Universidad de Buenos Aires

Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Tema: Ciberseguridad

Título: Ciberseguridad implementando el "NIST CYBERSECURITY FRAMEWORK"

Autor: Lic. Dario RIZZO

Tutor: Ing. Hugo PAGOLA

Cotutor: Dr. Mariano MÉNDEZ

Año de Presentación: 2019

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

Dario Osvaldo RIZZO

D.N.I. 28.264.829

Resumen

Con el avance de Internet como medio de comunicación, canal de uso para realizar una transacción e incluso para el manejo de información sensible y privada, se han proliferado y masificado, los intentos de vulnerar los sistemas informáticos mediante la utilización de una infinidad de técnicas y/o herramientas tecnológicas, estos, motivados por distintas razones, pudiendo ser ideológicas, políticas, religiosas o simplemente pruebas de conceptos.

Esto propone un peligro para todas las Organizaciones Gubernamentales como las de índole privadas, ya que pueden ser atacadas con la misma intensidad y vocación por los ciber atacantes, esto apunta principalmente al robo de datos con un fin determinado, basado siempre en la motivación que tienen como detonante, los cuales serán tratados durante el desarrollo del presente trabajo.

Este trabajo final de Especialización propone abarcar el tema de la Ciberseguridad y analizar la estructura de un Marco de Implementación, habiéndose elegido el desarrollado por el NIST[1], pasando por sus orígenes, objetivos, conformación interna, aplicaciones en las distintas industrias, exponiendo que se encuentra basado en las mejores normas y estándares desarrollados que abarcan esta temática, su extensión y adopción como estándar, dado que el mismo adapta su implementación indistintamente del tamaño de la organización.

[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)

Palabras Claves

Ciberespacio, cibercrimen, ciberseguridad, ciberataque, infraestructuras críticas, tecnologías, información, amenaza, estrategia, redes, internet, virus informático, malware.

Índice

Prologo

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 basto conocimiento, hicieron de esta Especialización, una experiencia muy enriquecedora. No puedo olvidarme del Ministerio de SEGURIDAD de la Nación, quien me otorgo una beca para poder realizar la Especialización.

Y, por último, a mis tutores, quienes dieron su mayor esfuerzo, proporcionando sus puntos de vista y conocimientos en todo momento cuando lo requerí. Este documento hubiera sido imposible terminarlo y darle un sentido académico, sin ellos.

Introducción

El presente estudio tiene como objetivo analizar el estado actual de las políticas de seguridad de la información relacionados con la defensa y la gestión de la ciberseguridad, ya sean en el contexto de las organizaciones estatales como así también en las privadas. Se realizará un análisis detallado de la Normativas referentes a la ciberseguridad dentro del ámbito de Gubernamental de la República Argentina. Para comprender los fenómenos relacionados y que afectan directamente a la seguridad informática de los organismos, se contemplarán el conjunto de activos de la información; para tal fin, tomaremos como punto de partida el análisis sobre el marco de ciberseguridad desarrollado por el NIST[2]. En el mismo orden de ideas, se examinarán diferentes casos prácticos en los cuales se vieron afectadas organizaciones que administran servicios críticos y/o fundamentales para el desarrollo sustentable ligados a la calidad de vida de las personas. Profundizando, en los próximos acápites se identificarán los elementos que definen el origen y morfología de cada uno de los riesgos inherentes al área que se investiga. Finalmente, se elaborará una conclusión y recomendarán acciones estratégicas con la finalidad de eliminar o mitigar los riesgos y amenazas relacionados con la ciberseguridad.

[2] 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)

Marco Teórico

A raíz de la importancia que fueron tomando los sistemas informáticos en todos los ámbitos de nuestras vidas, impulsado por el avance tecnológico, la globalización y el intercambio continuo de información, sustentado en la proliferación de las redes de comunicación de datos, podríamos considerar a la seguridad informática como un componente crítico para cualquier clase de Organización.

Es frecuente observar publicaciones de informes de proveedores de tecnología y auditorías, en los cuales se revelan diferentes tipos de ataques -internos y externos- referentes a sus infraestructuras, dejando en evidencia las vulnerabilidades relacionadas con la pérdida, fuga, o robo de información -en el mejor de los casos-, generando consecuencias importantes a la estabilidad, imagen y prestigio de las organizaciones.

Las corporaciones o firmas proveedoras de servicios públicos básicos, o de vital importancia para la ciudadanía -en la actualidad-, tales como los destinados a la generación, gestión y distribución de energía -plantas potabilizadoras de agua, represas-, entre otras, como así también las empresas que administran el transporte público, aeronáutico, servicios financieros, telecomunicaciones y salud; han sido catalogadas como parte de la red de infraestructuras críticas de una Nación o Estado, resultando ser el principal o más incipiente blanco de ataque de los ciberdelincuentes. Estas circunstancias, en ocasiones, están impulsadas por la necesidad de ser oídos en sus reclamos y ser tenidos cuenta por parte de las agendas gubernamentales, ya sea por razones económicas, o bien, con la finalidad de instalar temas en las agendas de gobierno, a través del temor que genera en los decisores políticos por un potencial daño a su imagen y presiones por parte de la opinión pública. En este contexto, se encuentran en auge las amenazas efectuadas por grupos catalogados como Hacktivistas [1] -acrónimo de hacker y activismo- con el objeto de desestabilizar a través de medios cibernéticos, sobre cuestiones políticas, sociales o religiosas. En este sentido, y en virtud de los grandes volúmenes de información sobre

métodos de hacking disponibles abiertamente en redes y medios sociales, sumado al acceso universal de las personas a dispositivos informáticos -año tras año- aumentan exponencialmente los riesgos que los ataques a infraestructuras críticas se materialicen.

En tal sentido, es menester contar con herramientas de autonomía propia, capaces de detectar cualquier tipo de anomalía -o patrón-, a partir de la adopción de medidas proactivas erigidas, principalmente, a la mitigación o disminución de este tipo de amenazas.

Para reforzar conceptos sobre ciberseguridad, se puede destacar lo pronunciado por Javier Candau Romero en su obra “Estrategias Nacionales de Ciberseguridad-Ciberterrorismo”, donde se enseña que los ciberataques afectan a todas las organizaciones, tanto del sector público como el privado, pero fundamentalmente en todos los casos perjudican a los ciudadanos -más allá de su finalidad económica o política- [2]. Este hecho, hace evidente la voluntad de la comunidad de seguridad mediante la implementación de iniciativas para controlar las amenazas provenientes del ciberespacio, apostando a la implementación de técnicas y estrategias de coordinación sobre respuestas a incidentes de seguridad, sustentadas en estándares predefinidos en marcos de trabajo.

Marco Normativo en la Argentina

Como antecedentes locales, si bien la Argentina 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.

Si bien posteriormente, con fecha 12 de Julio del 2019, mediante el decreto Nro. 480/2019 [4], 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 [5].

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 [6], 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.

Todo lo mencionado anteriormente no tiene validez, si no se tiene en cuenta el punto de partida, el cual necesita, el estado actual de la Organización y de los activos informáticos. Siendo estos activos:

- Los recursos de información utilizados por la organización para sustentar sus procesos, entendiéndose por activo a la información propiamente dicha en sus múltiples formatos (papel, digital, imagen, audio y/o video);
- los equipos;
- los sistemas e infraestructura que soportan los diferentes formatos de información y las personas que utilizan esa información, los cuales tiene conocimiento de los procesos internos.

Atento a esto, mediante la resolución administrativa Nro. 252/2016 se solicitó un relevamiento de equipamientos tecnológicos, redes de comunicaciones y datos y estructuras de funcionamiento en centro de procesamiento de datos, para luego elaborar un plan integral, proponiendo un mejor aprovechamiento de los recursos, buscando reducir costos, una mejor eficiencia y una seguridad en las operaciones de toda la APN.

