de técnicas de piratería informática, amenazas avanzadas y persistentes, virus informáticos, programas maliciosos, phlooding o cualquier otro medio de acceso no autorizado o malicioso. Los ciberataques pueden nuclear/agrupar todas las características de un acto de terrorismo, incluido la acción psicológica de infundir temor con políticos o de reacción social. Cabe citar, como ejemplo de ciberataque, el sufrido por Israel en enero de 2012, que consistió en ataques contra múltiples sitios web israelíes simbólicos, tales como la web de la Bolsa de Valores de Tel Aviv y la de la compañía aérea de bandera, como así también la divulgación no autorizada de los detalles de cuentas de tarjetas de crédito de miles de nacionales israelíes [15].

El NIST ha definido ciberataque como: un ataque, por medio del ciberespacio, estrictamente dirigido al uso del ciberespacio de una empresa con el fin de interrumpir, deshabilitar, destruir o controlar de forma maliciosa un entorno y/o infraestructura informática; o bien, destruir la integridad de los datos o robar información controlada [11].

En una primera aproximación a la definición de *"ciberterrorismo"*, es válido pensarla como la convergencia del *terrorismo* con el *cibersespacio*. Del mismo modo, se deberá examinar lo enunciado en el año 2000 por la Dra. Dorothy E. Denning Al [15], de la Universidad de Georgetown (E.E.U.U.), cuando lo describía como el *"uso indebido de las tecnologías de las comunicaciones para promover actos de terrorismo"*. Ahora bien, veinte años más tarde, la historia ha comprobado que el fenómeno del vínculo del ciberespacio con el terrorismo trasciende a la utilidad como único objetivo de dañar ordenadores o redes informáticas. Es decir, destruir los sistemas informáticos tan solo puede ser considerado un objetivo del ataque, pero actualmente con el acceso global y universal a los dispositivos y redes, el ciberespacio se ha convertido también en un medio para la comisión de actos terroristas. En fin, podemos tomar la definición realizada por Mark M Pollitt, quien lo define como: *"el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos*

que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos" [18]

FIGURA 5. ***REPRESENTACIÓN PROPIA, REPRESENTACIÓN DE LA CONVERGENCIA DE LA PALABRA CIBERTERRORISMO***

Teniendo en cuenta que el ciberespacio no tiene fronteras, los ataques podrían provenir de cualquier punto del mundo, ejecutados por cualquiera de los siguientes actores [15] [19]:

- los Estados, mediante sus agencias de seguridad o entidades con finalidades específicas,
- los grupos extremistas, según su ideología o visión política,
- las organizaciones del crimen organizado y,
- las actuaciones delictivas individuales.

Fuentes potenciales de amenazas a la Ciberseguridad

Diversos tipos de organizaciones e individuos son capaces de dirigir ataques a las infraestructuras críticas de una Nación. Históricamente las embestidas mediante el uso de tecnologías a las infraestructuras han sido realizadas por un número relativamente pequeño de individuos u organizaciones. Sin embargo, en la actualidad, con la creciente dependencia de los sistemas informáticos y redes de datos para el desarrollo y mantenimiento de las infraestructuras críticas, un mayor número de

organizaciones e individuos pueden vulnerar las protecciones de acceso o causar daño a través del ciberespacio.

En esta inteligencia, los Gobiernos están observando con suma preocupación y prospectiva, la eventualidad de causar daños físicos mediante eventos informáticos, ya que podrían tener consecuencias devastadoras para las ciudades y consecuentemente hacia la población. A continuación, se enumeran las fuentes de amenazas que han sido identificadas por los servicios de inteligencia de EE. UU. en conjunto a otros países [19]:

- **Operadores de redes boot:** Los operadores de redes boot son piratas informáticos; sin embargo, en lugar de irrumpir en sistemas por el desafío o presumir derechos, se apoderan de múltiples sistemas con el fin de coordinar ataques y distribuir esquemas de phishing, spam y malware. Los servicios de estas redes a veces están disponibles en la DarkWeb (por ejemplo, comprar un ataque de denegación de servicio, servidores para retransmitir spam o ataques de phishing, etc.).

- **Grupos criminales:** Los grupos criminales buscan atacar los sistemas para obtener ganancias monetarias. Específicamente, los grupos del crimen organizado están utilizando spam, phishing y spyware / malware para cometer robo de identidad y fraude en línea. Los Espías corporativos internacionales y las organizaciones del crimen organizado también representan una amenaza, por su capacidad para conducir espionaje industrial y robo monetario a gran escala o para contratar o desarrollar talento de hackers.

- **Servicios de Inteligencia Extranjeros:** Los servicios de inteligencia extranjeros utilizan herramientas cibernéticas como parte de sus actividades de recopilación de información y espionaje. Además, varias naciones están trabajando agresivamente para desarrollar doctrinas de guerra de información, programas y capacidades, las que, permitirán que una sola entidad tenga un impacto significativo y grave al interrumpir las

infraestructuras críticas que apoyan el poder militar, impactos que podrían afectar la vida cotidiana de los ciudadanos.

- **Hackers:** Los Hackers, entran en las redes por un desafío personal o por los derechos de pertenecer a una comunidad. Si bien, alguna vez requirió habilidades específicas o amplios conocimientos informáticos, estos personajes pueden descargar scripts de ataque y protocolos de Internet, ejecutándolos contra los sitios que han definido como objetivo. Así, mientras las herramientas de ataque se han vuelto más sofisticadas, también se han vuelto más fáciles de usar. Por lo tanto, la población mundial de este tipo de amenaza plantea un peligro relativamente alto de interrupción aislada o breve que podría causar daños graves.

- **Usuarios internos:** La información privilegiada de una organización, por parte de un empleado disconforme, se considera, como una brecha de seguridad informática. No necesariamente, deben contar con un gran conocimiento sobre operaciones informáticas, porque su conocimiento del sistema objetivo, generalmente les permite obtener acceso sin restricciones para causar daños al sistema o robar datos de este. El presente concepto también incluye a proveedores externos, así como empleados que accidentalmente introducen malware en los sistemas.

- **Phishers:** Individuos, o pequeños grupos, que ejecutan esquemas de phishing con el intento de robar identidades o información para ganancia monetaria, además, suelen utilizar spam y spyware / malware para lograr sus objetivos.

- **Spammers:** Individuos u organizaciones que distribuyen correos electrónicos no solicitados con información oculta o falsa para vender productos, realizar esquemas de phishing, distribuir spyware / malware o atacar organizaciones (es decir, denegación de Servicio).

- **Programadores de Spyware y/o Malware:** Personas u organizaciones con intenciones maliciosas, llevan a cabo ataques contra usuarios, produciendo y distribuyendo spyware y/o malware. Varios virus y gusanos informáticos destructivos han efectuado un gran daño a sistemas informáticos, incluidos el macrovirus Melissa, el gusano Explore.Zip, el virus CIH (Chernobyl), Nimda, Code Red, Slammer y Blaster, por nombrar algunos.

- **Terroristas:** Los terroristas buscan destruir, incapacitar o explotar infraestructuras críticas, con la finalidad de amenazar la seguridad nacional, causar bajas masivas, debilitar la economía o dañar la moral y confianza de la sociedad hacia los Gobiernos. Estos actores, pueden utilizar esquemas de phishing o spyware / malware para autofinanciarse o recopilar información confidencial.

El Contexto Internacional

La utilización de internet como medio por los terroristas es un problema transnacional que necesita una respuesta integral más allá de los límites establecidos por las fronteras y entre los distintos sistemas nacionales de justicia penal. Teniendo en cuenta lo mencionado, las Naciones Unidas es el organismo encargado de desempeñar un papel fundamental para afrontar la cuestión transnacional, incentivando el debate y el constante intercambio de buenas prácticas entre sus Estados miembros, facilitando la creación de un consenso específico sobre los puntos comunes para afrontar la utilización de internet con fines terroristas [15].

Existe un marco jurídico especifico aplicable a esta temática que se tratan en una cantidad innumerable de Comités, como las Asambleas Generales y el Consejo de Seguridad, los tratados internaciones, la doctrina legal y el derecho internacional consuetudinario.

La Asamblea General en el año 2006 aprobó la Estrategia global contra el terrorismo[7], lo que representó un hito en las iniciativas multilaterales de lucha contra el terrorismo. Conforme con la mencionada Estrategia, los Estados miembros dictaminaron el siguiente plexo normativo [15]:

a. Condenar, de manera sistemática, inequívoca y firme, el terrorismo en todas sus formas y manifestaciones, independientemente de quién lo cometa y de dónde y con qué propósitos, puesto que constituye una de las amenazas más graves para la paz y la seguridad internacionales;
b. Adoptar medidas urgentes para prevenir y combatir el terrorismo en todas sus formas y manifestaciones;
c. Reconocer que la cooperación internacional y todas las medidas que [ellos] adopten para prevenir y combatir el terrorismo deben ajustarse a las obligaciones que les incumben en virtud del derecho internacional, incluida la Carta de las Naciones Unidas y los convenios y protocolos internacionales pertinentes, en particular las normas de derechos

[7] A/RES/60/288 Estrategia Global de las Naciones Unidas contra el Terrorismo, de fecha 08/09/2006.

humanos, el derecho de los refugiados y el derecho internacional humanitario;

d. Cooperar con las Naciones Unidas, teniendo debidamente en cuenta la confidencialidad, respetando los derechos humanos y de conformidad con otras obligaciones dimanadas del derecho internacional, a fin de estudiar formas de: *"1º) Coordinar esfuerzos, a nivel regional e internacional, para luchar contra el terrorismo en todas sus formas y manifestaciones en Internet; 2º) Utilizar Internet como instrumento para luchar contra la propagación del terrorismo, reconociendo al mismo tiempo que los Estados pueden necesitar asistencia a este respecto"*.

La Ciberseguridad como Riesgo Global

Como se puede observar en la figura 6, extraída del Informe de Riesgos Globales 2019, producido en la reunión anual del Foro Económico Mundial [20], en la que se destaca la preocupación en los encuestados sobre los Ciberataques, quedando en el cuarto lugar y quinto lugar (Cyber-attacks: Theft of data/money / Cyber-attacks: disruption of operations and infrastructure) respectivamente.

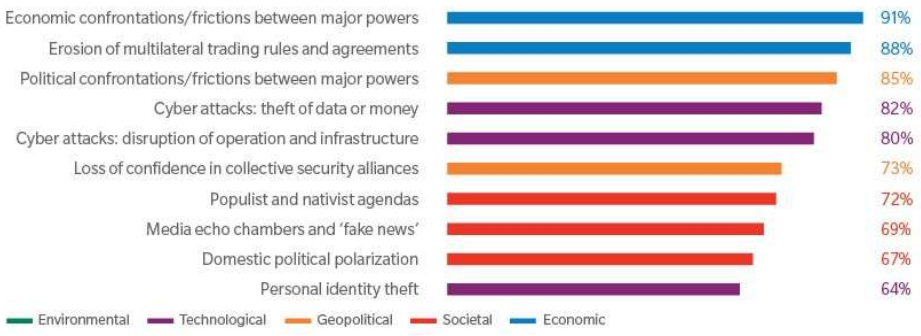

FIGURA 6. ***PERSPECTIVA DE RIESGO A CORTO PLAZO. PORCENTAJE DE ENCUESTADOS QUE ESPERAN QUE LOS RIESGOS AUMENTEN EN 2019. FUENTE: WORLD ECONOMIC FORUM GLOBAL RISKS PERCEPTION SURVEY 2018–2019*** **[20]**

Continuando, en la figura 7 más general y en la figura 8 más específico, se observa que existen dos riesgos vinculados a las TIC´s dentro de los 5 más probables de ocurrencia en el 2019, siendo el “Fraude o robo de datos” (Data fraud or theft) y los “Ciberataques” (Cyber-attacks).

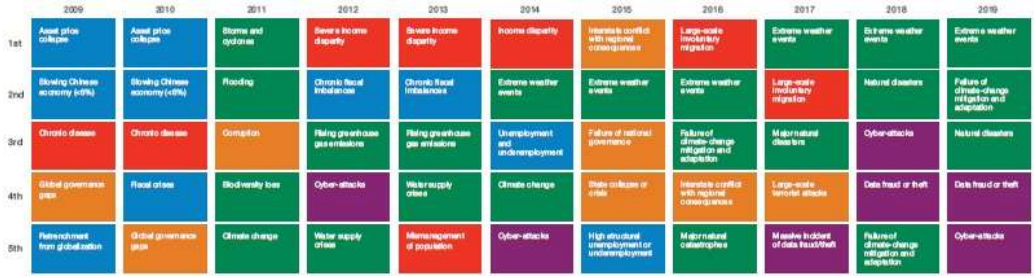

FIGURA 7. *LA DIRECCIÓN DE LA EVOLUCIÓN DE RIESGOS, PERIODO 2009-2019. FUENTE: WORLD ECONOMIC FORUM GLOBAL RISKS PERCEPTION SURVEY 2018–2019* [20]

FIGURA 8. *LOS 5 PRINCIPALES RIESGOS MUNDIALES EN TÉRMINOS DE PROBABILIDAD DURANTE 2019. FUENTE: WORLD ECONOMIC FORUM GLOBAL RISKS PERCEPTION SURVEY 2018–2019* [20]

La tecnología continúa jugando un rol importante en el moldeado del panorama del riesgo global para las personas, los gobiernos y los negocios.

En el GRPS[8], el fraude y robo masivo de datos fue clasificado en el 4° puesto de riesgo global (por probabilidad de ocurrencia) sobre un horizonte de 10 años, con los "ciberataques" ubicados en el quinto lugar.

Esto mantiene un patrón definido en relación con el año anterior (2018), respecto a los riesgos cibernéticos, consolidando su posición junto a los "riesgos ambientales", en el cuadro denominado "Panorama de Riesgo Global" como ALTO IMPACTO-ALTA PROBABILIDAD (figura 9).