En línea a lo detallado y concurrentemente con la Industria tecnológica, durante el 2019 conjuntamente con la reestructuración Institucional, se ha creado dentro del Organigrama de la Superintendencia FEDERAL de TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES de la Policía Federal Argentina, la Sección CIBERSEGURIDAD, la cual, tendrá a su cargo, el desarrollo e implementación del plan de seguridad de la información de toda la Institución, con el fin de unificar las medidas de prevención ante el robo de información sensible y cuidar los activos informáticos de toda la Organización; como así también, asumiendo la función específica de S.O.C., que puede definirse como: “un centro de seguridad informática, que monitorea la seguridad en la infraestructura de un Organismo, este puede ser interno (con personal propio destinado a tal fin) o externo (tercerizado a una empresa que provee los analistas y la infraestructura tecnológica necesaria para el desarrollo de la tarea)”; la que trabajará conjuntamente con la Sección CIBERTERRORISMO, que es la que judicializara las causas basadas en los delitos informáticos. Considerándose como tal aquella interacción ilegal en la que se utiliza como medio la tecnología o en el que se

busca realizar un daño a un servidor, a una aplicación, a un servicio web y/o redes informáticas. Algunos de estos sucesos se encuentran tipificados en un apartado del Código Penal, definidos bajo la Ley de Delitos Informáticos Nro. 26.388, que se vayan descubriendo. El Ciberterrorismo se 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” [7]

Ciberseguridad

El objetivo principal de la ciberseguridad es evitar la pérdida o robo de información crítica -o sensible-, de manera de garantizar la continuidad, disponibilidad, y acceso permanente a los servicios informáticos. Los tres pilares de la seguridad informática son confidencialidad, integridad y disponibilidad, estos se ven integrados y representados mediante la pirámide o triada CIA como se observa en la *figura 1.*

Figura 1. Representación propia, según la teoría de la Triada CIA.

El NIST [8] define estos importantes conceptos, de la siguiente manera:

- **Confidencialidad:** Preservar las restricciones autorizadas sobre el acceso y la divulgación de información, incluidos los medios para proteger la privacidad personal y la información privada.
- **Integridad:** La propiedad de que los datos confidenciales no se han modificado o eliminado de una manera no autorizada y no detectada.
- **Disponibilidad:** Garantizar el acceso oportuno y confiable y el uso de la información.

A raíz de la lectura de los conceptos mencionados anteriormente, se desprenden otros tres conceptos, no menos importantes y fundamentales, los que en conjunto hacen a la seguridad de la información, debiéndose tenerlos presentes en nuestra labor:

- **Identificación:** El proceso de comprobar la identidad de un usuario, proceso o dispositivo, inicialmente, antes de otorgarle acceso a los recursos de un sistema informático.
- **Autenticación:** El proceso de establecer la confianza de autenticidad.
- **Autorización:** Los privilegios de acceso otorgados a un usuario, programa o proceso.

Definiciones

El NIST ha definido ciberseguridad como la habilidad de proteger o defender el uso del ciberespacio de los ciberataques. De esta definición se desprenden dos grandes interrogantes, ciberespacio y ciberataques. Un ciberataque lo define como, un ataque, mediante la utilización del ciberespacio, que intenta interrumpir, deshabilitar, destruir o controlar maliciosamente un entorno informático y/o infraestructura; o simplemente, destruir la integridad de los datos o robo de información reservada. A su vez, ciberespacio, se define 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. [8]

Una definición más, efectuada por el ISO[3], en su norma ISO/IEC 27032:2012 Gestión de la Ciberseguridad [9], aborda la "Ciberseguridad" o "la seguridad del Ciberespacio", como la "preservación de la confidencialidad, integridad y disponibilidad de información en el Ciberespacio". A su vez, "el ciberespacio" se considera como "el entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos y redes conectadas a él, que no existe en cualquier forma física" [9].

Desde el punto de vista comercial, la firma privada denominada Akamai [10], líder en distribución de servicios de seguridad informática, la cual define ciberseguridad como: sistemas y principios los cuales se han diseñado para proteger sitios y aplicaciones web, de los atacantes, que pretenden interrumpir, retrasar, modificar o redirigir el flujo de datos. Estos atacantes pueden tener objetivos, niveles de organización y capacidad técnica diferente, como hemos veremos posteriormente en su clasificación, por este motivo, los organismos públicos y empresas privadas deben adoptar cada vez más medidas preventivas para mitigar los ciberataques. Desde estos dos puntos de vistas, la ciberseguridad se presume de la siguiente manera:

- Desde el Gubernamental, se mantienen medidas de ciberseguridad para proteger la integridad de las infraestructuras críticas de sus sistemas financieros, instituciones de atención sanitaria, científicas y de seguridad, y organismos de defensa, aeroespaciales y de inteligencia.
- Desde el de las empresas privadas utilizan ciberseguridad y protección de datos online para evitar pérdidas de ingresos, daños

[3] International Organization for Standardization (Organización Internacional de Normalización ISO, por sus siglas en inglés)

en la reputación de la marca y posibles multas o responsabilidades legales. [10]

Agentes de la amenaza

Teniendo en cuenta que el ciberespacio no tiene fronteras, los ataques podrían provenir de cualquier punto del mundo, perpetrados por alguno de los siguientes actores:

- 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.

Estos actores pueden tener múltiples motivaciones y cuestiones que buscan una finalidad determinada: inteligencia, espionaje industrial, propiedad intelectual, motivos políticos, extremismo, motivaciones económicas, etc. En especial, los Estados, tienen un aparato preparado por el cual podrán ejecutar estos ataques, sus servicios de inteligencia, las unidades de ciberdefensa de las Fuerzas Armadas, contratando servicios a privados o mercenarios, o solamente motivando mediante la opinión pública a grupos extremistas. Estos últimos, por lo general, son los que definen los ataques como ciberterrorismo [2].

Teniendo en cuenta el poder de ataque y el impacto que se desea lograr en el ciberespacio, podemos destacar las siguientes manifestaciones:

- **Crimen Organizado.** Estas organizaciones tienen como fin, el robo de información sensible o certificados digitales asociadas a las personas, para realizar fraudes telemáticos, asociados a operaciones bancarias o transacciones digitales, buscando el blanqueo de este, introduciéndolo al mercado financiero para financiar sus actividades ilegales [2].

- **Espionaje industrial.** Son empresas o gobiernos que tienen como objetivo, obtener información crítica y/o reservada de patentes de nuevas tecnologías o industriales de la competencia [2].
- **Hacking Político / Patriótico.** Este tipo de actividad se conoce por medio de la prensa o los medios de comunicaciones masivos, siendo el reflejo de conflictos que tienen como precursor, problemas regionales, étnicos, religiosos o culturales en el ciberespacio. Diariamente se observan ataques de denegación de servicio entre países China y Japón; Azerbaiyán y Turquía; India y Pakistán, chiitas y sunitas o el conflicto entre árabes e israelíes. Por lo general, no tienen gran impacto en los Sistemas de Información de un País, ya que se atacan Servicios Web públicos, no llegando a los servicios internos [2].
- **Servicios de inteligencia.** Son considerados las principales amenazas contra la información sensible o clasificada que manejan los sistemas informáticos las Infraestructuras Criticas o Gubernamentales. Poseen recursos, tanto económicos como técnicos, capaces de un gran poder de acción. Sus actividades son a un largo plazo, utilizando herramientas de desarrollo propio, que difícilmente sean detectadas por las tecnologías de defensa convencionales que son utilizadas en los puntos atacados, necesitando de un gran poder de análisis humano complementado por herramientas de manejo de datos [2].
- **Unidades cibernéticas de Fueras Armadas.** Pueden ser considerados un vector de amenaza critico en momentos de crisis o conflicto. Algunos países este rol lo cumplen los servicios de inteligencias, aunque en otros las F.F.A.A., estas últimas, disponen de unidades tanto para la defensa como para ejecutar ataques coordinados contra un punto determinado como enemigo [2].
- **Terrorismo.** Los grupos terroristas utilizan el ciberespacio como medio para perpetrar sus actos ilícitos o atentados virtuales, además, lo utilizan como enlace de comunicación para enviarse información

entre sus aliados y o células distribuidas, de los puntos de interés de ataque o financiamiento económico [2].

- **Hackers.** Existen numerosas definiciones respecto a este tipo de denominación, depende de las presunciones que posea el observador. Nos centraremos en aquel individuo que utiliza su conocimiento para ingresar en un activo informático (sistema o red), con la finalidad de sustraer información o afectar el normal funcionamiento de un sistema [8]. Un ejemplo de esto es el reciente caso que sufrió una fuerza de seguridad de la Nación, blanco de un robo de información por un grupo de estos individuos, utilizando técnicas por las que aprovecharon una vulnerabilidad en la infraestructura de red y utilizaron ingeniería social para el robo de credenciales, pudiendo acceder a información sensible, conceptos que serán desarrollados posteriormente [11].
- **Actores Internos.** Nos referimos a empleados internos de una Organización o compañía, que producen daño internamente, aprovechando sus privilegios de acceso a ciertos sistemas o brindando información a entes externos para que realicen el ataque [12].
- **Desarrolladores de Programas Maliciosos.** En este punto se considera a aquellos individuos que utilizan su alto conocimiento en un lenguaje de programación, para desarrollar aplicaciones que utilizan alguna vulnerabilidad conocida de un sistema operativo, que tienen como resultado efectos negativos para las sociedades, organizaciones o individuos [12].

Metodologías utilizadas para la perpetración de ciberataques

Ya habiendo realizado una definición, los Ciberataques comparten ciertas características comunes entre ellos, agrupándolos de la siguiente manera:

- Inversión mínima o nula: existen innumerables herramientas de uso gratuito que se pueden descargar para realizar ataques, funcionales en los múltiples sistemas operativos (como ser: Aircrack-ng, THC Hydra, John the Ripper, Metasploit Framework, Netcat, Nmap “Network Mapper”, Nessus; las cuales se encuentran disponibles en la red para su descarga e instalación, siendo de fácil acceso y usabilidad), cabe destacar, que estas herramientas son utilizadas éticamente, para realizar análisis de vulnerabilidades externas, a pedido de un organismo u empresa a sus proveedores de servicios de seguridad informática.
- Facilidad de uso: para realizar los ataques estándares o básicos, no se necesita de una experticia técnica elevada, ya que estas herramientas poseen interfaces sencillas y amigables, con guías para su utilización, incluso muchas de estas o similares, se ven en las capacitaciones de ética hacking o en las distintas cátedras del ámbito académico.
- Certeza: cuentan con una alta probabilidad de llegar al objetivo buscado con el ataque ejecutado, ya que, del lado de la defensa, existen vulnerabilidades desconocidas, tanto en las aplicaciones de software como en la infraestructura que estas utilizan, falta de inversión en tecnología específica aplicada a la seguridad informática, una baja concientización respecto a la seguridad informática en la Organizaciones, Instituciones y personas, siendo este el eslabón más bajo en la cadena de la seguridad.
- Baja exposición y riesgo para el ciber atacante: se torna muy difícil atribuir el suceso a un individuo, debido a la implementación de técnicas de rastreo, además, de ser muy difícil la aplicabilidad de una ley para tipificar el delito, siendo que el ataque puede venir dirigido de cualquier punto del planeta, utilizando INTERNET como medio para llegar a un determinado objetivo.

Los ciberdelincuentes, ya sea su motivo o ideología para realizar su ofensiva, utilizan múltiples métodos de ataques, pueden ser adaptados o

combinados para que el daño sea mayor, o se complementen para llegar al objetivo final.

Estos ataques pueden ser de diferentes estilos y modalidades: el "spear-phishing", DDoS -Denial Of Service (Denegación de Servicio), Inyección SQL, ataques de fuerza bruta, la evolución del Malware, Spoofing, el filtro de scripts de sitios (XSS), por nombrar algunos; buscando ser mitigados por todo tipo de herramientas tecnológicas, tanto de Software como de Hardware específicos, para tal fin, o un paso más allá, implementando un SOC (Security Office Center) que monitoree las 24 horas la Infraestructura el que cuente con distintos niveles de operadores que cumplan la función de analistas:

- Spear-phishing: consiste en una estafa por correo electrónico en el que se apunta directamente a un usuario especifico, empresa u organización, como único fin, el robo de información [8].

- DDoS -Denial Of Service (Denegación de Servicio): son ataques de red distribuidos, en el que se aprovecha la limitación de recursos asignado a un recurso informático, por el cual, se producen varias peticiones al recurso definido como blanco, buscando desbordar la capacidad de este, produciendo un colapso del mismo, a fin de no poder seguir atendiendo peticiones [8]. Un caso actual: “This fear was realized with a massive distributed denial of service attack that crippled the servers of services like Twitter, NetFlix, NYTimes, and PayPal across the U.S. on October 21st, 2016. It’s the result of an immense assault that involved millions of Internet addresses and malicious software, according to #Dyn, the prime victim of that attack. "One source of the traffic for the attacks was devices infected by the Mirai botnet" the link to the source code of #Mirai malware on GitHub is here.” [13]

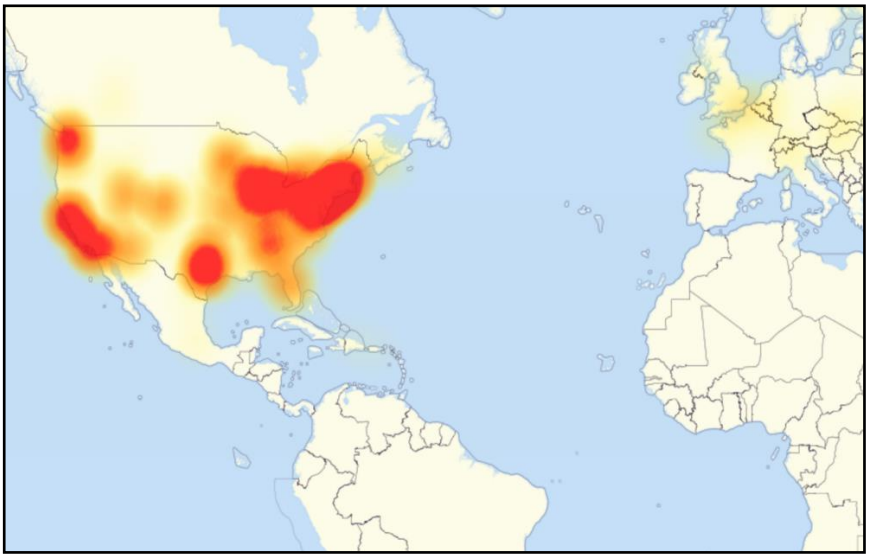

Figura 2. Mapa que muestra las áreas afectadas por el corte de Internet el viernes 21 de octubre de 2016 [13]

- Inyección SQL: es una técnica, por la que el atacante crea o altera comandos SQL almacenados en un servidor, buscando de esta manera acceder a datos ocultos [14].

- Ataques de fuerza bruta: este tipo de ataque busca descifrar las credenciales de acceso a un Sistema Informático, para robar información, introducir algún tipo de malware, siendo una ventana abierta para iniciar cualquier ataque de los detallados anteriormente [8].

- Malware: Programa que se introduce en un sistema informático, generalmente de forma encubierta, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos, las aplicaciones o el sistema operativo de la víctima, o de molestar o perturbar a la víctima [8].

- Spoofing: se refiere al uso de metodologías y/o técnicas para la suplantación de identidad, Involucrando:

    - la capacidad de recibir un mensaje haciéndose pasar por el destino legítimo de recepción, o

    - haciéndose pasar por la máquina de envío y enviando un mensaje a un destino. [8]

- Sniffer: es un programa que captura los paquetes de datos de una comunicación informática, examinándolos, permitiendo de esta manera encontrar información valiosa que permite perpetrar un posterior ataque o simplemente robarla [8].
- Troyano: o bien llamado Caballo de Troya, es un malware que se presenta ante un usuario como un programa legítimo, que en su interior esconde código malicioso que evita los mecanismos de seguridad, con lo cual, una vez ejecutado, el atacante puede tomar control remoto del equipo infectado [8].
- Virus: es un programa de computadora que puede copiarse e infectar una computadora sin permiso o conocimiento del usuario. Puede corromper o eliminar datos en una computadora, usar programas para propagarse hacia otros sistemas o incluso eliminar toda la información de un disco de almacenamiento [8].
- Gusano: es un programa de software malicioso que se replica así mismo en una computadora, y se distribuye aprovechando las conexiones que posee el equipo infectado hacia otras, sin intervención del usuario [8].
- Ingeniería Social: es una técnica que usan los atacantes, por la cual tratan de engañar, mediante habilidades sociales, a usuarios legítimos con la finalidad de adquirir información confidencial o que efectúen ciertas acciones [8].
- Ransomware: es un tipo de programa dañino que priva el acceso a información a un usuario, encriptándola, para luego exigirle un pago como rescate por facilitarle el acceso nuevamente a la misma [15].

Por eso, es tan importante la implementación de un marco de trabajo de integral, en el que se involucre a toda la Organización, como así, también a la totalidad de los integrantes de esta para que el mismo tenga un correcto

fin. Siendo un Profesional en la Materia, hemos visto y analizado varias normas, estándares y procedimientos que actualmente son guías sobre esta temática, como ser: ISO/IEC 27001:2013, COBIT, las directrices de COSO o NIST SP 800-53, por solo nombrar algunos.

Framework de Ciberseguridad según el NIST

El NIST (Instituto Nacional de Estándares y Tecnología) de los Estados Unidos, posee un “Marco para la mejora de la Seguridad cibernética en infraestructuras críticas”, actualmente se encuentra disponible en su versión 1.1 publicado el 16 de Abril del 2018, el que ofrece, la posibilidad de implementar mejoras en lo que refiere a la Ciberseguridad, teniendo en cuenta, que existen riesgos específicos para cada tipo de Organización acorde a su función dentro de la estructura del Estado en sí, lo que se busca con la implementación es reducir y gestionar mejor los riesgos de la seguridad cibernética.