Según el Informe de Riesgos Globales 2019, producido en la reunión anual del Foro Económico Mundial [20]:

- ✓ La gran mayoría de encuestados esperaba un aumento del riesgo en 2019 de ciberataques, producido por el *robo de dinero y datos* (82%) e *interrupción de operaciones* (80%). Este estudio, refleja que nuevas fuentes de inestabilidad están siendo originadas por la *profunda integración de tecnologías digitales en todos los aspectos de la vida*. Alrededor de dos tercios de los encuestados, espera que los riesgos asociados a "*fake news"* y "*robo de identidad*" se incrementen para el año siguiente, mientras que poco más del 65% opina lo mismo acerca de la *perdida de privacidad* en manos de compañías o gobiernos.

- ✓ Las vulnerabilidades cibernéticas pueden surgir de lugares inesperados, como fuera demostrado en las amenazas de Meltdown y Spectre, que involucraban debilidades en el hardware en lugar del software.

  Esto afectó potencialmente a todos los procesadores Intel producidos en los últimos 10 años. En el último año se vio una continua evidencia que los ciberataques plantean riesgos serios para las infraestructuras críticas.

- ✓ En julio próximo pasado, el gobierno estadounidense declaró que los hackers habían logrado el acceso a las salas de control de los servicios públicos de Estados Unidos.

[8] Global Risk Perception Survey (Encuesta Global de Percepción de Riesgo, por sus siglas en inglés)

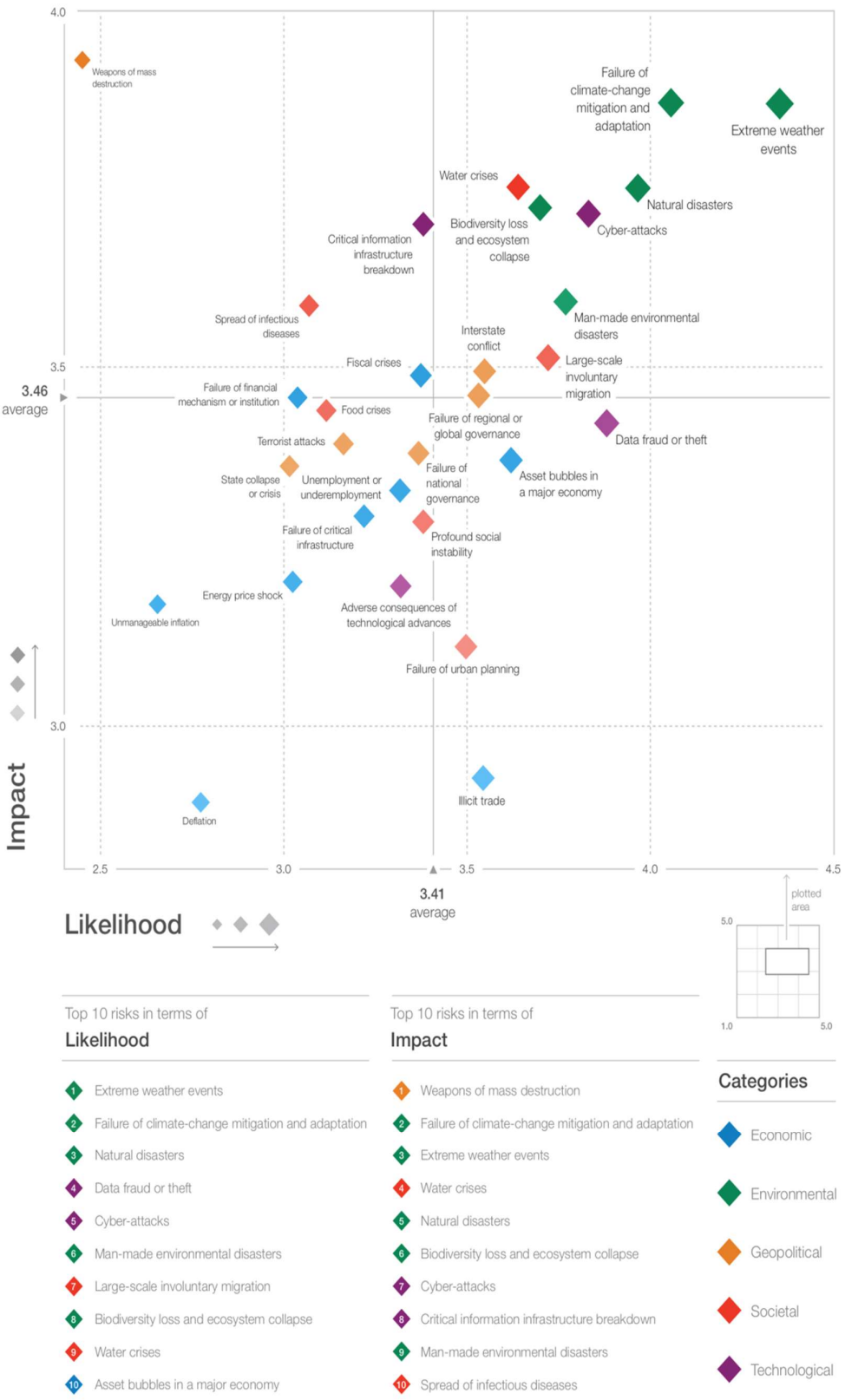

FIGURA 9. ***PAISAJES DE RIESGOS GLOBALES 2019. FUENTE: WORLD ECONOMIC FORUM GLOBAL RISKS PERCEPTION SURVEY 2018–2019*** **[20]**

- ✓ Los perjudiciales Ciberataques y los laxos protocolos de ciberseguridad, condujeron una vez más a una masiva filtración de información en el año 2018; la más importante fue en India, donde la base de datos (Aadhaar) de identificación biométrica de los habitantes de ese país sufrió múltiples ataques que comprometieron los registros de sus 1.1 billones de ciudadanos. En enero, se reportó que los criminales estaban vendiendo acceso a la información de la base de datos a un costo de 500 rupias (U$S 7 dólares estadounidenses aproximadamente) durante un periodo de 10 minutos, mientras que, en marzo una filtración en una campaña Estatal de servicios públicos permitió a cualquier persona descargar nombres y números de identificación. Por otro lado, las filtraciones de datos personales afectaron a unos 150 millones de usuarios de la aplicación MyFitnessPal y cerca de 50 millones de usuarios de Facebook.

- ✓ Una potencial vulnerabilidad en las tecnologías utilizadas en las infraestructuras críticas tiende a convertirse con severidad en una preocupación de seguridad a nivel nacional. El segundo riesgo de interconexión más frecuentemente citado en el GPRS de este año fue el nexo de los ciberataques con la ruptura de la información de las infraestructuras críticas.

- ✓ El aprendizaje automático o la inteligencia artificial (IA), se está volviendo más sofisticado y frecuente, con crecimiento potencial para amplificar riesgos o crear otros nuevos, particularmente como IoT (Internet of Things, por sus siglas en inglés), que interconecta miles de millones de dispositivos a lo largo y ancho del mundo.

- ✓ En una encuesta realizada el año pasado por Brookings, el 32% de los encuestados dijo que veían a la IA como una amenaza para la humanidad, mientras que solo el 24% no lo hacía.

- ✓ IBM reveló el año pasado, un malware que puede ocultar una amenaza conocida -WannaCry- en una aplicación de videoconferencia, activándose

solo cuando reconoce la cara del objetivo deseado. Es probable que estén ocurriendo innovaciones similares en otros campos. Por ejemplo, se destaca el potencial para actores maliciosos en biología sintética para usar IA para crear nuevos patógenos. Uno de los futuros shocks considera las potenciales consecuencias de la "computación afectuosa" -refiriéndose a que la IA puede reconocer, responder y manipular las emociones humanas.

- ✓ Entre los más difundidos y disruptivos impactos, ocurridos recientemente, de la IA en años ha sido su rol en el aumento de las cámaras de eco de media y las "fake news", un riesgo que el 69% de los encuestados del GRPS espera que se acreciente en años venideros. Los investigadores el último año estudiaron la trayectoria de 126.000 tweets y encontraron que aquellos que contenían fake news superaron consistentemente a aquellos que contenían información verdadera, en porcentaje llegando a 1.500 personas, seis veces más rápido.

- ✓ Una posible razón, mencionada por los investigadores es que las fake news tiende a evocar emociones potentes: Los tweets fake tienden a poseer palabras asociadas con sorpresa y disgusto, muestras que los tweets certeros evocan palabras asociadas con la tristeza y la confianza. La interacción entre las emociones y la tecnología es probable que se convierta en una fuerza cada vez más disruptiva.

Alcance del Terrorismo orientado al Ciberespacio

Para entender la potencialidad que ofrece el ciberespacio a las organizaciones criminales, orientadas tanto a la utilización de los sistemas informáticos como medio u objetivo de los ataques, es necesario realizar un breve análisis comparativo sobre variantes o matrices en las cuales se observen los diferentes alcances o beneficios del uso de las tecnologías en las entidades delictivas.

Si se toma como ejemplo una *matriz terrorista tradicional* (figura 10) de dos organizaciones diferentes, se puede observar que las actividades, alcances, acciones, modos de operación, entre otros factores, se encuentran acotados tanto geográfica como operativamente. En cambio, si se toma como ejemplo y se compara las mismas organizaciones con aplicación o uso de las TIC´s, tal como se muestra en la *matriz ciberterrorista* (figura 11), se contemplará la suma de aptitudes, beneficios o usos que el ciberespacio aporta a la actividad criminal.

MATRIZ TERRORISTA		
GRUPO	**TIGRES TAMILES**	**SECTA VERDAD SUPREMA**
AUTOR	Grupo	Grupo
LUGAR	Sri Lanka	Japón
ACCIÓN	Amenazas/ Violencia	Violencia
HERRAMIENTA	Secuestro/hostigamiento	Gas nervioso
MOTIVACIÓN	Social/Cambio político	Dominación mundial

FIGURA 10. ***REPRESENTACIÓN PROPIA CORRESPONDIENTE A UNA MATRIZ TERRORISTA TRADICIONAL.***

MATRIZ CIBERTERRORISTA		
GRUPO	**TIGRES TAMILES**	**SECTA VERDAD SUPREMA**
AUTOR	Grupo/Individuo	Grupo/Individuo
LUGAR	Sri Lanka/Londres/ Australia/Global	Japón/Estados Unidos/Global
ACCIÓN	Amenazas/ Violencia/Captación/ Entrenamiento/Estrategias	Violencia/Captación/Entrenamiento/Estrategias
HERRAMIENTA	Secuestro/Hostigamiento/Propaganda/Entrenamiento	Gas nervioso/Entrenamiento
MOTIVACIÓN	Social/Cambio político	Dominación mundial

FIGURA 11. ***REPRESENTACIÓN PROPIA CORRESPONDIENTE A UNA MATRIZ TERRORISTA CIBERTERRORISTA.***

Gracias a esta matriz comparativa, sin limitarse a la actividad utilizada como ejemplo, se está en condiciones de entender pragmáticamente las facilidades que ofrece el ciberespacio a las tareas y alcances de los grupos cualesquiera sean sus fines.

En la siguiente sección se tratará de mencionar los principales casos, o más significativos, registrados a través de los años como sucesos que atentaron a la ciberseguridad producto del ataque a los sistemas informáticos

o, simplemente, efectuados a través de ellos. En suma, se evidenciará como la evolución de las tecnologías informáticas aumenta la magnitud, o facilitan, un mayor impacto o alcance de los objetivos. Estos últimos causados por grupos o por individuos con acceso al conocimiento y la tecnología.

Historial de ataques perpetrados

Los ataques a infraestructuras críticas no se ejecutaron en la actualidad, vienen transcurriendo de hace décadas, pudiéndose elaborar un análisis cronológico de los más destacados [2]:

- **Oleoducto siberiano:** Al nombrar las palabras ciberataques a infraestructuras críticas, es inevitable que el término Internet sea pensado casi de forma inmediata. Sin embargo, el primer ciberataque sucedió tiempo antes de que Internet existiera tal como la conocemos. Tuvo lugar en **1982,** en el cual los atacantes consiguieron instalar un troyano en el sistema SCADA el que controlaba un oleoducto siberiano, provocándose una enorme explosión en el mismo. El ataque fue diseñado y ejecutado por la C.I.A., el que se mantuvo en secreto hasta el año 2004, cuando Thomas C. Reed, quien fuera subsecretario del Ministerio de Defensa de los Estados Unidos y asesor del expresidente Ronald Reagan, publicara el libro “At the Abyss: An Insider’s History of the Cold War”, donde exponía esta historia.

- **Chevron:** El siguiente incidente sucedió en el año **1992,** cuando un trabajador fuera despedido de la compañía petrolera Chevron, quien hackeo los servidores centrales en las sedes de la compañía en las ciudades de Nueva York y San José, donde se encargaban del sistema de alertas, siendo estos reconfigurados para que no funcionen cuando se pusieran en marcha. No se identificó el sabotaje hasta que, en la ciudad de Richmond, California, se produjo un incidente en el que se liberó una sustancia nociva y el sistema no emitió la alerta correspondiente, lo que puso en riesgo a miles de personas en el transcurso de 10 horas, en las que el sistema estuvo sin funcionar.

- **Salt River Project:** En agosto de **1994** Lane Jarret Davies consiguió ingresar a la red del Salt River Project mediante un módem, consiguiendo acceso a información sensible y borrando ficheros de los sistemas que realizaban la monitorización, entrega de agua y electricidad a sus consumidores. Además, accedió a información personal y financiera tanto de clientes como de trabajadores.

- **Aeropuerto Worcester:** El sector aéreo también ha sufrido ataques dirigidos. El 10 de marzo de **1997** un hacker se introdujo en el sistema de control utilizado para las comunicaciones de tráfico aéreo en el aeropuerto de Worcester, Massachusets, produciendo una falla que dejó inutilizado el sistema de telefonía por un lapso de 6 horas. En definitiva, afectó a los servicios telefónicos de la torre de control, al departamento de bomberos del aeropuerto, el del servicio meteorológico y la totalidad de las compañías aéreas que operaban en el aeropuerto.

- **Gazprom:** En el año **1999,** un hacker consiguió traspasar los sistemas de seguridad de la organización rusa Gazprom –con ayuda de un trabajador infiel de la empresa- obteniendo control de los sistemas SCADA de la compañía, en definitiva, la central encargada de manejar los flujos de gas. Se utilizó un troyano. Afortunadamente no se produjeron mayores consecuencias y en unas horas la empresa recuperó el control.

- **Maroochy Water System:** Dos años de prisión fue la condena impuesta a un ex empleado del Maroochy Water System que en el año **2000** hackeó con información robada a la empresa el sistema que controlaba el agua, provocando un derrame de casi un millón de litros de aguas residuales en un río cercano, lo que inundo también los bajos de un hotel.

- **Planta de gas:** Una planta encargada del procesamiento de gas operada por una compañía petrolífera de EE. UU. sufrió un ataque durante **2001.** Luego de una investigación durante 6 meses, se averiguó que fue ejecutado por uno de sus proveedores, que buscando encubrir un error que habían provocado en uno de los ordenadores crearon esta "distracción" hackeando 3 sistemas de la empresa y provocando el corte en el suministro de gas en hogares y empresas de un país europeo.

- **PDVSA:** En diciembre de **2002,** la petrolera venezolana PDVSA sufrió un ataque que disminuyo la producción de petróleo del país durante ese día de 3 millones de barriles a 370.000. El ataque se perpetro hackeando distintos ordenadores dentro de la compañía. Se ejecuto mientras personal de la empresa estaba en huelga, por lo que se dedujo a que se trató de un sabotaje realizado por uno de sus empleados.

- **Semáforos de los Ángeles:** En **2006,** dos ingenieros encargados del tráfico de Los Ángeles hackearon los semáforos de la ciudad durante una protesta laboral. Cambiaron la programación de algunos de ellos – estratégicamente escogidos en cruces muy transcurridos- para que la luz roja para vehículos se prolongara más tiempo activada, lo que genero grandes dificultades.

- **Tranvías de Lodz:** En **2008**, un estudiante polaco de 14 años hackeó el sistema de tranvías de la ciudad de Lodz, en Polonia. Resultando: 4 tranvías descarrilaron, produciéndole heridas a 12 personas. El estudiante elaboro un control infrarrojo similar a un control de televisión mediante el cual podía controlar los cruces de vías.

- **Juegos Olímpicos:** En **2010**, el presidente electo Barack Obama, en su llegada a la casa blanca intensifico un programa secreto de ciberataques, el que tenía como objetivo el programa nuclear de Iran,

logrando deshabilitar 1000 centrifugadoras de la planta situada en Natanz. Pero por un error en la programación del troyano, infecto una computadora portátil de un científico iraní, quien lo difundió involuntariamente por la Red, infectando computadoras en Irán, Indonesia, India y Estados Unidos. Más adelante se detalla en profundidad. [21]

- **Saudi Aramco:** En **2012,** la compañía petrolera más grande del mundo, Saudi Aramco, fue víctima de un ataque dirigido a su casa matriz. Los atacantes habían conseguido acceso a la red interna mediante el ataque a uno de sus empleados, desde donde consiguieron acceso a 30.000 computadoras de la firma. Los atacantes eliminaron el contenido de la totalidad de computadoras mientras que en las pantallas se mostraba una bandera estadounidense en llamas. Un grupo autodenominado “Cutting Sword of Justice” hizo mención adjudicándose el ataque.

- **RasGas:** Luego de dos semanas transcurridas del ataque ejecutado a Saudi Aramco, la firma RasGas, la segunda mayor productora de gas natural licuado del mundo sufrió un ataque con un idéntico malware utilizado en la petrolera saudí. Por el transcurso de varios días, la red interna de la empresa como su página web estuvieron inoperativas.

- **Planta metalúrgica alemana:** En **2014**, una planta metalúrgica de Alemania sufrió un ataque. Mediante el uso de técnicas de ingeniería social los atacantes consiguieron acceder al ordenador de un empleado, y desde allí acceso a la red interna del sistema de control. Produciendo esto, que al pretender apagar uno de los altos hornos este no obedeció quedando encendido, lo que produjo un daño masivo en las instalaciones.

- **Red eléctrica ucraniana:** Durante **2015**, Ucrania sufrió un ciberataque dirigido a su red eléctrica, lo que dejó sin suministro eléctrico a más de 600.000 habitantes del país.

Primer ciberataque de la historia contra la infraestructura de Internet

Si bien este es un largo historial, el primer ciberataque en la historia ejecutado contra la infraestructura de internet, se llevó a cabo el 27 de abril del 2007. Esto ocurrió en Estonia, país que es identificado como ***la nación más digital del planeta*** ya que el 99% de los servicios que ofrece el estado están online y 98% de los ciudadanos tienen una identificación digital, mediante una serie de ataques de forma simultaneas contra los sitios web de distintos organismos gubernamentales, produjeron un colapso total de los mismos. El Ministro de Relaciones Exteriores del Gobierno Estonio, atribuyo la responsabilidad de los ataques públicamente al Gobierno Ruso, no pudiendo ofrecer pruebas contundentes que demostraran su suposición [2].

El ciberataque a infraestructuras críticas más conocido de la historia: Stuxnet

En 2010 tuvo lugar el más conocido ataque a una infraestructura crítica de la historia de la humanidad, bautizado como Stuxnet. A la fecha se sabe que fue un ataque coordinado entre la inteligencia israelí y la norteamericana, el que tenía como objetivo, realizar un sabotaje a un programa nuclear iraní.

Esto se perpetro, mediante la utilización de un gusano, que fuera creado especialmente para este fin, por el cual, al infectar las computadoras de la red por las que se controlaban las maquinas centrifugadoras de uranio de la planta iraní de la ciudad de Natanz, hacían que las mismas funcionen a su máxima velocidad, pero a los sistemas de control le enviaban la información de un funcionamiento normal. Esto provocó la rotura física de todas las centrifugadoras de uranio de la planta, siendo este, el desencadenante para que se tome conciencia sobre los ciberataques [2].

Metodologías utilizadas para la perpetración de ciberataques

Ya habiéndose analizado su definición, los Ciberataques cuentan con características comunes entre ellos, por lo que se las puede agrupar de la siguiente manera [22]:

- **Inversión mínima o nula:** se disponen de innumerables herramientas de libre distribución, pudiéndose ser descargadas para efectuar ciertos ataques, permitiéndose ejecutar en los múltiples sistemas operativos.

- **Facilidad de uso:** con el avance de la tecnología, las herramientas poseen interfaces sencillas y amigables, juntamente con referencias para hacer uso de las mismas, permitiendo esto, realizar ataques estándares o básicos, no necesitando de una experticia técnica elevada; inclusive, algunas herramientas se estudian en las capacitaciones de Ethical Hacking o en las distintas cátedras del ámbito académico.

- **Certeza:** estos ciberdelincuentes cuentan con una alta probabilidad de lograr su objetivo inicial, dado que, desde el punto de vista de los objetivos existen vulnerabilidades del día 0 o desconocidas, que impactan tanto sobre el software y hardware que los soporta, baja o poca inversión en tecnologías para aplicar seguridad informática, baja concientización en las Organizaciones, Instituciones y/o personas.

- **Baja exposición y riesgo para el ciberatacante:** atribuir el hecho consumado a un ciberdelincuente se torna casi imposible, dado que los mismos utilizan herramientas que implementan técnicas para evitar el rastreo del punto de origen del ataque, además, de ser muy difícil la aplicabilidad de una ley que tipifique el delito, ya que, el ataque puede venir dirigido de cualquier punto del mundo, no disponiendo legislación alguna que trate esta temática, utilizando la INTERNET como medio para llegar a un determinado objetivo.

Según la Oficina Federal de Investigaciones de los Estados Unidos, los terroristas, los delincuentes transnacionales y los servicios de inteligencia se están dando cuenta rápidamente y utilizan herramientas como virus informáticos, troyanos, gusanos, bombas lógicas y programas de espionaje ("sniffers") con los que pueden negar el acceso, degradar la integridad de, interceptar o destruir datos. A continuación, se detallan metodologías y herramientas que son utilizadas para perpetrar ciberataques [19]:

- **Exploit tools (Herramientas de explotación):** Herramientas sofisticadas y fácilmente accesibles, por las cuales los ciberdelincuentes con diversos niveles de habilidades y/o conocimientos puedan hacer uso, para determinar vulnerabilidades y obtener acceso a sistemas específicos.

- **Logic bombs (Bombas lógicas):** Una forma de sabotaje en el que un programador inserta un código fuente, por el cual el programa realizara una acción destructiva cuando se ejecute algún evento que lo desencadene.

- **Phishing:** La creación y el uso de correos electrónicos y/o sitios web, diseñados para asimilarse a negocios legítimos, instituciones financieras y agencias gubernamentales, con el fin de engañar a los usuarios para que divulguen sus datos personales, como los bancarios y financieros, información de cuenta y contraseñas. Posteriormente *los phishers* toman esa información y la usan para propósitos criminales, como robo de identidad y fraude.

- **Denial of Service (Denegación de Servicio):** un método de ataque de una sola fuente que niega el acceso del sistema a usuarios legítimos al abrumar la computadora objetivo con mensajes y bloquear el tráfico legítimo. Puede evitar que un sistema pueda intercambiar datos con otros sistemas o usar Internet.

- **DDoS -Distributed Denial of Service (Denegación de Servicio Distribuida):** una variante del ataque de denegación de servicio que utiliza un ataque coordinado desde un sistema distribuido de computadoras en lugar de desde una sola fuente. A menudo utiliza gusanos para propagarse a múltiples computadoras que luego pueden atacar al objetivo. Un ejemplo actual de este tipo de ataque fue realizado como un golpe masivo de Denegación de Servicio Distribuido que dejo paralizados los servidores de empresas como Twitter, NetFlix, NYTimes y PayPal a lo largo de todos los Estados Unidos de América, el día 21 de Octubre de 2016. Esto fue el resultado de un inmenso ataque que tuvo como perpetradores millones de direcciones IP y software malicioso, según #Dyn victima principal del ataque. Una de las fuentes del ataque fueron dispositivos infectados por Mirai botnet [23].

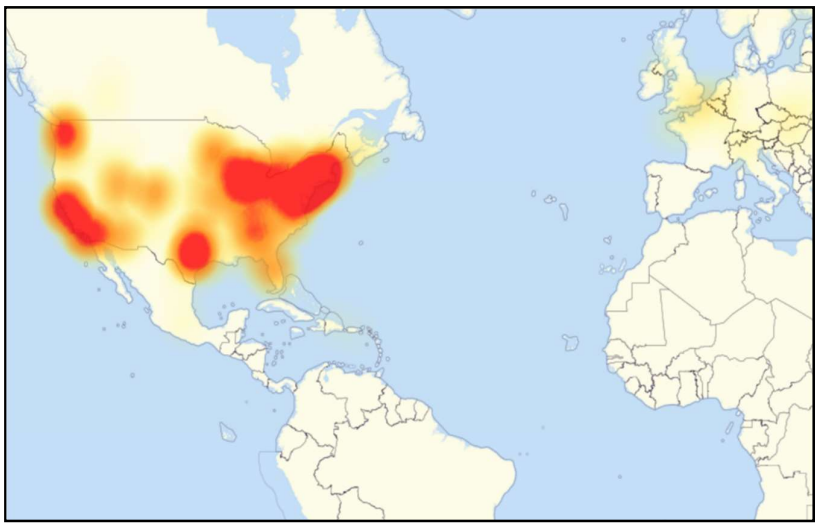

FIGURA 12. *MAPA QUE MUESTRA LAS ÁREAS AFECTADAS POR EL CORTE DE INTERNET EL VIERNES 21 DE OCTUBRE DE 2016* **[23]**

- **Sniffer (Programas de Espionaje):** Sinónimo de sniffer de paquetes. Un programa que intercepta los datos enrutados y examina cada paquete en busca de información específica, como las contraseñas transmitidas en texto plano.

- **Trojan horse (Caballo de Troya):** Un programa de computadora que oculta código dañino. Un caballo de Troya generalmente se encubre como un programa útil que un usuario desearía ejecutar.

- **Virus:** Un programa que infecta archivos informáticos, generalmente programas ejecutables e insertando una copia de sí mismo en el archivo. Estas copias generalmente se ejecutan cuando el archivo infectado se carga en la memoria, lo que permite que el virus infecte otros archivos. A diferencia del gusano informático, un virus requiere la participación humana (generalmente involuntaria) para propagarse.

- **War dialing (Marcación de Guerra):** Programas simples que marcan números de teléfono consecutivos en busca de módems.

- **War driving (Manejo de Guerra):** Un método para ingresar a las redes inalámbricas de computadoras mediante la utilización de una computadora portátil, antenas y un adaptador de red inalámbrica, que implica patrullar ubicaciones para obtener acceso no autorizado.

- **Worm (Gusano):** Programa informático independiente que se reproduce al copiarse de un sistema a otro mediante una red de computadoras. A diferencia de los virus informáticos, los gusanos no requieren la participación humana para propagarse.

- **Phlooding:** Este término hace referencia a un ataque dirigido contra los servidores de autenticación de una organización, enviando en forma simultánea múltiples solicitudes de autenticación, buscando de esta manera sobrecargar los servidores, ocasionando una denegación de servicio distribuida [15].

En este apartado, se han detallado diversas metodologías y herramientas que los ciberdelincuentes utilizan para ejecutar ataques informáticos, de manera individual o en grupo, con el objeto de potenciar el efecto deseado. Estos factores, nuevamente dejan en evidencia la importancia de la necesidad de diseñar e implementar un marco de trabajo de ciberseguridad, en el que se valore a la Organización en forma transversal, con la finalidad de generar conciencia entre los individuos,

independientemente su jerarquía o funciones dentro de ella, sumado a una comunicación eficaz al momento de tratar este tópico. Atendiendo esta problemática, diferentes organismos internacionales se han alineado en la cuestión de la ciberseguridad y ciberdefensa. Siguiendo esa directriz, actualmente se encuentran vigentes varias normas, estándares y procedimientos que son instrumentados como guía, como, por ejemplo, las ISO/IEC 27001:2013, COBIT, las directrices de COSO o NIST SP 800-53, por solo nombrar algunas de ellas.

Modelos de Gobernanza a Nivel Internacional

Contexto Normativo Internacional

Seguidamente, se describirán las características de distintos modelos de gobernanza en materia de Ciberseguridad a nivel internacional, juntamente, con el modelo local recientemente publicado.