Origen

Visto lo mencionado anteriormente, alineado con la problemática en el que se encontraban las Organizaciones Gubernamentales de los Estados Unidos de Norteamérica, en lo concerniente a la ciberseguridad ya que eran blancos constantes de los ciber atacantes, lo que demostraba la necesidad de una mejora continua en esta especificidad, es que nace el Marco de Trabajo de Ciberseguridad del NIST (National Institute of Standards and Technology), en el período de Barack Obama como presidente, a través de la Orden Ejecutiva Nro. 13.636 del 12 de febrero del 2013, la cual consta de 12 secciones, siendo el foco principal la protección de las Infraestructuras Críticas de ese País, introduciéndolas dentro del ámbito de aplicación de la Seguridad Nacional y la Economía; ya que son la base de lo antes mencionado, definiéndolas como todo sistema y activos, ya sean físicos o virtuales, tan vitales que la incapacidad o destrucción de tales sistemas y

activos tendría un impacto debilitante en la seguridad, la seguridad económica nacional, la opinión pública nacional. Salud o seguridad, o cualquier combinación de esos asuntos. [16]

Marco de trabajo

Las bases del Marco de Trabajo se pueden desprender directamente de la Orden Ejecutiva Nro. 13.636, siendo las siguientes:

- El centro del Marco es el conjunto de funciones que engloban la seguridad cibernética siendo comunes en todos los sectores de la Organizaciones.
- Definir una guía para el manejo de los riesgos de ciberseguridad como parte de la gestión de los procesos de la Organización.
- Enfocar en la aplicación de iniciadores de negocios para la totalidad de las actividades desarrolladas para la ciberseguridad.
- Ayudará a la Organización a alinear y priorizar los recursos y/o actividades de seguridad cibernética, teniendo en cuenta el negocio.
- El marco representa un documento dinámico, en constante mejora, en base a las recomendaciones y comentarios de las Organizaciones que lo implementen.
- Evitar la implementación de nuevos estándares, si ya se cuenta con una normativa que ya cubre o abarque los descritos en dicha orden ejecutiva. [16]

¿En qué Estándares, Normativas, Mejores Prácticas e Informes se basa la presente Guía de implementación?

- Control Objectives for Information and Related Technology (COBIT) [17]
- Council on Cybersecurity (CCS) Top 20 Critical Security Controls (CSC) [18]

- ANSI/ISA-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program [19]
- ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels [20]
- ISO/IEC 27001:2013, Information technology –Security techniques – Information security management systems –Requirements [21]
- NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations [22]

Composición del marco de trabajo

El marco de trabajo [23] define, con la finalidad de entender, gestionar y definir, los riesgos inherentes de ciberseguridad, a la totalidad de las partes interesadas (tanto internas como externas), teniendo en cuenta como ámbito de aplicación un ente u organismo. Una de sus finalidades, es brindar ayuda para identificar y priorizar operaciones, buscando de esta manera reducir los riesgos de ciberseguridad. Siendo una herramienta útil para alinear los puntos de vistas en lo referente a las políticas, negocios y tecnologías, disponibles para el manejo de los riesgos. Pudiéndose destacar, su utilización para el manejo de riesgos en los componentes de la organización o focalizándose en los servicios críticos internos de la misma.

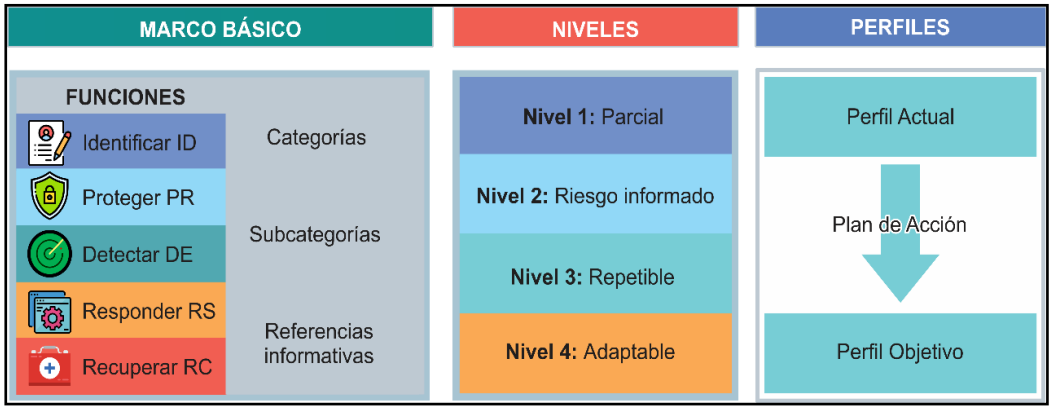

Figura 3. Representación propia, composición NIST Cybersecurity Framework [23]

Núcleo del Marco

El núcleo de trabajo [23] ofrece un conjunto de actividades cronológicamente ordenadas, que en conjunto logran resultados significativos en la seguridad informática de la organización, las cuales poseen referencias a ciertos ejemplos y guías de implementación para poder llevarlas a cabo, representando los resultados que son claves para todas las partes interesadas, como así también, útiles para la gestión del riesgo. Como puede observarse en la figura 4, el núcleo consta de cuatro elementos: Funciones, Categorías, Subcategorías y Referencias Informativas, las que van interactuando entre sí.

Estas funciones organizan las actividades básicas de ciberseguridad en su nivel más alto, siendo: Identificar, Proteger, Detectar, Responder y Recuperar. Estas ayudan a la organización a expresar su gestión de riesgos de ciberseguridad, organizando los activos informáticos, permitiendo de esta manera, una correcta toma de decisiones para su gestión, afrontando las amenazas y realizar un aprendizaje de las actividades que las anteceden. Las mismas se corresponden con las metodologías existentes para la gestión de sucesos y ayudan a mostrar el gran impacto que pueden tener las inversiones que se realizan en ciberseguridad, la que tiene como finalidad mitigarlos.

Estas cinco funciones no están definidas como un camino estático, el cual hay que seguirlo en forma secuencial, sino, lo que se busca es que se ejecuten en forma concurrente y continua, teniendo como objetivo, formar una cultura operacional que afronte el dinamismo de los retos continuos que ofrece la temática que estamos desarrollando. Se encuentran identificadas con dos letras, ID, PR, DE, RS y RC, respectivamente como se puede observar en la Figura 4.

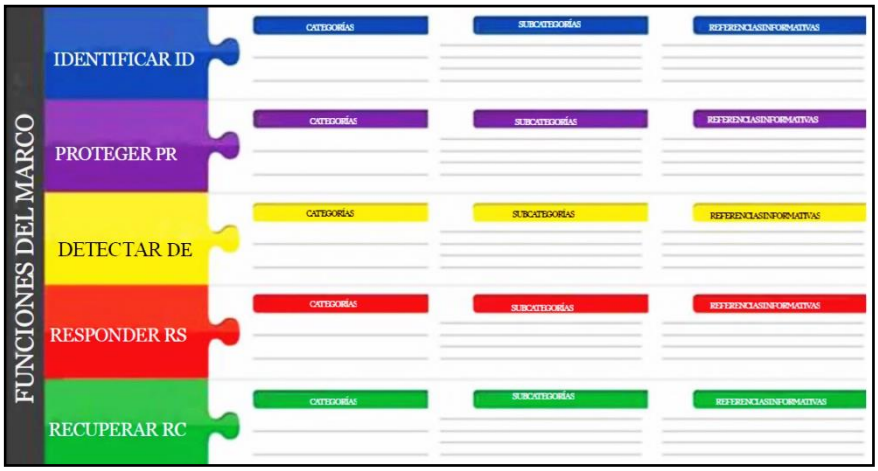

Figura 4. Núcleo del NIST Cybersecurity Framework [23]

- IDENTIFICAR -ID-: Desarrollar una comprensión organizacional para la gestión de riesgo de ciberseguridad en los activos de información. Las actividades de la función Identificar son fundamentales para el efectivo uso del marco. Se busca entender la lógica y contexto del negocio, identificar los recursos que le dan soporte a las funciones críticas y los riesgos de ciberseguridad relacionados a estos, permitiendo a la organización enfocarse y priorizar sus esfuerzos relacionados con su estrategia y las necesidades que el negocio impone. Algunos ejemplos dentro de esta función son: Gestión de Activos, Contexto del Negocio, Estimación de Riesgos, Gobernanza y Estrategia de gestión de riesgos.