Para entender la importancia que cumple una Estrategia Nacional de Ciberseguridad en el rol del funcionamiento de un País, se deberá entender que comprende este significado, pudiéndose tomar la definición que nos ofrece ENISA: *"siendo un plan de acción diseñado para mejorar la seguridad y la capacidad de recuperación de las infraestructuras y servicios nacionales. Es un enfoque de alto nivel de arriba hacia abajo para la seguridad cibernética que establece una gama de objetivos y prioridades nacionales que deben lograrse en un marco de tiempo específico"* [24].

La principal normativa multilateral que regula la Ciberseguridad es el Convenio sobre Ciberdelincuencia del Consejo de Europa, más conocido como Convenio sobre Cibercriminalidad de Budapest, firmado el 23 de noviembre de 2001, cuyo objetivo principal, es el de prevenir las conductas delictivas en el ciberespacio (Convenio sobre la Ciberdelincuencia, 2001). Otro texto legal concerniente a esta materia es la Resolución AG/RES 2004 (XXXIV-O/04), de la Asamblea General de la Organización de Estados Americanos (OEA), desde la cual se define una estrategia multidimensional para definir los desafíos que trae aparejada la seguridad cibernética (OEA, 2004). Además, es de mencionar la Declaración de la Cumbre de Gales, de la Organización del Tratado del Atlántico Norte (OTAN), suscrita en 2014 (NATO, 2014); y la Declaración sobre la Protección de Infraestructuras Críticas ante las Amenazas Emergentes, aprobada en la V Sesión Plenaria de la OEA, el 20 de marzo de 2015 (OEA, 2015).

Se han seleccionado Países de los continentes americano (Estados Unidos de América, por estar en la vanguardia de la tecnología y Uruguay) y Europeo (en el caso de este continente, los seleccionados fueron aquellos que hayan elaborado Estrategias de Seguridad tras la publicación de la Estrategia

Europea de Seguridad: Reino Unido, Estonia, España, Francia y Alemania), con la finalidad de que sea diverso y enriquecedor, ya que, poseen complejidades y particulares por las cuales se los identifica:

Continente	Americano	Europeo
Descripción	América es el segundo continente más grande de la Tierra, después de Asia. Ocupa gran parte del hemisferio occidental del Planeta	Europa es uno de los continentes que conforman el supe continente euroasiático, situado entre los paralelos 35º 30' y 70º 30' de latitud norte
Superficie	42.55 millones km²	10.18 millones km²
Población	1.002 miles de millones (2016)	741.4 millones (2016)
Densidad	23.6 hab./km²	70 hab./km²
Subdivisiones	América del Norte, del Sur y Central	Unión Europea, Consejo de Europa, etc.

TABLA 3. COMPARATIVA DE LOS CONTINENTES A LOS QUE PERTENECEN LOS PAÍSES EN LOS QUE SE HA EVALUADO SUS ESTRATEGIAS.

En el siguiente mapa se observan los países que han sido elegidos para realizar un análisis comparativo de sus Estrategias Nacionales de Ciberseguridad.

FIGURA 13. PAÍSES ELEGIDOS PARA REALIZAR LA COMPARACIÓN DE SUS ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD: CANADÁ, ESTADOS UNIDOS DE NORTEAMÉRICA, URUGUAY, REINO UNIDO, ESTONIA, ESPAÑA, FRANCIA Y ALEMANIA.

N°	País	Año	Denominación	Extensión (Pag.)
1	República Oriental del Uruguay	2018	Marco de Ciberseguridad	175
2	Reino Unido	2016	National Cyber Security Strategy	59
3	Canadá	2018	National Cyber Security Strategy	40
4	Estados Unidos de América	2018	National Cyber Strategy	40
5	Estonia	2019	Cybersecurity Strategy	71
6	España	2019	Estrategia Nacional de Ciberseguridad	68
7	Francia	2015	Strategie Nationale Securite	44
8	Alemania	2011	Cyber Security Strategy for Germany	20

TABLA 4. RESUMEN COMPARATIVO ENTRE ESTRATEGIAS

A continuación, se desplegarán ciertos aspectos considerados significativos de las estrategias de ciberseguridad de Estados Unidos de América, de la República Argentina, del Reino de España y de la República de Estonia, por ser, las más actuales en sus continentes. La información que se analizó es de acceso público, por lo que se encuentra en los sitios oficiales de los organismos que cumplen la función de elaborar los planes de ciberseguridad de cada uno de los países elegidos.

Estrategias Nacionales de Ciberseguridad

Estrategia Nacional de los Estados Unidos de América

Su origen se remonta a el período de Barack Obama como presidente, quien en función emitiera la Orden Ejecutiva (EO) N° 13.636 "Mejora de la Ciberseguridad de las Infraestructuras Críticas" el 12 de febrero de 2013, que estableció: *"Es política del Gobierno de los Estados Unidos aumentar el volumen, la puntualidad y la calidad de la información sobre amenazas cibernéticas que se comparte con las entidades del sector privado de los EE. UU. para que estas entidades puedan protegerse y defenderse mejor de las amenazas cibernéticas"* [25].

Esta responsabilidad recae sobre el Departamento de Seguridad Nacional de los Estados Unidos, siendo sus objetivos:

1. Asegurar que la Fuerza Conjunta pueda cumplir sus misiones en un entorno de ciberespacio disputado;
2. El fortalecimiento de la fuerza conjunta, mediante la realización de operaciones en el ciberespacio que mejoren las ventajas militares de los EE. UU.;
3. Defender la infraestructura crítica de EE. UU. de la actividad cibernética maliciosa solo o como parte de una campaña, la que podría causar un incidente cibernético significativo para la Nación;
4. Asegurar la información y los sistemas informáticos del Departamento de Defensa contra la actividad cibernética maliciosa, incluido el Departamento de Defensa información sobre redes no pertenecientes al DoD;
5. Expansión de la cooperación cibernética del Departamento de Defensa con socios interinstitucionales, industriales e internacionales.

La Estrategia Nacional, cuenta con los siguientes pilares rectores:

Pilar I. Proteger al pueblo estadounidense, la patria y el estilo de vida estadounidense: Gestione los riesgos de ciberseguridad para aumentar la seguridad, la resistencia de la información y los sistemas de información de la nación.

Pilar II. Promover la prosperidad americana, preservando la influencia de los Estados Unidos en el ecosistema tecnológico y el desarrollo del ciberespacio como motor abierto del crecimiento económico, la innovación y la eficiencia.

Pilar III. Preservar la paz a través de la fuerza: identifique, contrarreste, interrumpa, degrade y disuada el comportamiento en el ciberespacio que es desestabilizador y contrario a los intereses nacionales, al

tiempo que preserva la superación de Estados Unidos en y a través del ciberespacio.

Pilar IV. *Avanzar con la influencia estadounidense: Preserve la apertura, interoperabilidad, seguridad y confiabilidad a largo plazo de Internet, que respalda y se ve reforzada por los intereses de los Estados Unidos.* [26]

Estrategia Nacional de la República Argentina

En la República Argentina, desde el desarrollo de la Estrategia Nacional de Ciberseguridad, a cargo del COMITÉ DE CIBERSEGURIDAD, creado por el Decreto N° 577 del 28 de julio de 2017, dependiente este, del Poder Ejecutivo Nacional; la Secretaría de Modernización de Gobierno emitió en el Boletín oficial de la República Argentina la Resolución 829/2019, la cual aprueba la Estrategia Nacional de Ciberseguridad, presente en el Anexo I de dicha resolución.

Los principios rectores de la Ciberseguridad son:

- Respeto por los derechos y las libertades individuales.
- Liderazgo, construcción de capacidades y fortalecimiento federal.
- Integración internacional.
- Cultura de Ciberseguridad y responsabilidad compartida.
- Fortalecimiento del desarrollo socioeconómico.

Siendo sus objetivos:

1. Concientización del uso seguro del Ciberespacio: En el marco del presente documento, es el proceso de formación del discernimiento en cuanto a los riesgos que conlleva el uso de las tecnologías, entender la cultura del Ciberespacio y junto a ello la adopción de hábitos basados en las mejores prácticas.

2. Capacitación y educación en el uso seguro del Ciberespacio: En el marco del presente documento, es entendido como el proceso de

formación y adquisición de conocimientos, aptitudes y habilidades necesarias para un uso seguro del Ciberespacio.

3. Desarrollo del marco normativo: Adecuar y generar las normas jurídicas, marcos regulatorios, estándares y protocolos, para hacer frente a los desafíos que plantean los riesgos del ciberespacio, asegurando el respeto de los derechos fundamentales.

4. Fortalecimiento de capacidades de prevención, detección y respuesta: Fortalecer las capacidades de prevención, detección y respuesta frente al uso del Ciberespacio con fines ilegales.

5. Protección y recuperación de los sistemas de información del Sector Público: Garantizar que los sistemas de información que utiliza el Sector Público, incluyendo sus organismos descentralizados, posean un adecuado nivel de seguridad y recuperación.

6. Fomento de la industria de la Ciberseguridad: Promover el desarrollo de la industria nacional en los sectores vinculados a la Ciberseguridad.

7. Cooperación Internacional: Contribuir a la mejora de la Ciberseguridad en el ámbito internacional.

8. Protección de las Infraestructuras Críticas Nacionales de Información: Fortalecimiento de la cooperación público-privada en resguardo de las infraestructuras críticas de la información del país. [4]

Estrategia Nacional del Reino de España

En cuanto al modelo español, el Consejo Nacional de Ciberseguridad es la entidad subordinada al presidente, que tiene a su cargo el desarrollo de la Ciberseguridad, tanto en lo que respecta a la situación de la sociedad civil,

la academia, las compañías privadas y los sectores públicos estratégicos del país.

La Estrategia Nacional de Ciberseguridad fue actualizada en el 2019, y consta de 5 Capítulos, que se describen a continuación:

- Primer Capítulo titulado “El ciberespacio, más allá de un espacio común global”, el que proporciona una visión del ámbito de la Ciberseguridad, los avances que surgieron desde aquella primera Estrategia publicada en el año 2013. Se especifican los lineamientos, por lo que, se considera una iniciativa del Gobierno, identificando las principales características que impulsan su desarrollo.

- Segundo Capítulo titulado “Las amenazas y desafíos en el ciberespacio”, se identifican las principales amenazas del ciberespacio, clasificándolas en dos grandes categorías: en primer lugar, las que amenazan los activos que conforman el ciberespacio, y en segundo lugar, aquellos que lo utilizan como medio para realizar sus actividades maliciosas o ilícitas de cualquier índole.

- Tercer Capítulo titulado “Propósito, principios y objetivos para la Ciberseguridad”, se aplican los principios rectores de la Estrategia de Seguridad Nacional 2017 (Unidad de acción, Anticipación, Eficiencia y Resiliencia) a los cinco objetivos que se identifican para la Seguridad Nacional del País.

- Cuarto Capítulo titulado “Líneas de acción y medidas”, se desarrollan los tópicos mencionados en el Capítulo anterior, estableciéndose siete líneas de acción, identificándose las medidas a cumplir para cada uno de ellos. Las líneas de acción tienen como finalidad:

    - Reforzar las capacidades ante amenazas provenientes del ciberespacio.
    - Garantizar la seguridad y resiliencia de los activos estratégicos del País.

- Impulsar la Ciberseguridad de ciudadanos y empresas.
- Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio.
- Potenciar la industria nacional de Ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital.
- Contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable, en apoyo de los intereses nacionales y desarrollar una cultura de Ciberseguridad de manera que contribuya al Plan integral de Cultura de Seguridad Nacional.

- Quinto Capítulo titulado "La Ciberseguridad en el Sistema de Seguridad Nacional", se define la Estructura Orgánica de la Ciberseguridad Nacional, dependiente del Presidente directamente, la que se compone de tres órganos: el Consejo de Seguridad Nacional, cumpliendo la función de Comisión Delegada del Gobierno para la Seguridad Nacional; el Consejo Nacional de Ciberseguridad, que apoya al Consejo de Seguridad Nacional y asiste al Presidente en la dirección y coordinación de la Política, regulando la colaboración entre sector Público y Privado; por último, el Comité de Situación, encargado de afrontar y gestionar la situación de crisis en cualquier ámbito, que por su problemática, desborden las capacidades de respuesta establecidas. [27]

Estrategia Nacional de la República de Estonia

El modelo de Estonia tiene como base el accionar del Consejo de Ciberseguridad, organismo con origen en el año 2009, en el interior del Comité de Seguridad de dicho Gobierno, con la misión principal de: "contribuir a allanar la cooperación interinstitucional y supervigilar la implementación de las metas de la Estrategia de Ciberseguridad del país".

Como se ha mencionado anteriormente, Estonia, es un país considerado 100% digital, ofreciéndoles a sus ciudadanos la posibilidad de utilizar sus servicios totalmente online. Esto conlleva, peligros en lo que respecta a la Ciberseguridad, ya que si se vulnera la plataforma utilizada podría ser devastador para el Gobierno.

Los objetivos definidos a cumplir en la Estrategia de Ciberseguridad son [28]:

1. Una sociedad digital sostenible: Estonia es una sociedad digital sostenible, confiando en una fuerte resiliencia tecnológica y preparada ante la ocurrencia de una emergencia.
2. Una Industria de Ciberseguridad, generando investigación y desarrollo: la industria de Ciberseguridad en estonia es fuerte, innovadora, orientada a la investigación y globalmente competitiva, cubriendo todas las competencias clave para el Gobierno.
3. Un líder internacional contribuyente: Estonia sea un socio creíble y capaz en internacionalmente.
4. Una sociedad ciberalfabetizada: Estonia sea una cibersociedad alfabetizada, asegurando suficiente talento con visión de futuro. [28]

Del análisis detallado de estas políticas se destaca, que España juntamente con Estonia, poseen una estructura muy solvente para afrontar los desafíos que procura la Ciberseguridad, teniendo en cuenta, que han adquirido una madures en lo que respecta a la materia, siendo referentes en ese continente; a su vez, los que más han avanzado en el desarrollado de sus actuales estrategias de Ciberseguridad. Estos gobiernos, han tomado muy en serio la temática introduciéndolas en las agendas de sus administraciones. A nivel estratégico y operacional cuentan con las capacidades y conocimientos para la gestión los riesgos de una ciberamenaza.