- PROTEGER -PR-: Desarrollar e implementar defensas acordes para asegurar la continuidad de los servicios que fueron identificados como críticos. Esta función permite que el impacto de un posible un evento de ciberseguridad sea mitigado o contenido en un corto tiempo. Algunos ejemplos dentro de esta función son: Gestión de identidad y control de acceso, Dictado de capacitación y concientización, Seguridad de datos, Procesos y procedimientos de protección de información, Mantenimiento e Implementación de tecnologías de protección.

- DETECTAR -DE-: Desarrollar e implementar actividades para identificar la ocurrencia de un evento de ciberseguridad. La función de detección permite un prematuro reconocimiento de un evento de ciberseguridad. Algunos ejemplos dentro de esta función son: Eventos y anomalías, Monitoreo continuo de seguridad y Procesos de detección.

- RESPONDER -RE-: Desarrollar e implementar actividades acordes para ejecutar ante un incidente de ciberseguridad. Esta función permite contener el impacto de un potencial evento de ciberseguridad, encapsulándolo y tomando las acciones que sean necesarias para mitigarlo. Algunos ejemplos dentro de esta función son: Plan de respuesta ante incidentes, Comunicación, Análisis, Mitigación y Mejoras.

- RECUPERAR -RC-: Desarrollar e implementar actividades para llevar a cabo planes de resiliencia y restitución de cualquier servicio que se haya visto afectado o disminuido por un evento de ciberseguridad. Esta función da soporte al restablecimiento de las operaciones, para evitar que esto no impacte negativamente en la operativa normal de las funciones que se llevan a cabo. Algunos ejemplos de los resultados de esta función son: Plan de recuperación ante desastres, Mejoras y Comunicación.

Niveles de implementación del Marco

Los niveles de implementación del Marco de Trabajo [23] otorgan un contexto de como la organización observa los riesgos de ciberseguridad y los procesos que utilizan para gestionarlos. Desde el Nivel Parcial (Nivel 1) al Adaptativo (Nivel 4), describen el aumento parcial del grado de rigor y sofisticación en la gestión de riesgos de ciberseguridad. Estos permiten determinar el alcance de la gestión de riesgos de ciberseguridad, integrando el manejo de estos dentro de la organización. Esta gestión, incluye muchos

aspectos de la ciberseguridad, incluyendo, en primera medida, en como la privacidad y libertades civiles se integran a dicha gestión de la organización y sus posibles respuestas. Dicho proceso, debe tener en cuenta las prácticas de gestión de riesgos que se utilizan, ambientes de amenazas, requerimientos legales y reglamentarios específicos, prácticas en el intercambio de información entre organismos, los objetivos del negocio, los requerimientos de ciberseguridad en toda la cadena de provisión y los limites organizacionales.

Las organizaciones deben especificar el Nivel al que se desea llegar, contrastando de que cumpla o este alineado con los objetivos de la organización, sea posible de implementar (por distintos factores) y ofrezca una reducción en los riesgos cibernéticos para los activos o recursos críticos que soportan el negocio, a niveles aceptables. Como punto importante, las organizaciones deben considerar utilizar cualquier ayuda externa, proveniente de Organizaciones Gubernamentales, los Centros de Análisis e Intercambio de información (ISAC), las Organizaciones de Análisis e Intercambio de Información (ISAO) o cualquiera fuente que estimen que es acorde al nivel de madurez de la organización, con la finalidad de determinar su Nivel deseado.

Si bien, las organizaciones identificadas como Nivel 1 (Parcial) son alentadas a considerar el Nivel 2 o superior, sin olvidar, que los niveles no representan niveles de madurez; los niveles fueron determinados para que contribuyan y sirvan de soporte para la toma de decisiones para gestionar los distintos riesgos que vayan surgiendo, así como, para determinar que dimensión de la organización tiene prioridad sobre otra a fin de recibir recursos extras. En definitiva, se incentiva escalar de Nivel, cuando como resultado de un análisis de costo beneficio impacta directamente en una reducción rentable del riesgo.

La implementación exitosa del marco está basada en logar los resultados descritos en el perfil(s) objetivo(s) de la organización y no en la

determinación del nivel. Sin embargo, la selección y designación de nivel afecta naturalmente a los perfiles del marco. La recomendación de nivel por los gerentes de negocio o de proceso, ayudará a establecer en forma general cómo se gestionará el riesgo de ciberseguridad dentro de la organización, e influyendo en la selección de un Perfil Objetivo y en las evaluaciones del progreso para abordar las vulnerabilidades.

Nivel 1: Parcial

- **Proceso de gestión de riesgos:** las prácticas de gestión de riesgos de ciberseguridad organizacional no están formalizadas, y los riesgos se gestionan de manera ad hoc y de forma reactiva. La priorización de las actividades de ciberseguridad puede no ser informada directamente por los objetivos de riesgo de la organización, el entorno de amenaza o los requisitos del negocio y misión.

- **Programa Integrado de Gestión de Riesgos:** la concientización sobre el riesgo de ciberseguridad a nivel organizativo es limitado. La organización, implementa la gestión del riesgo de ciberseguridad de forma irregular, caso por caso, debido a la experticia o al nivel de información obtenida de fuentes externas. Es posible que la organización no tenga procesos que permitan compartir la información de ciberseguridad dentro de la organización, por distintas razones.

- **Participación externa:** la organización no entiende su papel en el ecosistema al que pertenece con respecto a sus dependencias o dependientes. La organización no colabora ni recibe información (por ejemplo, inteligencia sobre amenazas, mejores prácticas, tecnologías) de otras entidades (por ejemplo, compradores, proveedores, dependencias, dependientes, investigadores, gobiernos), ni comparte información. La organización generalmente desconoce los riesgos cibernéticos de la cadena de suministro de los productos y servicios que proporciona y que utiliza.

Nivel 2: Riesgo Informado

- **Proceso de gestión de riesgos:** las prácticas de gestión de riesgos son aprobadas por la gerencia, pero pueden no estar establecidas como una política en toda la organización. La priorización de las actividades de ciberseguridad y las necesidades de protección están directamente informadas en los objetivos de riesgo de la organización, el entorno de amenaza o los requisitos del negocio / misión.

- **Programa Integrado de Gestión de Riesgos:** existe una conciencia del riesgo de ciberseguridad a nivel organizacional, pero no se ha definido un enfoque en toda la organización para su gestión. La información sobre ciberseguridad se comparte en la organización por canales informales. La consideración de la ciberseguridad en los objetivos y programas de la organización se encuentra parcialmente establecida, pero no en algunos niveles. La evaluación del riesgo cibernético de los activos organizativos y externos se realiza, pero no suele actualizarse, es decir, no se efectúa en forma repetida con la constancia necesaria.

- **Participación externa:** en general, la organización entiende su papel en el ecosistema más amplio con respecto a sus propias dependencias o dependientes, pero no a ambas. Colabora y recibe información de otras entidades y genera parte de su propia información, pero no procede a compartirla. Además, la organización es consciente de los riesgos cibernéticos de la cadena de suministro asociado con los productos y/o servicios que proporciona y/o utiliza, pero no actúa de manera consistente o formal sobre esos riesgos.

Nivel 3: Repetible

- **Proceso de gestión de riesgos:** Las prácticas de gestión de riesgos de la organización se aprueban formalmente y se expresan como

políticas. Las prácticas de ciberseguridad organizacional se actualizan periódicamente en función de la aplicación de los procesos de gestión de riesgos a los cambios en los requisitos empresariales sobre la misión y ante un panorama cambiante de amenazas y tecnología, fuera del ámbito de la organización.

- **Programa integrado de gestión de riesgos:** Existe un enfoque en toda la organización para la gestión de los riesgos de ciberseguridad. Las políticas, procesos y procedimientos informados sobre el riesgo se definen e implementan según lo previsto y son revisados. Existen métodos consistentes para responder de manera efectiva a los cambios en el riesgo. Los recursos humanos poseen el conocimiento y las habilidades necesarias para cumplir con sus funciones y responsabilidades asignadas. La organización monitorea de manera constante y precisa el riesgo de los activos de toda la organización. Los encargados de la ciberseguridad como de los otros sectores poseen una comunican fluida, con respecto al riesgo de ciberseguridad. Los altos ejecutivos observan y aseguran que se tome en consideración la ciberseguridad en todas las líneas de operación de la organización, dentro de la cultura organizacional.

- **Participación externa:** La organización entiende su función, sus dependencias y sus dependientes dentro del ambiente al que pertenece y contribuye a comprender los riesgos a los que se enfrenta la comunidad. Colabora y recibe información de otras entidades regularmente que complementa la información generada internamente, compartiéndola con otros entes. La organización es consciente de los riesgos cibernéticos en la cadena de suministro asociados con los productos y servicios que proporciona y que utiliza. Actuando de manera formal sobre esos riesgos, por ejemplo, con mecanismos como acuerdos escritos para comunicar los requisitos, las estructuras de gobierno (por ejemplo, los consejos de riesgo) y la implementación y supervisión de políticas.

Nivel 4: Adaptable

- **Proceso de gestión de riesgos:** La organización adapta sus prácticas de ciberseguridad basadas en actividades anteriores y actuales, incluidas las lecciones aprendidas y los indicadores predictivos. A través de un proceso de mejora continua que incorpora tecnologías y prácticas avanzadas de ciberseguridad, la organización se adapta activamente a un panorama de constantes cambios en las amenazas y tecnología, respondiendo de manera oportuna y eficaz a las más sofisticadas y evolucionadas.

- **Programa integrado de gestión de riesgo:** Existe un enfoque en toda la organización para gestionar el riesgo de ciberseguridad en el que se utilizan políticas, procesos y procedimientos como un todo, informados sobre el riesgo para abordar posibles eventos de ciberseguridad. La relación entre el riesgo de ciberseguridad y los objetivos de la organización son comprendidos y tomados muy en cuenta en la toma de decisiones sobre el negocio. Los ejecutivos monitorean el riesgo de ciberseguridad en el mismo contexto que el riesgo financiero y otros riesgos organizacionales, poniéndolos al mismo nivel en la toma de decisiones. El presupuesto de la organización está basado en la comprensión del entorno de riesgo actual y previsto, con la correspondiente tolerancia al riesgo. Las unidades de negocios implementan la visión ejecutiva y analizan los riesgos a nivel del sistema en el contexto de las tolerancias de riesgo organizacionales. La gestión del riesgo de ciberseguridad es parte de la cultura organizacional. esta evoluciona desde el conocimiento de las actividades anteriores y un conocimiento continuo de las actividades en sus sistemas y redes. La organización puede dar cuenta rápida y eficazmente de los cambios en los objetivos de negocio o misión en la forma en que se aborda y se comunica el riesgo.

- **Participación externa:** La organización comprende su función, sus dependencias y sus dependientes del ecosistema, contribuyendo a la comunidad sobre los riesgos. Recibe, genera y revisa información calificada por su relevancia, en base al análisis continuo de sus riesgos, a medida que evolucionan las amenazas y la tecnología. La organización comparte esa información interna y externamente con otros colaboradores. La organización utiliza información prácticamente en tiempo real para comprender y actuar de manera coherente con los riesgos de la cadena de suministro cibernéticos asociados con los productos y servicios que proporciona y utiliza. Además, se comunica de forma proactiva, utilizando mecanismos formales (por ejemplo, acuerdos) e informales para desarrollar y mantener relaciones sólidas con la cadena de suministro, como se muestra en la siguiente Figura 5.

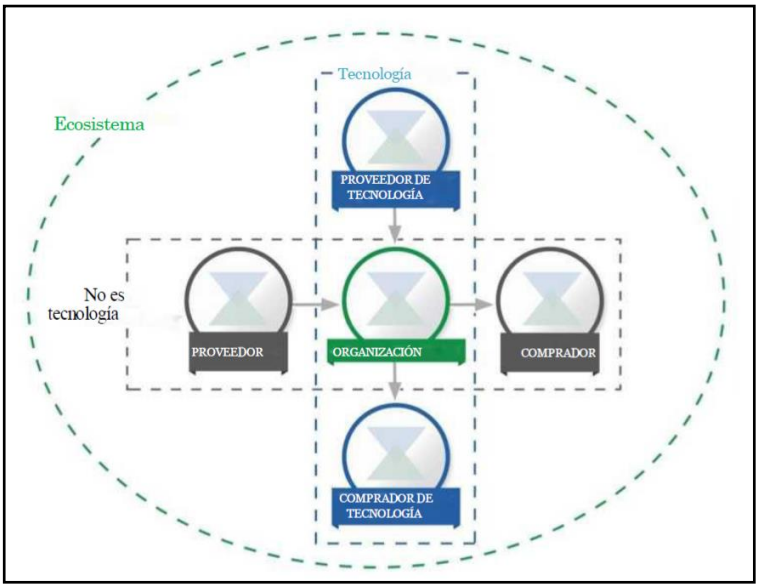

Figura 5. Relaciones de la cadena de suministros cibernéticos [22]

Perfil del Marco

El perfil del marco de trabajo determinado por el NIST [23] es la alineación entre las funciones, categorías y subcategorías con los requerimientos comerciales, la tolerancia al riesgo y los recursos de la organización. Permitiendo a las organizaciones establecer una hoja de ruta para reducir el riesgo de ciberseguridad, a la vez que se alinean con los objetivos organizacionales y sectoriales, considerándose, requisitos legales o reglamentarios y las mejores prácticas de la industria, reflejando de esta manera las prioridades para su gestión. Teniendo en cuenta la compleja estructura de muchas organizaciones, pueden elegir tener múltiples perfiles, alineados con componentes particulares reconociendo sus necesidades individuales.

Los perfiles del marco pueden describir el estado actual o el estado deseado para las actividades específicas de ciberseguridad. El perfil actual indica los resultados de ciberseguridad que se están logrando. El perfil de objetivos indica los resultados necesarios para lograr los objetivos de gestión de riesgos de ciberseguridad deseados. Estos perfiles respaldan los requisitos empresariales o de misión, ayudando, a comunicar el riesgo dentro y entre las organizaciones. Este marco no determina plantillas de perfil, lo que permite flexibilidad en su implementación.

Al efectuar una comparación de perfiles (por ejemplo, el perfil actual y el perfil objetivo) puede revelar las vulnerabilidades que deben abordarse para cumplir con los objetivos de la gestión de riesgos de ciberseguridad. Un plan de acción para atacarlas, para satisfacer una Categoría o Subcategoría dada puede contribuir a la hoja de ruta descrita anteriormente. Priorizar la mitigación de las vulnerabilidades se debe a las necesidades comerciales de la organización y los procesos de administración de riesgos. Este enfoque basado en el riesgo permite a una organización medir los recursos necesarios (por ejemplo, personal, financiamiento) para lograr los objetivos de ciberseguridad de manera rentable y prioritaria. Además, el marco es un

enfoque basado en el riesgo donde la aplicabilidad y el cumplimiento de una subcategoría determinada están sujetos al alcance del perfil.

Gestión de Riesgos

La gestión de Riesgos desde la perspectiva del NIST [23], se puede observar en la figura 6, en la que se describe el flujo común de información y decisiones entre los niveles de la organización:

- Ejecutivo,
- Empresarial / Proceso,
- Implementación / Operaciones

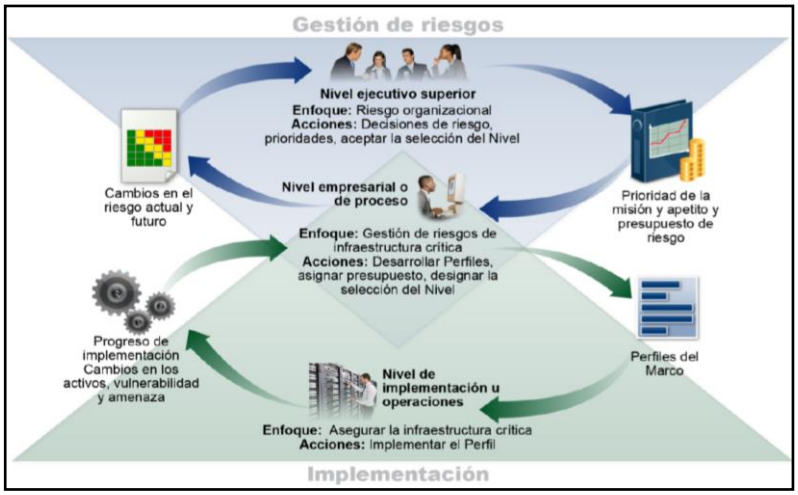

Figura 6: Flujos de comunicación y decisión dentro de una Organización [23]

El nivel ejecutivo comunica las prioridades de la misión, los recursos disponibles para cumplirla y la tolerancia al riesgo general con la que se actuara a nivel empresarial o proceso. Esto utiliza la información como entrada para el proceso de gestión de riesgos, y luego se comparte con el nivel de implementación u operaciones, para informarle las necesidades del negocio y crear un Perfil. El nivel de implementación u operaciones comunica el avance en el establecimiento del perfil al nivel empresarial o de proceso. Este utiliza la información como entrada, para realizar una evaluación del impacto. La administración de nivel empresarial o de proceso

informa los resultados de esa evaluación de impacto al nivel ejecutivo para informar el proceso general de gestión de riesgos de la organización y el nivel de implementación u operaciones para la conciencia del impacto comercial.