Al analizar el caso particular de la República Argentina se observa, que existen múltiples actores abocados a esta temática, pero no hay un centro específico que coordine los esfuerzos realizados, debiendo funcionar de nexo,

entre el sector Público y Privado, pensando en las personas, los procesos y la tecnología.

Marco de Referencia de Ciberseguridad

El ciclo de vida de la Ciberseguridad, según el Marco propuesto por el NIST [29], consta de 5 funciones continuas e iterativas, que se grafican en la Figura 14, con las que se buscan, abordar y gestionar los riesgos inherentes de la ciberseguridad en las Infraestructuras Críticas.

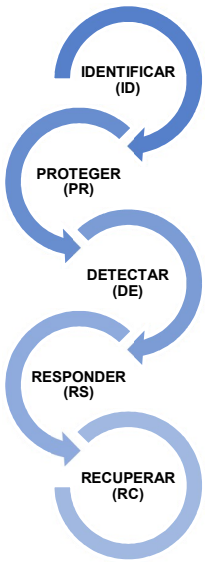

FIGURA 14. *FUNCIONES CONTINUAS PARA EL ABORDAJE DE LA CIBERSEGURIDAD PROPUESTAS POR EL NIST* [29]

Tomando como base el Marco de Ciberseguridad desarrollado por el NIST y la adaptación realizada por la Agesic[9] [30], se procedió a confeccionar un Marco abocado a la temática que sea factible de implementación en los Organismos del Estado, que, por su responsabilidad hacia la ciudadanía, se encuentran encuadrados dentro de la clasificación de Infraestructuras Críticas desarrollada anteriormente.

[9] Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento, de la República Oriental del Uruguay.

Cabe destacar que el mismo, presenta flexibilidad como característica principal, ya que permite aplicarse en cualquier tipo de Organización, sin importar su tamaño.

Descripción del Marco de Estrategia de Ciberseguridad Nacional

A continuación, se describirá detalladamente el Marco de Estrategia de Ciberseguridad propuesto para Organismos Nacionales, se tomó como base el confeccionado por del NIST, en el cual, se observa el ciclo de vida del proceso de gestión de la ciberseguridad desde una óptica técnico y organizacional. Ofreciendo actividades muy específicas para lograr resultados en materia de ciberseguridad. Se divide en funciones, categorías, referencias y cumplimiento. Cada subcategoría tiene asociada referencias a normas y estándares de seguridad internacionales, juntamente, con las recomendaciones propuestas para realizar un guía de cumplimiento.

FUNCION	SUBCATEGORIA	REFERENCIAS	CUMPLIMIENTO
IDENTIFICAR (ID)	**ID.AM Gestión de Activos:** La información, dispositivos, sistemas e instalaciones que son utilizados por la organización con el fin de alcanzar los objetivos organizacionales propuestos, se identifican y administran en forma consistente, en relación con los objetivos y la estrategia ante el riesgo de la organización.		
	ID.AM-1: Los dispositivos y sistemas físicos dentro de la organización se encuentran inventariados.	**CIS CSC 1** **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5	**ID.AM.CUM-01**
	ID.AM-2: Las plataformas de software y las aplicaciones dentro de la organización están inventariadas.	**CIS CSC 2** **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5	
	ID.AM-3: Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) se priorizan en función de su clasificación, criticidad y valor comercial.	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6	**ID.AM.CUM-02**

	ID.AM-4: Los roles y las responsabilidades de la seguridad cibernética para toda la fuerza de trabajo y terceros interesados (por ejemplo, proveedores, clientes, socios) están establecidas.	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1 **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11	**ID.AM.CUM-03**
	ID.BE Ambiente Organizacional: La misión de la organización, sus objetivos, interesados y actividades son comprendidas y priorizadas. Esta información es utilizada para informar a los recursos de ciberseguridad sobre responsabilidades y decisiones relacionadas a la gestión de riesgos.		
	ID.BE-1: Se identifica y se comunica el lugar de la organización en la infraestructura crítica y su sector industrial.	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Cláusula 4.1 **NIST SP 800-53 Rev. 4** PM-8	**-///-**
	ID.BE-2. Se definen las dependencias y funciones críticas para la entrega de los servicios críticos.	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14	**-///-**
	ID.GV Gobernanza: Las políticas, procedimientos y procesos para gestionar y monitorear los requisitos regulatorios, legales, ambientales y operativos de la organización, son comprendidos y se informa a las gerencias sobre los riesgos de ciberseguridad.		
	ID.GV-1: Se establece y se comunica la política de seguridad cibernética organizacional.	**CIS CSC 19** **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 **ISA 62443-2-1:2009** 4.3.2.6 **ISO/IEC 27001:2013** A.5.1.1 **NIST SP 800-53 Rev. 4**-1 controles de todas las familias de control de seguridad	**ID.GV.CUM-01**
	ID.GV-2: Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos.	**CIS CSC 19** **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2	**ID.GV.CUM-02**
	ID.GV-3: Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.	**CIS CSC 19** **COBIT 5** BAI02.01, MEA03.01, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.7 **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 **NIST SP 800-53 Rev. 4**-1 controles de todas las familias de control de seguridad	**ID.GV.CUM-03**
	ID.RA Evaluación de riesgos: La Organización comprende los riegos inherentes a su función dentro del ecosistema de ciberseguridad referente a sus operaciones, activos e individuos.		
	ID.RA-1: Se identifican y se	**CIS CSC 4**	**ID.RA.CUM-01**

	documentan las vulnerabilidades de los activos.	**COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	
	ID.RA-2: La inteligencia de amenazas cibernéticas se recibe de foros y fuentes de intercambio de información.	**CIS CSC 4** **COBIT 5** BAI08.01 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16	**ID.RA.CUM-02**
	ID.RA-3: Se identifican y se documentan las amenazas, tanto internas como externas.	**CIS CSC 4** **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** Cláusula 6.1.2 **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16	**ID.RA.CUM-03**
	ID.RA-4: Se utilizan las amenazas, las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo.	**CIS CSC 4** **COBIT 5** APO12.02 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16	**ID.RA.CUM-04**
	ID.RM Estrategia para la gestión de riesgos: Se establecen las prioridades, restricciones, tolerancia al riesgo y supuestos de la organización, utilizándose para soportar las decisiones a fin de afrontar los riesgos operacionales.		
	ID.RM-1: Los actores de la organización establecen, gestionan y acuerdan los procesos de gestión de riesgos.	**CIS CSC 4** **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** Cláusula 6.1.3, Cláusula 8.3, Cláusula 9.3 **NIST SP 800-53 Rev. 4** PM-9	**-///-**
	ID.RM-2: La determinación de la tolerancia del riesgo de la organización se basa en parte en su rol en la infraestructura crítica y el análisis del riesgo específico del sector.	**COBIT 5** APO12.02 **ISO/IEC 27001:2013** Cláusula 6.1.3, Cláusula 8.3 **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11	**-///-**
PROTEGER (PR)	**PR.AC Control de acceso:** El acceso a los activos e instalaciones se limita a usuarios, procesos o dispositivos, actividades y transacciones autorizadas.		
	PR.AC-1: Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.	**CIS CSC** 1, 5, 15, 16 **COBIT 5** DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.5.1 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	**PR.AC.CUM-01**

	PR.AC-2: Se gestiona y se protege el acceso físico a los activos.	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009 4.3.3.3.2**, 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8	**PR.AC.CUM-02**
	PR.AC-3: Se gestiona el acceso remoto.	**CIS CSC 12** **COBIT 5** APO13.01, DSS01.04, DSS05.03 **ISA 62443-2-1:2009** 4.3.3.6.6 **ISA 62443-3-3:2013** SR 1.13, SR 2.6 **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-17, AC-19, AC-20, SC-15	**PR.AC.CUM-03**
	PR.AC-4: Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.	**CIS CSC** 3, 5, 12, 14, 15, 16, 18 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.7.3 **ISA 62443-3-3:2013** SR 2.1 **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24	**PR.AC.CUM-04**
	PR.AC-5: Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor o múltiples factores) acorde al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11	**PR.AC.CUM-05**
	PR.AT Concientización y capacitación: El personal de la organización y el que interactuara con la misma, reciben entrenamiento y concientización sobre seguridad de la información. Están adecuadamente entrenados para cumplir con sus obligaciones referentes a la seguridad de la información y alineados con las políticas, procedimientos y acuerdos existentes.		
	PR.AT-1: Todos los usuarios están informados y capacitados.	**CIS CSC** 17, 18 **COBIT 5** APO07.03, BAI05.07 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 **NIST SP 800-53 Rev. 4** AT-2, PM-13	**PR.AT.CUM-01**
	PR.AT-2: Los usuarios privilegiados comprenden sus roles y responsabilidades.	**CIS CSC** 5, 17, 18 **COBIT 5** APO07.02, DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13	
	PR.AT-3: El personal de seguridad física y cibernética comprende sus	**CIS CSC 17** **COBIT 5** APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, IR-2, PM-13	

	roles y responsabilidades.		
	PR.DS Seguridad de los datos: La información y registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.		
	PR.DS-1: Los datos en reposo están protegidos.	**CIS CSC** 13, 14 **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 **ISA 62443-3-3:2013** SR 3.4, SR 4.1 **ISO/IEC 27001:2013** A.8.2.3 **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28	**PR.DS.CUM-01**
	PR.DS-2: Los datos en tránsito están protegidos.	**CIS CSC** 13, 14 **COBIT 5** APO01.06, DSS05.02, DSS06.06 **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12	
	PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.	**CIS CSC 1** **COBIT 5** BAI09.03 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16	**PR.DS.CUM-02**
	PR.DS-4: Se implementan protecciones contra las filtraciones de datos.	**CIS CSC 13** **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 **ISA 62443-3-3:2013** SR 5.2 **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4	**PR.DS.CUM-03**
	PR.DS-5: Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.	**CIS CSC** 2, 3 **COBIT 5** APO01.06, BAI06.01, DSS06.02 **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 **NIST SP 800-53 Rev. 4** SC-16, SI-7	**PR.DS.CUM-04**
	PR.DS-6: Los ambientes de desarrollo y testing se encuentran separados del entorno de producción.	**CIS CSC** 18, 20 **COBIT 5** BAI03.08, BAI07.04 **ISO/IEC 27001:2013** A.12.1.4 **NIST SP 800-53 Rev. 4** CM-2	**PR.DS.CUM-05**
	PR.IP Procesos y procedimientos para la protección de la información: Las políticas de seguridad, procesos y procedimientos se mantienen y son utilizados para gestionar la protección de los sistemas de información y los activos.		
	PR.IP-1: Se cuenta con una configuración base, la que incorpora los principios de seguridad de la información, aplicable a los	**CIS CSC** 3, 9, 11 **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	**PR.IP.CUM-01**

	sistemas de información, manteniéndose en forma constante.		
	PR.IP-2: Se implementa el ciclo de vida de desarrollo del software para la gestión de los sistemas.	**CIS CSC 18** **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17	**PR.IP.CUM-02**
	PR.IP-3: Se encuentran establecidos procesos de control de cambio de la configuración.	**CIS CSC** 3, 11 **COBIT 5** BAI01.06, BAI06.01 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10	**PR.IP.CUM-03**
	PR.IP-4: Se realizan, se mantienen y se prueban copias de seguridad de la información.	**CIS CSC** 10 **COBIT 5** APO13.01, DSS01.01, DSS04.07 **ISA 62443-2-1:2009** 4.3.4.3.9 **ISA 62443-3-3:2013** SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9	**PR.IP.CUM-04**
	PR.IP-5: Los datos son eliminados acorde con las políticas de seguridad.	**COBIT 5** BAI09.03, DSS05.06 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 **NIST SP 800-53 Rev. 4** MP-6	**PR.IP.CUM-05**
	PR.IP-6: Se encuentran establecidos y se gestionan los planes de respuesta (ante Incidentes y Continuidad del Negocio) y los planes de recuperación (de Incidentes y de Desastres).	**CIS CSC 19** **COBIT 5** APO12.06, DSS04.03 **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17	**PR.IP.CUM-06**
	PR.IP-7: Los planes de respuesta y recuperación son probados con regularidad.	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14	
	PR.IP-8: La Ciberseguridad se encuentra incluida en las políticas de recursos humanos.	**CIS CSC** 5, 16 **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21	**PR.IP.CUM-07**
	PR.IP-9: Se cuenta con un plan de gestión de las vulnerabilidades.	**CIS CSC** 4, 18, 20 **COBIT 5** BAI03.10, DSS05.01, DSS05.02 **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2	**PR.IP.CUM-08**
	PR.MA. Mantenimiento:		

	El mantenimiento y las reparaciones de los componentes de los sistemas de información y de control industrial se llevan a cabo en consonancia con las políticas y procedimientos.		
	PR.MA-1: El mantenimiento y la reparación de los activos de la organización se realizan y están registrados con herramientas aprobadas y controladas.	**COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.7 **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6	**-///-**
	PR.MA-2: El mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de manera que evite el acceso no autorizado.	**CIS CSC** 3, 5 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 **NIST SP 800-53 Rev. 4** MA-4	**-///-**
	PR.PT Tecnología de protección: Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y resistencia de los sistemas y activos de la organización, en consonancia con las políticas, procedimientos y acuerdos.		
	PR.PT-1: Los registros de auditoría (logs), se documentan, implementan y revisan de conformidad con la PSI.	**CIS CSC** 1, 3, 5, 6, 14, 15, 16 **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 **NIST SP 800-53 Rev. 4** Familia AU	**PR.PT.CUM-01**
	PR.PT-2: Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la PSI.	**CIS CSC** 8, 13 **COBIT 5** APO13.01, DSS05.02, DSS05.06 **ISA 62443-3-3:2013** SR 2.3 **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 **NIST SP 800-53 Rev. 4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8	**PR.PT.CUM-02**
	PR.PT-3: El control de acceso a los sistemas y activos se realiza mediante el principio de menor privilegio.	**COBIT 5** DSS05.02 **ISO/IEC 27001:2013** A.9.1.2 **NIST SP 800-53 Rev. 4** AC-3, CM-7	**PR.PT.CUM-03**
DETECTAR (DE)	**DE.AE. Anomalías y eventos:** La actividad maliciosa se detecta de forma temprana y se comprende el potencial impacto de los eventos de ciberseguridad.		
	DE.AE-1: Los eventos detectados se analizan para entender los objetivos y métodos de ataque utilizados.	**CIS CSC** 3, 6, 13, 15 **COBIT 5** DSS05.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4	**DE.AE.CUM-01**
	DE.AE-2: Los datos de los	**CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 **COBIT 5** BAI08.02	**-///-**

	eventos clasifican y se constatan con múltiples fuentes y sensores de análisis.	**ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	
	DE.AE-3: Se determina el impacto de los eventos de ciberseguridad.	**CIS CSC** 4, 6 **COBIT 5** APO12.06, DSS03.01 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4	**DE.AE.CUM-02**
	DE.AE-4: Se establecen parámetros para las alertas de incidentes.	**CIS CSC** 6, 19 **COBIT 5** APO12.06, DSS03.01 **ISA 62443-2-1:2009** 4.2.3.10 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8	**DE.AE.CUM-03**
	DE.CM. Monitoreo continuo de la seguridad: Los sistemas de información y como los activos son monitoreados de manera continua para identificar eventos de seguridad cibernética y verificar la eficacia de las medidas de protección tomadas.		
	DE.CM-1: Se monitorea la red para detectar potenciales eventos de ciberseguridad.	**CIS CSC** 1, 7, 8, 12, 13, 15, 16 **COBIT 5** DSS01.03, DSS03.05, DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	**DE.CM.CUM-01**
	DE.CM-2: Se monitorea el ambiente físico para detectar potenciales eventos de ciberseguridad.	**COBIT 5** DSS01.04, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20	**DE.CM.CUM-02**
	DE.CM-3: Se monitorea la actividad del personal para detectar potenciales eventos de ciberseguridad.	**CIS CSC** 5, 7, 14, 16 **COBIT 5** DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	**DE.CM.CUM-03**
	DE.CM-4: Se detecta el código malicioso.	**CIS CSC** 7, 8 **COBIT 5** DSS05.01 **ISA 62443-3-3:2013** SR 2.4 **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44	**DE.CM.CUM-04**
	DE.CM-5: Se detecta el código móvil no autorizado.	**CIS CSC** 7, 8 **COBIT 5** DSS05.01 **ISA 62443-3-3:2013** SR 2.4 **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44	**DE.CM.CUM-05**
	DE.CM-6: Se monitorea la actividad de los proveedores de servicios externos para detectar posibles eventos de seguridad cibernética.	**COBIT 5** APO07.06, APO10.05 **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4	**DE.CM.CUM-06**
	DE.CM-7: Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados	**CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 **COBIT 5** DSS05.02, DSS05.05 **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	**-///-**

	DE.CM-8: Se realizan escaneos de vulnerabilidades.	**CIS CSC** 4, 20 **COBIT 5** BAI03.10, DSS05.01 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-5	**DE.CM.CUM-08**
	DE.DP. Procesos de detección: Se mantienen procesos, procedimientos de detección y prueba para asegurar el conocimiento oportuno y adecuado de los eventos sospechosos.		
	DE.DP-1: Los roles y los deberes de detección están bien definidos para asegurar la responsabilidad.	**CIS CSC 19** **COBIT 5** APO01.02, DSS05.01, DSS06.03 **ISA 62443-2-1:2009** 4.4.3.1 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14	**DE.DP.CUM-01**
	DE.DP-2: Las actividades de detección cumplen con todos los requisitos aplicables.	**COBIT 5** DSS06.01, MEA03.03, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.2 **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14	**-///-**
	DE.DP-3: Se comunica la información de la detección de eventos.	**CIS CSC 19** **COBIT 5** APO08.04, APO12.06, DSS02.05 **ISA 62443-2-1:2009** 4.3.4.5.9 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4	**DE.DP.CUM-03**
RESPONDER (RS)	**RE.RP. Planificación de la respuesta:** Los procesos y procedimientos de respuesta se ejecutan y se mantienen garantizando una respuesta oportuna para detectar eventos de ciberseguridad.		
	RS.RP-1: El plan de respuesta se ejecuta durante o después de un incidente.	**CIS CSC 19** **COBIT 5** APO12.06, BAI01.10 **ISA 62443-2-1:2009** 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8	**RS.RP.CUM-01**
	RE.CO. Comunicaciones: Las actividades de respuesta se coordinan con las partes interesadas internas y externas, según corresponda.		
	RS.CO-1: El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.	**CIS CSC 19** **COBIT 5** EDM03.02, APO01.02, APO12.03 **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8	**RS.CO.CUM-01**
	RS.CO-2: El intercambio voluntario de información se produce con las partes interesadas externas para lograr una mayor conciencia situacional de seguridad cibernética.	**CIS CSC 19** **COBIT 5** BAI08.04 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15	**-///-**
	RE.AN. Análisis: Se efectúa análisis para asegurar una respuesta adecuada y dar soporte a las actividades de recuperación determinadas.		
	RS.AN-1: Se investigan las notificaciones de los sistemas de detección.	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS02.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5	**RS.AN.CUM-01**

		NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4	
	RS.AN-2: Se comprende el impacto del incidente.	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53 Rev. 4** CP-2, IR-4	**RS.AN.CUM-02**
	RS.AN-3: Se realizan análisis forenses.	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 4** AU-7, IR-4	**-///-**
	RS.AN-4: Los incidentes se clasifican de acuerdo con los planes de respuesta	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev. 4** SI-5, PM-15	**-///-**
	RE.MI. Mitigación: Se ejecutan actividades para prevenir la expansión de un evento, mitigar su impacto y eliminar el incidente.		
	RS.MI-1: Los incidentes son contenidos.	**CIS CSC 19** **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR-4	**RS.MI.CUM-01**
	RS.MI-2: Los incidentes son mitigados.	**CIS CSC** 4, 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR-4	
	RS.MI-3: Las vulnerabilidades recientemente identificadas son mitigadas o se documentan como riesgos aceptados.	**CIS CSC 4** **COBIT 5** APO12.06 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5	**-///-**
	RE.IM. Mejoras: Las actividades de respuesta de la organización son mejoradas por la incorporación de lecciones aprendidas de las actividades de detección y respuesta actuales y anteriores.		
	RS.IM-1: Los planes de respuesta incorporan las lecciones aprendidas.	**COBIT 5** BAI01.13 **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8	**-///-**
	RS.IM-2: Se actualizan las estrategias de respuesta.	**COBIT 5** BAI01.13, DSS04.08 **ISO/IEC 27001:2013** A.16.1.6, Clausula 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8	**-///-**
RECUPERAR (RC)	**RC.RP. Planificación de la recuperación:** Los procesos y procedimientos de recuperación son ejecutados y mantenidos para asegurar la restauración oportuna de los sistemas o activos afectados por eventos de ciberseguridad.		
	RC.RP-1: El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.	**CIS CSC 10** **COBIT 5** APO12.06, DSS02.05, DSS03.04 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8	**RC.RP.CUM-01**
	RC.IM. Mejoras: Se mejoran los planes y procesos de recuperación incorporando en actividades futuras las lecciones aprendidas de sucesos anteriores.		

	RC.IM-1: Se actualizan las estrategias de recuperación.	**COBIT 5** APO12.06, BAI07.08 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8	**-///-**
	RC.CO. Comunicaciones: Las actividades de recuperación se coordinan con las partes interesadas internas y externas (como ser: centros de coordinación, proveedores de servicios de Internet, propietarios de los sistemas afectados, las víctimas, otros CSIRT y vendedores).		
	RC.CO-1: Se gestionan las relaciones públicas.	**COBIT 5** EDM03.02 **ISO/IEC 27001:2013** A.6.1.4, Clausula 7.4	**RC.CO-CUM-01**
	RC.CO-2: La reputación se repara después de un incidente.	**COBIT 5** MEA03.02 **ISO/IEC 27001:2013** Clausula 7.4	**-///-**
	RC.CO-3: Las actividades de recuperación se comunican a las partes interesadas internas y externas, así como también a los equipos ejecutivos y de administración.	**COBIT 5** APO12.06 **ISO/IEC 27001:2013** Cláusula 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4	**-///-**

TABLA 5. MARCO DE ESTRATEGIA DE CIBERSEGURIDAD PROPUESTO [29] [30]

Cumplimiento

IDENTIFICAR (ID)

ID.AM.CUM-01

El Organismo es responsable de desarrollar, documentar, revisar y actualizar, con una frecuencia prestablecida por la Gerencia el inventario de componentes de sus sistemas informáticos. Siendo responsables de verificar que:

a. Se refleja con precisión el sistema actual.
b. Incluyen todos los componentes dentro del límite de autorización.
c. Está en el nivel de granularidad que se considera necesario para el seguimiento y la presentación de informes.
d. Incluye la información prescrita por la política de gestión de la configuración que se considera necesaria para lograr la responsabilidad efectiva de los componentes del sistema de información.

ID.AM.CUM-02

El Organismo es responsable de desarrollar un plan de contingencia para sus sistemas que:

a. Identifique las misiones y funciones esenciales, junto con sus requisitos asociados.
b. Proporcione objetivos de recuperación y prioridades de restauración
c. Aborde los roles de contingencia, responsabilidades, y personas asignadas con información de contacto.
d. Direcciones que mantienen misiones esenciales y funciones comerciales a pesar de una interrupción, compromiso o falla del sistema de información.
e. Direcciones eventuales, restauración completa del sistema de información sin deterioro de las salvaguardas de seguridad originalmente planificadas e implementadas, y
f. Es revisado y aprobado por personal o roles definidos por la organización de acuerdo con la política de planificación de contingencia.

Además, deberán categorizar su información y su sistema de información de acuerdo con las leyes regulatorias, documentando los resultados en el plan de seguridad, y sea revisada y aprobada por el responsable asignado.

ID.AM.CUM-03

La Organización es responsable de:

a. Establecer los requisitos de seguridad del personal, incluidas las funciones y responsabilidades de seguridad para los proveedores externos.
b. Requerir que los proveedores externos cumplan con las mismas políticas y procedimientos de seguridad que la organización.

c. Documentar los requisitos de seguridad del personal.
d. Requerir que los proveedores notifiquen a la Organización, en forma inmediata, sobre cualquier cese de contrato de personal que posean credenciales y/o privilegios de sistema, en un período tiempo definido por la organización.
e. Monitoreo del cumplimiento del proveedor.

Además, deberán determinar las necesidades de protección de la información con respecto a los controles de seguridad requeridos para la organización y los sistemas de información asociados que respaldan los procesos, con relación a la normativa vigente.

ID.GV.CUM-01

El Organismo es responsable de desarrollar, documentar, mantener, difundir e implementar una política de seguridad de la información (PSI), como así también, son responsables de revisar y actualizar la política y los procedimientos con la frecuencia definida por su Gerencia.

ID.GV.CUM-02

El Organismo es responsable de designar un referente de la Seguridad de la Información, como así también, conformar un Comité de Seguridad de Información.

ID.GV.CUM-03

El Organismo es responsable de desarrollar, documentar, mantener, difundir e implementar una política de evaluación de riesgos junto con los procedimientos de apoyo, como así también, son responsables de revisar y actualizar la política y los procedimientos con la frecuencia definida por su Gerencia, que permitan cumplir con todas las regulaciones en las que se encuentran enmarcados por su misión específica.

ID.RA.CUM-01

El Organismo es responsable de realizar evaluaciones de seguridad para sus sistemas. Dentro de este contexto y de acuerdo con su política de evaluación y autorización de seguridad, son responsables de:

a. Desarrollar un plan de evaluación de seguridad, que describa los controles y sus mejoras, los procedimientos de evaluación, el entorno de evaluación, el equipo de evaluación, las funciones y responsabilidades de la evaluación.
b. Evaluar los controles de seguridad en su sistema y su entorno de operación, con una frecuencia determinada, a fin de dar cumplimiento a los requisitos de seguridad establecidos.
c. Producir un informe de evaluación de seguridad que documente los resultados de la evaluación.
d. Proporcionar los resultados de la evaluación a los responsables definidos por la organización.

Además, son responsables de desarrollar una estrategia e implementar un programa de monitoreo continuo de acuerdo con su política de evaluación y autorización de seguridad que defina:

a. Métricas para monitorear.
b. Frecuencias para el monitoreo e informes.
c. Responsables de llevar a cabo el monitoreo y quienes analizaran la información de análisis en forma continua.

Se deberán realizar pruebas de penetración en los sistemas o componentes del sistema definidos por la organización con la frecuencia prescrita por su política de evaluación y autorización de seguridad.

Los Organismos son responsables de:

a. Realizar una evaluación del riesgo que incluya la probabilidad y la magnitud del daño por: el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada del sistema informático, como también, la información que procesa almacena o transmite.

b. Documentar los resultados de la evaluación en el plan del sistema, el informe de evaluación de seguridad u otro documento definido por la organización.
c. Revisar los resultados de la evaluación de riesgos con una frecuencia definida por la organización.
d. Difundir los resultados de la evaluación de riesgos a los responsables definidos por la organización.
e. Actualizar la evaluación de riesgos con una frecuencia definida por la organización o siempre que haya cambios significativos en el sistema de información (incluida la identificación de nuevas amenazas y vulnerabilidades) u otras condiciones que puedan afectar el estado de seguridad del sistema.

Los Organismos asumen la responsabilidad de:

a. Identificar, informar y corregir fallas en sus sistemas de información.
b. Probar actualizaciones de software y firmware relacionadas con la corrección de fallas para determinar la efectividad y los posibles efectos secundarios antes de la instalación.
c. Instalar software relevante para la seguridad y actualizaciones de firmware dentro de un período de tiempo definido por la organización desde el lanzamiento de las actualizaciones.
d. Incorporar la corrección de fallas en el proceso de administración de la configuración organizacional.

ID.RA.CUM-02

El Organismo es responsable de mantener un contacto continuo con grupos y asociaciones de seguridad que faciliten la educación y capacitación en seguridad continúa para el personal de la organización. Manteniendo de esta manera actualizadas las prácticas, técnicas y tecnologías de seguridad. Se deberá compartir información actualizada relacionada con la seguridad, incluidas amenazas, vulnerabilidades e incidentes.