Implementación del Marco de Ciberseguridad en una Organización

La implementación del marco de trabajo de ciberseguridad basado en el NIST tiene como finalidad crear un nuevo plan o simplemente realizar una mejora del implementado, consta de 7 pasos, los que se deben ejecutar en forma iterativa tomando el paso anterior como punto de entrada para corroborar la ciberseguridad de la Organización:

Paso 1. Priorización y definición de alcance: la organización debe identificar los objetivos y misión organizacionales del negocio. Habiendo efectuado esto, se realiza la estrategia de implementación de ciberseguridad, buscando proteger los procesos fundamentales del negocio, siempre teniendo en cuenta la tolerancia al riesgo con la que se cuenta.

Paso 2. Orientación: una vez definido el alcance del plan de ciberseguridad del negocio, la organización debe identificar los activos y marcos regulatorios; debiéndose consultar fuentes para identificar amenazas y vulnerabilidades que se aplican a los activos.

Paso 3. Crear un perfil actual: la organización desarrolla un relevamiento con la finalidad de identificar qué perfil indicando que categoría y subcategoría del marco que se encuentra implementado.

Paso 4. Ejecutar un análisis de riesgos: la organización realiza un análisis del entorno productivo sobre la probabilidad de ocurrencia de un evento de ciberseguridad, es importante, que se utilice información técnica de fuentes externas e internas con el fin de que la misma sea actualizada.

Paso 5. Crear un perfil objetivo: la organización crea el perfil deseado al que se pretende llegar, utilizando el marco, utilizando también información externa para determinarlo.

Paso 6. Determinar, analizar y priorizar brechas: la organización compara los perfiles desarrollados en los puntos 3 y 5, con la finalidad de desarrollar un plan para atacar las vulnerabilidades, a fin de cumplimentar con la misión de la organización. Además, se determinan los recursos económicos y humanos necesarios para llevar a cabo la tarea.

Paso 7. Implementar plan de acción: la organización ejecuta las acciones definidas en el plan desarrollado en el punto anterior, y realiza una mejora en el plan de ciberseguridad actual para evitar la ocurrencia de los eventos conocidos.

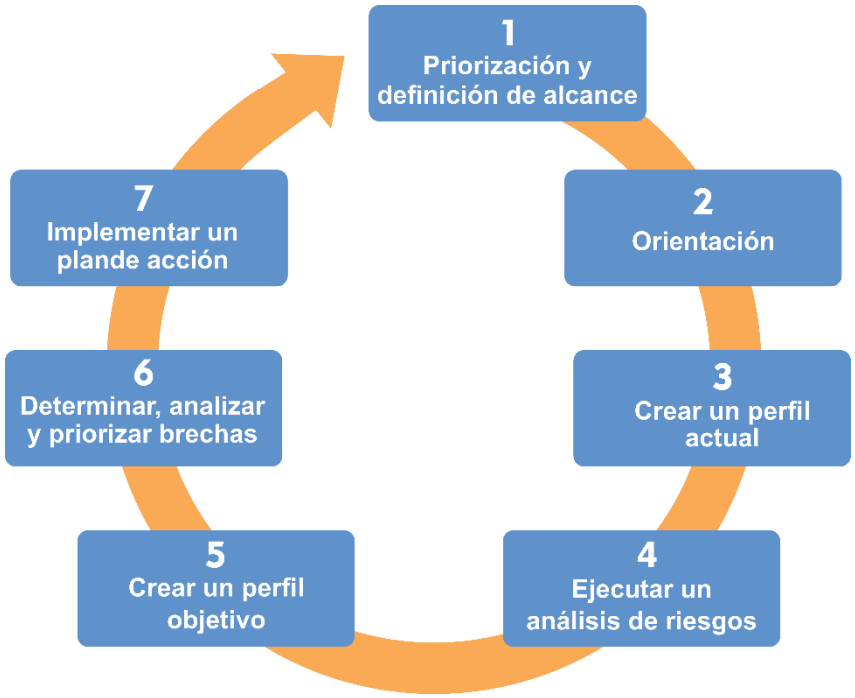

Figura 7. Representación propia, implementación del Marco de Trabajo NIST [22]

Proyección de implementación en una Organización Gubernamental

Habiendo hecho un análisis del marco de trabajo elaborado por el NIST, se realizará una propuesta posible de implementar en una Organización Gubernamental, a fin de resguardar las Infraestructuras Criticas de la Nación.

Al ser un marco iterativo, nos da la posibilidad de una mejora continua, controlando constantemente los procesos que se realizan en cada etapa.

Se ha elegido para efectuar el análisis de aplicabilidad la metodología del Ciclo de PDCA (acrónimo de las siglas Plan, Do, Check, Act siendo sus equivalentes a Planificar, Hacer, Verificar y Actuar) basado en el ciclo de Deming[4], debido a que es la base de todas las Normas como ser: ISO 9000 (Calidad), ISO 27000 (SGSI), etc.; con el fin de llevar a cabo un orden en el desarrollo del Proyecto. Dado que la misma contempla un ciclo de mejora continua, en el que se prioriza la planificación, pasando a la ejecución de lo planificado, se verifica si su ejecución es acorde a lo planificado y se realizan las correcciones necesarias para cumplir con la planificación retroalimentando el proceso mediante el control.

Lo que se propone es implementar en una primera instancia, el Nivel 1 Parcial (en el cual podrá haber varios ciclos de PDCA hasta encontrar el nivel de maduración necesario para poder pasar de Nivel), inicialmente se definirá el perfil actual de la Organización para luego determinar al perfil al que se desea llegar, confeccionando un proceso integral de gestión de riesgos cibernéticos, que abarque a las áreas de gobierno que manejan información sensible o que se encuentren dentro del alcance de infraestructuras críticas, factible de implementarse siendo este el primer paso para su logro, teniéndose en cuenta que los procesos de comunicación

[4] **William Edwards Deming** (14 de octubre de 1900-20 de diciembre de 1993) fue un estadístico estadounidense, profesor universitario, autor de textos, consultor y difusor del concepto de calidad total.

sean eficientes entre los distintos actores de la Organización, como así también, entre ellas.

El tiempo de implementación que llevará esto, deberá ser coherente con el tamaño de la Organización, como así también, en qué etapa de madurez se encuentra en lo que se refiere a la ciberseguridad y con los recursos que se cuenten.

PDCA en NIST

- **PLAN (Planificar):** en primera instancia se deberá realizar un relevamiento de ciberseguridad integral (el que incluya toda la infraestructura tecnológica del Organismo y los sistemas informáticos en uso, tanto los desarrollos internos como externos), con personal externo idóneo en la materia, que incluya la exposición que posee el Organismo con relación a la seguridad de la información ante una amenaza, lo que determinará el perfil actual de la institución, involucrando a las áreas tecnológicas, económicas y legales; lo que se busca es identificar los riesgos a los que la Organización se encuentra expuesta, evaluando su probabilidad de ocurrencia y su nivel de impacto.

  Se deberá clasificar la información en base a su nivel de criticidad, en criticidad baja, criticidad media y criticidad alta, esta clasificación deberá ser definida en base a su disponibilidad y confidencialidad.

  Se creará un Comité de Crisis que actúe ante la aparición de un ciberataque, con personal referente de las distintas áreas tecnológicas, quienes serán los interlocutores entre los distintos responsables de las áreas que manejan información sensible, con el fin de agilizar los canales de comunicación.

  Además, se deberán establecer canales eficientes y fluidos de comunicación entre las distintas áreas y niveles de la Organización, por los cuales deberán estar constantemente en contacto ante un hecho de esta magnitud. Estos canales se

deberán hacer extensivos hacia los Organismos con los que interactúen las áreas involucradas.

Se confeccionará un plan de accion con la finalidad de mitigar y controlar sus consecuencias, ante la ocurrencia de algún hecho de ciberseguridad, determinando de esta manera el perfil objetivo al que se desea llegar. Esto deberá estar alineado con la Política de Seguridad de la Información desarrollada por la Institución.

- **DO (Hacer):** se asignarán los recursos y responsabilidades a los actores que se involucran dentro del proceso de la ciberseguridad en la Organización.

  Se implementarán los procesos que dan soporte al plan de mejora determinado en función del relevamiento efectuado, que se alineen con lograr el perfil objetivo, estos podrán ser en un proceso determinado o en uno identificado crítico, ya que es de suma relevancia para el negocio.

  Se deberán definir y documentar los niveles de autorización dentro de cada unidad funcional, de modo que se pueda establecer que personal pueda acceder a cada activo de información, teniendo en cuenta el principio de mínimo privilegio.

  Se efectuarán boletines informativos, capacitaciones y jornadas de concientización, periódicas a todo el personal de la Organización, sin importar el nivel que tengan dentro de la misma.