Así también, se deberá de implementar un programa de concientización de amenazas que tiene la capacidad de compartir información en toda la organización.

ID.RA.CUM-03

El Organismo es responsable de realizar una evaluación del riesgo, incluyendo la probabilidad y la magnitud del daño, a causa del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada a sus sistemas informáticos y la información que estos procesan o almacena. Esto deberá quedar debidamente documentado en un documento definido por la organización, al cual tendrá acceso el rol definido con la finalidad de revisar los resultados con una frecuencia establecida. Esto deberá actualizarse con una frecuencia periódica, definida por la organización o siempre que haya cambios significativos en el sistema de información o en su entorno de operación que puedan afectar el estado de seguridad (incluida la identificación de nuevas amenazas y vulnerabilidades ajenas al Organismo).

Además, es responsable de recibir alertas, avisos y directivas de seguridad de organizaciones externas de manera continua, mediante la suscripción de convenios marcos. Se generarán alertas, avisos y directivas de seguridad internas según se considere necesario; difundiéndolas al personal que interactúe. Se Implementarán directivas acordes a los plazos establecidos o notificar a la organización emisora de la alerta, como así también, su grado de incumplimiento.

ID.RA.CUM-04

El Organismo es responsable de cumplir con el requerimiento ID.RA.CUM-03. Además, se deberá cumplimentar los siguientes ítems:

a. Categorizar su información y sus sistemas de información acorde las leyes, órdenes ejecutivas, directivas, políticas, regulaciones y estándares.

b. Documentar los resultados de la categorización de seguridad (incluida su justificación) en el plan de seguridad desarrollado.
c. Asegurarse que la decisión de categorización de seguridad sea revisada y aprobada por el responsable del Área de Seguridad Informática o el representante designado como tal.

PROTEGER (PR)

PR.AC.CUM-01

El Organismo es responsable de administrar las cuentas asociadas con sus aplicaciones, debiéndose configurar sus sistemas para identificar y autenticar de manera única a los usuarios de la organización (o procesos que actúan en nombre de los usuarios).

El Organismo es responsable de configurar sus sistemas para identificar y autenticar de manera única los dispositivos y / o tipos de dispositivos específicos definidos por la organización antes de establecer conexiones locales, remotas y/o de red de acuerdo con su política de identificación y autenticación.

Así mismo, son responsables de administrar los identificadores del sistema de información al:

a. Recibir autorización del personal o roles definidos para asignar un identificador individual, grupal, de rol o de dispositivo.
b. Seleccionar un identificador que identifique a un individuo, grupo, rol o dispositivo.
c. Asignación del identificador al individuo, grupo, rol o dispositivo previsto.
d. Prevención de la reutilización de identificadores para un período de tiempo definido por la organización.
e. Desactivación del identificador después de un período de tiempo definido por la organización de inactividad.

El Organismo es responsable de configurar sus sistemas para implementar mecanismos de autenticación mediante un módulo criptográfico que cumpla con los requisitos de las leyes, órdenes ejecutivas, directivas, políticas, regulaciones, estándares y orientación para dicha autenticación.

PR.AC.CUM-02

El Organismo deberá cumplir con la RESOLUCIÓN Nº 48/05 de la Sindicatura General de la Nación.

PR.AC.CUM-03

El Organismo es responsable de establecer y documentar las restricciones de uso, los requisitos de configuración / conexión y la guía de implementación para cada tipo de acceso remoto permitido a sus sistemas de acuerdo con su política de control de acceso, autorizando el acceso remoto a sus sistemas antes de permitir tales conexiones.

El Organismo puede controlar el acceso remoto a su sistema utilizando listas de accesos para definir el tipo de acceso y las ubicaciones remotas permitidas.

PR.AC.CUM-04

El Organismo es responsable de administrar las cuentas asociadas con sus aplicaciones, debiendo configurar sus sistemas para imponer el acceso lógico basado en autorizaciones aprobadas y de acuerdo con su política de control de acceso.

PR.AC.CUM-05

El Organismo es responsable de configurar sus sistemas y los interconectados para hacer cumplir sus políticas de flujo de información aprobadas. Siendo responsables de:

a. Monitorear y controlar las comunicaciones externas e internas del sistema, en sus puntos críticos.
b. Implementar subredes para componentes del sistema accesibles externamente, que están separados física o lógicamente de la organización.
c. Conexión a redes externas o sistemas de información mediante la utilización de interfaces acorde a la arquitectura de seguridad de la organización.

PR.AT.CUM-01

El Organismo es responsable de cumplir con el requerimiento ID.RA.CUM-02.

PR.DS.CUM-01

El Organismo es responsable de cumplir con el requerimiento PR.AC.CUM-01.

PR.DS.CUM-02

El Organismo es responsable de definir una política y procedimiento documentado para la destrucción de la información como así los medios de almacenamiento que los contengan, evitándose de esta manera la fuga de información, esto busca que terceras partes accedan a información si obtienen acceso físico al bien eliminado.

PR.DS.CUM-03

El Organismo es responsable de incluir en los contratos laborales restricciones inherentes a la seguridad de la información en las que se definan las responsabilidades legales que puede acarrear un mal uso de sus privilegios, acorde a su función dentro de la misma. Definiendo un procedimiento formal, para el momento de la desvinculación del personal, con el fin de revocar los privilegios lógicos y físicos.

Se deberán establecer acuerdos de confidencialidad al momento del ingreso a la misma.

PR.DS.CUM-04

El Organismo es responsable de confeccionar una política de control de Software malicioso, que contenga:

a. Mecanismos y/o procedimientos para la detección de software no autorizado o malicioso.
b. Mantener una lista de software autorizado (lista blanca).
c. Mantener una lista de sitios Web maliciosos y/o no autorizados (lista negra).
d. Protección antivirus centralizada y su consola de gestión, identificando quien será el responsable de su administración.
e. Capacitar al personal afectado en la operación y uso de la solución antivirus, así como cualquier otro mecanismo utilizado para la detección de software malicioso.
f. Procedimientos para obtener información en forma regular (suscripción a listas de correo, comprobación de los sitios Web especializados que brindan información sobre nuevo software malicioso).

Se deberá contar con herramientas automatizadas que analicen, identifiquen y eliminen cualquier amenaza, monitorizando estaciones de trabajo como servidores y dispositivos móviles, identificados en el inventario realizado en el cumplimiento ID.AM.CUM-01.

Dentro de las Política de Seguridad de la Información, se mencione los privilegios que se les asignará a los diferentes usuarios para la instalación de software en sus equipos. Debiendo haber un procedimiento por el cual se controle la solicitud efectuada por un usuario, identificando quien aprueba dicha instalación.

PR.DS.CUM-05

El Organismo es responsable de contar con diferentes entornos informáticos para el Desarrollo, Pruebas, Preproducción y Producción, debiendo estar bien definidos e identificados, con la finalidad de evitar errores de interpretación por parte del personal autorizado para tal fin. Como recomendación los ambientes de Desarrollo y Prueba deben estar separados del de Producción.

Además, se deberá desarrollar un procedimiento de pasaje entre ambientes, en el que se detalle: motivo de la solicitud, quienes autorizan y solicitan, comprobación de funcionamiento y los pasos para volver al estado inicial, ante una posible caída.

PR.IP.CUM-01

El Organismo deberá Gestionar los cambios de manera formal, controlando que estos cambios no comprometan a la Seguridad, verificando que estos estén aprobados y justificados, que cumplan con la Normativa vigente acorde a la PSI, abarcando a toda la Organización.

La política de gestión de cambios debería contar con la siguiente información:

a. Solicitud.
b. Registro.
c. Autorización.
d. Evaluación de riesgos e impacto.
e. Priorización.
f. Ejecución, prueba y aprobación.
g. Gestión de configuración.
h. Prever la posibilidad de volver atrás para la recuperación a un estado estable conocido anterior en caso de imprevistos o errores.
i. Control de versionado y línea base.

j. Cambios de emergencia, es decir aquellos que por su urgencia no pueden realizarse según lo establecido en el procedimiento de gestión de cambios tradicional.
k. Herramientas disponibles en la organización para dar soporte a la gestión de los cambios.

PR.IP.CUM-02

El Organismo es responsable de incluir los siguientes requisitos, descripciones y criterios explícitamente o por referencia en el contrato de adquisición del sistema de información, componente del sistema o servicio del sistema de información de acuerdo con las leyes nacionales, órdenes ejecutivas, directivas, políticas, normas, estándares, pautas y necesidades de la organización:

a. Requisitos funcionales de seguridad,
b. Requisitos de seguridad,
c. Requisitos de garantía de seguridad,
d. Requisitos de documentación relacionados con la seguridad,
e. Requisitos para proteger la documentación relacionada con la seguridad,
f. Descripción del entorno de desarrollo del sistema de información y el entorno en el que está destinado a funcionar el sistema,
g. Criterios de aceptación.

Además, es responsable de aplicar los principios de ingeniería de seguridad en todas las actividades del SDLC[10].

PR.IP.CUM-03

El Organismo es responsable de cumplir con el requerimiento PR.IP.CUM-01.

[10] Systems Development Life Cycle (Ciclo de Vida del Desarrollo de Sistemas, por sus siglas en inglés).

PR.IP.CUM-04

El Organismo es responsable de probar su plan de contingencia con una frecuencia definida por el Comité de Seguridad de la Información, utilizando pruebas definidas por la organización para determinar la efectividad del plan y la disposición de la organización para ejecutar el plan. Deberán revisar los resultados con el fin de implementar acciones correctivas cuando sea necesario.

PR.IP.CUM-05

El Organismo es responsable de cumplir con el requerimiento PR.DS.CUM-02.

PR.IP.CUM-06

El Organismo es responsable de desarrollar un plan de contingencia para su sistema que:

a. identifique las funciones críticas,
b. proporcionar los objetivos de recuperación y prioridades de restauración,
c. especifique los roles de contingencia, responsabilidades e individuos asignados con su información de contacto,
d. Las ubicaciones que ejecutan las misiones esenciales y funciones durante una interrupción, compromiso o falla del sistema de información,
e. Abarca la restauración eventual y completa del sistema de información sin pérdida de las salvaguardas de seguridad originalmente planificada e implementada.

Además, deben desarrollar un Plan de respuesta a incidentes que:

a. Proporcione una guía para implementar su capacidad de respuesta a incidentes.
b. Describa la estructura y organización de la capacidad de respuesta a incidentes.

c. Cumple con los requisitos únicos de la organización, que se relacionan con la misión, el tamaño, la estructura y las funciones.
d. Define los incidentes reportables.
e. Proporciona métricas cuantificar la capacidad de respuesta a incidentes ocurridos dentro de la organización.
f. Define los recursos y el apoyo administrativo necesarios para mantener y actualizar la capacidad de respuesta ante incidentes.

Ambos documentos deben ser revisado y aprobado por personal o roles definidos por la organización de acuerdo con las políticas de planificación definidas.

PR.IP.CUM-07

El Organismo es responsable de cumplir con el requerimiento PR.DS.CUM-03.

PR.IP.CUM-08

El Organismo es responsable de cumplir con el requerimiento IR.RA.CUM-01.

PR.PT.CUM-01

El Organismo es responsable de desarrollar, documentar, mantener, difundir e implementar una política de auditoría.

Se deberán configurar sus sistemas para generar registros de auditoría, los que contengan información con el que se pueda establecer el tipo de evento, cuándo y dónde ocurrió, la fuente del evento, el resultado y la identidad de cualquier individuo asociado al evento. Para esto deberán usar relojes de sistema internos para generar marcas de tiempo para registros de auditoría como ser un NTP.

Se deberá ejecutar un análisis de los registros de auditoría con una frecuencia definido, a fin de detectar, indicios de actividad sospechosa e

informar de estos hallazgos al personal o roles definidos acorde con la política de auditoría.

La política de auditoría deberá especificar el tiempo de retención de los registros de auditoría, a fin de ser brindados como apoyo para futuras investigaciones a los incidentes de seguridad, buscando cumplir con los requisitos de retención de información regulatoria y organizacional si los existiera.

PR.PT.CUM-02

El Organismo es responsable de cumplir con el requerimiento ID.AM.CUM-01.

El Organismo deberá establecer pautas para su uso, buscando de esta manera proteger y controlar el acceso a estos medios extraíbles, a fin de bloquear el uso de estos dispositivos para aquellos usuarios que utilicen puestos donde no sean de uso obligatorio para su labor diario; debiéndose extender el concepto de información sensible al contenido de estos dispositivos.

PR.PT.CUM-03

El Organismo es responsable de cumplir con el requerimiento PR.AC.CUM-04.

DETECTAR (DE)

DE.AE.CUM-01

El Organismo es responsable de cumplir con el requerimiento PR.PT.CUM-01.

El Organismo es responsable de implementar proceso de manejo de incidentes de seguridad informática que incluya:

a. Preparación.
b. Detección y análisis.
c. Contención.
d. Erradicación y recuperación de acuerdo con la política.

Además, se deberán coordinar las actividades para el manejo de incidentes con las de planificación de contingencias; incorporar lecciones aprendidas de los procedimientos de respuesta a incidentes ejecutados, capacitación y ejercicios efectuados; a fin de implementar las mejoras resultantes.

El Organismo es responsable de detectar y analizar eventos para comprender los objetivos y métodos de ataque, mediante la implementación de un Firewall de Aplicación (Web Application Firewall - WAF) en toda Aplicación Web expuesta a la Red Publica u Internet, como así también, en su Red Interna o Intranet.

DE.AE.CUM-02

El Organismo es responsable de cumplir con los requerimientos ID.RA.CUM-02, PR.IP.CUM-01 y PR.IP.CUM-06.

DE.AE.CUM-03

El Organismo es responsable de cumplir con los requerimientos DE.AE.CUM-01 y DE.AE.CUM-02.

DE.CM.CUM-01

El Organismo es responsable de cumplir con el requerimiento DE.AE.CUM-02.

DE.CM.CUM-02

El Organismo es responsable de cumplir con los requerimientos PR.AC.CUM-02 y DE.CM.CUM-01.

DE.CM.CUM-03

El Organismo es responsable de cumplir con los requerimientos PR.AC.CUM-05 y DE.AE.CUM-03.

DE.CM.CUM-04

El Organismo es responsable de cumplir con el requerimiento PR.DS.CUM-04.

DE.CM.CUM-05

El Organismo es responsable de cumplir con el requerimiento PR.IP.CUM-03.

DE.CM.CUM-06

El Organismo es responsable de incluir los requisitos de seguridad en forma detalla y explícita o por referencia, en el contrato de adquisición o componente del sistema de información y/o servicio de acuerdo con la Normativa Vigente, a fin de que los proveedores externos cumplan con los requisitos de seguridad de la información organizacional y empleen controles de seguridad definidos por la organización.

El Organismo es responsable de monitorear la actividad del proveedor de servicios externos para detectar eventos de ciberseguridad, que pongan en riesgo a la información almacenada.

DE.CM.CUM-08

El Organismo es responsable de cumplir con el requerimiento ID.RA.CUM-03.

DE.DP.CUM-01

El Organismo es responsable de cumplir con el requerimiento PR.PT.CUM-01.

DE.DP.CUM-03

El Organismo es responsable de cumplir con los requerimientos ID.RA.CUM-02, DE.AE.CUM-01 y PR.IP.CUM-08.

Además, deberán mantener una comunicación fluida y constante con el CERT dependiente de la Dirección Nacional de CIBERSEGURIDAD de la Jefatura de Gabinete de MINISTROS.

RESPONDER (RS)

RS.RP.CUM-01

El Organismo es responsable de cumplir con el requerimiento PR.IP.CUM-06.

RS.RP.CUM-01

El Organismo es responsable de cumplir con los requerimientos PR.AT.CUM-01, RS.RP-CUM01, DE.DP.CUM-01 y PR.IP.CUM-06.

RS.AN.CUM-01

El Organismo es responsable de cumplir con los requerimientos DE.AE.CUM-01, RS.RP.CUM-01 y DE.DP.CUM-01.

RS.AN.CUM-02

El Organismo es responsable de cumplir con los requerimientos DE.AE.CUM-01 y RS.RP.CUM-01.

RS.MI.CUM-01

El Organismo es responsable de cumplir con los requerimientos RS.RP.CUM-01 y DE.AE.CUM-01.

RECUPERAR (RC)

RC.RP.CUM-01

El Organismo es responsable de cumplir con los requerimientos RS.CO.CUM-01 y PR.IP.CUM-06.

Además, debe tener la capacidad técnica y organizativa de evaluar correctamente los daños causados (imagen Institucional, económicos y financieros, legales y administrativos, etc.), debiéndose ejecutar el Plan de Recuperación y Contingencia.

RC.CO.CUM-01

El Organismo es responsable de contar con un equipo de Comunicación Institucional, el que tendrá la función de informar a las partes interesadas sobre las acciones de ciberseguridad. Esta comunicación tendrá un formato específico, como se detalla a continuación, abordando ciertos puntos de interés:

a) Apreciación del incidente determinado (qué aconteció, cuándo, dónde, qué acciones se están tomando, etc.)
b) Notificación (al vocero del equipo de comunicaciones).
c) Determinar el nivel de comunicación requerido (alto, medio, bajo, por ejemplo) y elaborar los mensajes necesarios.
d) Aprobar y difundir los mensajes (por la Dirección o área competente que se determine).
e) Monitoreo de las comunicaciones (revisar la cobertura que los medios de comunicación han realizado con la información proporcionada sobre la crisis).

Conclusiones

Durante el desarrollo del presente Trabajo se ha introducido lentamente al lector, a la temática de la Ciberseguridad, concepto muy importante en un Mundo hiperconectado como el de hoy, enfocándose especialmente en lo que está sucediendo en nuestro País a nivel Gobierno, para lo cual se ha analizado toda normativa vigente referente a esta problemática de antigua data a la actualidad, observándose claramente, un notorio crecimiento en el interés sobre los desafíos tecnológicos que necesitamos afrontar como Republica, introduciéndolos en la agenda de nuestros responsables.

Se han mencionado los tipos de amenazas que podrían atentar contra las Infraestructuras Críticas las que son la columna vertebral de un País, ya que sustentan el poder económico, la seguridad nacional, la privacidad y las libertades civiles de una sociedad; juntamente, con las herramientas que cuentan estos Ciberdelincuentes. Pudiéndose observar, que existe una gran cantidad de amenazas cada vez más potentes y sofisticadas, fáciles de utilizar no requiriendo un conocimiento basto de TIC's ni contar con un alto poder de procesamiento.

Se ha analizado el contexto Internacional, como así también Estrategias Nacionales de Ciberseguridad de distintos Países y Continentes, observándose claramente, la brecha que existe entre nuestro País y Estados Unidos de Norteamérica, y si la comparación se realiza, con los Países Europeos como España y Estonia, la brecha se hace más extensa y profunda aún.

El modelo de Marco de Ciberseguridad propuesto en este Trabajo Final de Maestría identifica los lineamientos básicos a cumplir para gestionar los riesgos inherentes a la Ciberseguridad en un Organismo Público. Para esto, se tomó el desarrollado por el NIST (en su versión 1.1 del Marco, que fuera publicado el 16 de abril de 2018 el que proporciona un conjunto de actividades

para la gestión de los riesgos), ya que compila las buenas prácticas de diversas certificaciones de seguridad específicas del sector, nacionales e internacionales (COBIT, CSC, ANSI/ISA e ISO entre otros) y las agrupa según afinidad, proporcionando una guía para la Gobernanza de la Ciberseguridad.

Lo desarrollado, intenta ser una guía inicial para seguir por los responsables de Seguridad Informática o de la Información de un Organismo Público, a falta de un protocolo unificado para un ordenamiento de la gestión de los recursos tecnológicos; tomando pequeños lineamientos a cumplir por ser considerados buenas prácticas por parte de Organizaciones referentes en la materia. Esto facilitaría la comunicación entre los Organismos Nacionales ayudando a mitigar los riegos que se asocian a esta temática, ya que existe una interrelación continua a nivel operacional, consumiendo servicios que se complementan entre sí; buscándose de esta manera llegar a tener un alto grado de madurez en Ciberseguridad a este Nivel.

Es digno destacar, que la implementación de un Marco de Ciberseguridad no solventa los riegos con los que se afronta por pertenecer a un mundo conectado, debemos trabajar diariamente y en forma constante en la capacitación de los recursos humanos, por medio de campañas de concientización, introducir contenidos mínimos dentro de los programas de formación de los nuevos agentes, confeccionar boletines informativos con recomendaciones para su ámbito particular y profesional, por nombrar algunos; estos se consideran el eslabón más débil en la cadena de la Seguridad Informática, de esta manera fortaleceremos el margen de exposición ante los Ciberdelincuentes.

Con este Marco, se busca suplir la falta de respuesta de cumplimiento con los principios establecidos en la Estrategia Nacional de Ciberseguridad de la República Argentina, dando los lineamientos para unificar los esfuerzos realizados por las Áreas de Gobierno y Privadas, que juntas conforman las Infraestructuras Críticas.

Trabajos Futuros

De este trabajo se desprenden las siguientes líneas futuras de investigación y posibles cursos de acción:

- Elevar el presente Marco para su análisis y posterior implementación, al Departamento CIBERSEGURIDAD de la Policía Federal Argentina, utilizándola como caso testigo para futuras implementaciones.
- Realizar campañas de concientización diseñadas acorde a los niveles de Gestión y Operación definidos en el Organigrama de la Organización.
- Diseñar y establecer un CERT en la Organización, para que sea un vínculo activo con las distintas Organizaciones Nacionales e Internacionales referentes en la materia.
- Implementar el marco propuesto en otras entidades Públicas y Privadas en el ámbito Nacional.

Bibliografía

[1] Departamento de Seguridad Nacional, Gobierno de ESPAÑA, «Estrategia de Seguridad Nacional».

[2] P. Security, «Panda Security,» 10 2018. [En línea]. Available: https://www.pandasecurity.com/spain/mediacenter/src/uploads/2018/10/1611-WP-InfraestructurasCriticas-ES.pdf. [Último acceso: 14 12 2019].

[3] P. d. l. Nación, «COMITÉ DE CIBERSEGURIDAD,» 31 Julio 2017. [En línea]. Available: https://www.boletinoficial.gob.ar/detalleAviso/primera/168225/20170731.

[4] Nación, Presidencia de la, «ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DE LA REPUBLICA ARGENTINA,» 28 Mayo 2019. [En línea]. Available: https://www.boletinoficial.gob.ar/detalleAviso/primera/208317/20190528. [Último acceso: 16 Enero 2020].

[5] P. d. l. Nación, «COMITÉ DE CIBERSEGURIDAD -Modificatoria-,» 12 Julio 2019. [En línea]. Available: https://www.boletinoficial.gob.ar/detalleAviso/primera/211277/20190712.

[6] P. d. l. Nación, «SUBSECRETARÍA DE TECNOLOGÍA Y CIBERSEGURIDAD,» 27 Julio 2016. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/260000-264999/263831/norma.htm.

[7] P. d. l. Nación, «POLITICA DE SEGURIDAD DE LA INFORMACION,» 12 Diciembre 2012. [En línea]. Available: http://servicios.infoleg.gob.ar/infolegInternet/anexos/100000-104999/102188/texact.htm.

[8] P. d. l. Nación, «INFRAESTRUCTURAS CRITICAS,» JEFATURA DE GABINETE DE MINISTROS SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN, 18 09 2019. [En línea]. Available: https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918.

[9] P. d. l. Nación, «CIBERDEFENSA,» MINISTERIO DE DEFENSA, 29 10 2019. [En línea]. Available: https://www.boletinoficial.gob.ar/detalleAviso/primera/219968/20191029.

[10] Information System Authority, «Republic of Estonia Information System Authority,» [En línea]. Available: https://www.ria.ee/en/cyber-

security/critical-information-infrastructure-protection-ciip.html. [Último acceso: 15 Diciembre 2019].

[11] R. L. Kissel, «Glossary of Key Information Security Terms,» NIST, 2013.

[12] W. A. F. A. M. B. y. J. A. M. L. ROSAS BELLO, «Metodologías de evaluación del riesgo en ciberseguridad aplicadas a sistemas SCADA para compañías eléctricas,» *Revista ESPACIO,* vol. 41, nº 7, p. 27, 2020.

[13] European Union Agency for Network and Information Security, «Methodologies for the identification of Critical Information Infrastructure assets and services,» ENISA, Vassilika Vouton, 700 13, Heraklion, Greece, 2014.

[14] www.deChile.net, «Diccionario Etimológico Español en Línea,» [En línea]. Available: http://etimologias.dechile.net/?ciber. [Último acceso: FEBRERO 2020].

[15] Unidas, Naciones, «El uso de internet con fines terroristas,» Publicación de las Naciones Unidas, Austria, 2013.

[16] I. O. f. Standardization, «Information Technology–Security Techniques–Guidelines for Cybersecurity ISO/IEC 27032:2012,» International Organization for Standardization, 2012.

[17] Kaspersky Lab, «Kaspersky Lab Latam,» [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security. [Último acceso: 14 Diciembre 2019].

[18] Pollit M. Mark, «Ciberterrorism: Fact or Fancy,» FBI Laboratory, EE.UU..

[19] Department of Homeland Security, «CRITICAL INFRAESTRUCTURE PROTECTION,» U.S. Government Accountability, Washington D.C., 2005.

[20] World Economic Forum, «The Global Risks Report 2019 14th Edition,» World Economic Forum, Cologny/Geneva Switzerland, 2019.

[21] D. Alandete, «Ediciones El País, S.L.,» Ediciones El País, S.L., 1 Junio 2012. [En línea]. Available: https://elpais.com/internacional/2012/06/01/actualidad/1338572841_317814.html. [Último acceso: 07 Enero 2020].

[22] J. C. Romero, «Estrategias nacionales de ciberseguridad: Ciberterrorismo. Cuadernos de estrategia,» nº 149, pp. 257-322, 211.

[23] A. Banafa, «www.bbntimes.com,» 27 09 2018. [En línea]. Available: https://www.bbntimes.com/en/technology/ddos-attack-a-wake-up-call-for-the-internet-of-things. [Último acceso: 29 07 2019].

[24] ENISA, «The European Union Agency for Cybersecurity (ENISA),» [En línea]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies. [Último acceso: 10 Enero 2020].

[25] «www.whitehouse.gov,» 12 Febrero 2013. [En línea]. Available: https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[26] The White House, «The White House,» 2018. [En línea]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. [Último acceso: 12 Diciembre 2019].

[27] Presidencia de Gobierno, «Departamento de Seguridad Nacional de España,» 2019. [En línea]. Available: https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional. [Último acceso: 10 Enero 2020].

[28] Ministry of Economic Affairs and Communications Republic of Estonia, «Ministry of Economic Affairs and Communications Republic of Estonia,» [En línea]. Available: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf. [Último acceso: 15 Diciembre 2019].

[29] NIST, «https://www.nist.gov/,» Abril 2018. [En línea]. Available: https://www.nist.gov/cyberframework/framework.

[30] Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento, «Sitio oficial de la República Oriental del Uruguay,» [En línea]. Available: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-de-ciberseguridad. [Último acceso: 20 Diciembre 2019].

Anexo

Composición NIST Cybersecurity Framework [29]

Identificadores únicos de funciones y categoría [29]

FUNCIÓN IDENTIFICADOR ÚNICO	FUNCIONES	CATEGORÍA IDENTIFICADOR ÚNICO	CATEGORIAS
ID	IDENTIFICAR	ID.AM	Gestión de activos
		ID.BE	Ambiente de negocios
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	PROTEGER	PR.AC	Gestión de identidad, autenticación y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología de protección
DE	DETECTAR	DE.AE	Anomalías y Eventos
		DE.CM	Monitoreo continuo de seguridad
		DE.DP	Procesos de Detección
RS	RESPONDER	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
		RS.RP	Planificación de respuesta
RC	RECUPERAR	RC.RP	Planificación de la recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

Universidad de Buenos Aires
Facultad de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería
Maestría en Seguridad Informática

Tesis de Maestría

Marco de Referencia de Ciberseguridad para Infraestructuras Críticas

Autor: Esp. Dario Osvaldo RIZZO
Director: Dr. Mariano MENDEZ

Mayo de 2020
Cohorte 2017