  Se mantendrá una comunicación fluida y constante con referentes de la ciberseguridad, grupos de trabajos y proveedores de servicios a fin de obtener información actual del nivel global de la ciberseguridad.

  Se realizarán las actividades de gestión de riesgo de la seguridad de la información identificada como sensible o critica, acorde a su nivel de clasificación.

- **CHECK (Verificar):** transcurrido un tiempo prudencial, de efectuado lo del paso anterior, se deberá recopilar información y

reportes de control para efectuar un análisis exhaustivo, a fin de realizar una comparación de estos con los objetivos iniciales, observando que se hayan cumplido, emitiendo los reportes en el que se puedan observar el nivel de cumplimiento de la estrategia elegida.

Se implementarán los controles necesarios, de forma periódica, a fin de observar que se reflejan las directivas emitidas respecto a la seguridad de la información.

- **ACT (Actuar):** se tomarán las acciones necesarias para una mejora continua del plan efectuado, si se observan desviaciones de este contrastadas con las de las auditorías internas y externas, se deberá identificar el porqué de la desviación, para su corrección en la próxima iteración a realizarse. Esto facilitara la futura toma de decisiones en la gestión de los riesgos identificados.

Una manera de implementar esta metodología es utilizando los servicios en la nube ofrecidos por AWS[5], quien en sus procesos primarios y en toda su infraestructura interna, se encuentran alcanzados por la metodología desarrollada por el NIST, certificado por terceros quienes avalan esa implementación. Esta compañía ofrece planillas obligatorias de cumplimiento para la implementación de la seguridad en el proyecto, que son comprobadas y auditadas por personal certificado.

Para su implementación, este proceso debe hacerse de forma secuencial e iterativamente si es necesario, se debe analizar el cumplimento antes de avanzar de fase, esto, debe estar dentro de la cultura organizacional, ya que se deben involucrar a todos los niveles de esta, cada uno, tendrá una función distinta dentro de la planificación de la ciberseguridad debiéndolo asimilar, como así también, dentro del protocolo

[5] Amazon Web Services

de actuación para la mitigación de los riesgos de ciberseguridad identificados.

Cabe mencionar que el plan que he detallado tiene como función ser el disparador inicial para introducir al Organismo al marco de ciberseguridad propuesto por el NIST, siendo la primera iteración para ejecutarse, la cual se deberá cumplir en su totalidad para avanzar del Nivel 1 siendo el Inicial, según el ciclo iterativo incremental propuesto.

La implementación de los restantes niveles los que se observan en la figura 3, escapan al alcance del presente trabajo de investigación, ya que cada Organismo tiene una madurez determinada en lo que respecta a la ciberseguridad, quedando planteado como futuras posibilidades de estudio.

Conclusiones

En este trabajo final de especialización se trató de introducir al lector a la ciberseguridad, para lo cual, se han analizado los distintos marcos normativos, los cuales incluyen resoluciones y decretos emitidos por el Poder Ejecutivo de la República Argentina, en los que se demuestra claramente el interés por la temática de la ciberseguridad en los Organismos públicos que conforman las infraestructuras críticas del país.

Se pudo observar, las distintas motivaciones que poseen los atacantes mediante su clasificación, como así, las metodologías y/o herramientas que utilizan los mismos para perpetrar los ciberataques.

Se realizó un análisis del marco de ciberseguridad emitido por el NIST, pasando desde sus orígenes, el porqué de su creación y la necesidad del mismo, sus bases en otras normas y estándares, y un desarrollo exhaustivo de su estructura interna en el que se describió su núcleo, sus cuatro niveles y sus diferentes perfiles, enfocando los mismos en la problemática de la ciberseguridad, demostrando que el mismo nos permite descomponer los riesgos en acciones más pequeñas, las cuales se pueden atacar de manera iterativa.

Así mismo, se propuso una proyección de implementación del marco en su primer nivel, en un organismo gubernamental de alta sensibilidad como ser una fuerza de seguridad nacional.

Trabajos Futuros

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

- Iniciar contactos con Organismos internacionales y/o empresas del sector tecnológico del ámbito privado nacionales como internacionales, en los cuales se ha implementado con éxito el Marco del NIST.

- Crear una materia especifica dentro de los programas curriculares de los cursos de capacitación de los agentes de la Policía Federal Argentina.
- Enviar a ciertos recursos humanos calificados, a realizar capacitaciones en Instituciones referentes en la materia como ser: la OEA[6], la Universidad de Buenos Aires, el Ministerio de Modernización, etc.
- Confeccionar una base de conocimiento accesible por todos los Organismos Gubernamentales, en la cual poder buscar soluciones a problemas conocidos.
- Implementar el Marco de Ciberseguridad del NIST en la Policía Federal Argentina, utilizándola como caso testigo para futuras implementaciones.
- Mejorar los canales de comunicación entre todos los entes de gobierno, para compartir información sobre riesgos de ciberseguridad.
- Compartir recursos humanos calificados entre las distintas Organizaciones Gubernamentales.
- Confeccionar ejercicios periódicos en los que se simulen ciberataques a las infraestructuras críticas, a fin de observar cómo se comportan al respecto los referentes de cada área.
- Crear un área específica que se encargue de la ciberseguridad en los distintos Organismos Gubernamentales, teniendo como función: dictar la normativa específica, analizar los riesgos a los que se encuentra el Organismo, realizar auditorías informáticas e implementar las medidas para subsanar los riesgos identificados.

Por último, se puede mencionar que, con solo implementar el Marco de ciberseguridad, no alcanza, se debe trabajar diariamente para la mejora de los procesos que dan soporte al negocio, mejorar la comunicación entre

[6] Organización de los Estados Americanos

todos los niveles de la organización ante la ocurrencia de un suceso de ciberseguridad, no olvidando que es casi imposible tener un total control de la ciberseguridad, y determinar un proceso prestablecido actualizado para la mitigación de estos. Este plan, debe estar alineado con la visión, misión y objetivos de la organización, permitiendo de esta manera realizar una selección especifica de los procesos más riesgosos para el negocio, e invertir los recursos económicos y tecnológicos en ellos, para realizar una administración más eficiente.

Referencia Bibliográfica

[1] T. Jordan, Activism!: Direct Action, Hacktivism and the Future of Society, London: Reaktion Books Ltd, 2002.

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

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

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

[5] 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.

[6] 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.

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

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

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

[10] «Ciberseguridad,» 01 Agosto 2019. [En línea]. Available: https://www.akamai.com/es/es/resources/cyber-security.jsp.

[11] télam, «www.telam.com.ar,» 12 Agosto 2019. [En línea]. Available: http://www.telam.com.ar/notas/201908/383844-hackearon-la-cuenta-de-twitter-de-la-prefectura-naval-y-datos-secretos-de-la-policia.html. [Último acceso: 12 Agosto 2019].

[12] C. C. C. Nacional, «Ciberamenazas y tendencias 2019,» Ministerio de Defensa - Gobierno de España, 2019.

[13] 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].

[14] C. Anley, «Advanced SQL injection in SQL server applications,» 2002. [En línea]. Available: https://crypto.stanford.edu/cs155old/cs155-spring06/sql_injection.pdf. [Último acceso: 01 Agosto 2019].

[15] G. &. M. G. O'Gorman, Ransomware: A growing menace, Symantec Corporation, 2012.

[16] «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.

[17] «ISACA,» Information Systems Audit and Control Association, [En línea]. Available: http://www.isaca.org/COBIT/Pages/default.aspx.

[18] «CIS,» Center for Internet Security, [En línea]. Available: https://www.cisecurity.org/.

[19] «ISA,» The International Society of Automation, [En línea]. Available: https://www.isa.org/store/ansi/isa%E2%80%9362443-2-1-990201%E2%80%932009-security-for-industrial-automation-and-control-systems-establishing-an-industrial-automation-and-control-systems-security-program-/116731.

[20] «ISA,» The International Society of Automation, [En línea]. Available: https://www.isa.org/store/ansi/isa-62443-3-3-990303-2013-security-for-industrial-automation-and-control-systems-part-3-3-system-security-requirements-and-security-levels/116785.

[21] «ISO,» International Organization for Standardization, [En línea]. Available: https://www.iso.org/standard/54534.html.

[22] «NIST,» National Institute of Standards and Technology, [En línea]. Available: https://nvd.nist.gov/800-53/Rev4/.

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

Anexo

Identificadores únicos de funciones y categoría

Identificador único de función	Función	Identificador único de categoría	Categoría
ID	Identificar	ID.AM	Gestión de activos
		ID.BE	Entorno empresarial
		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 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 protectora
DE	Detectar	DE.AE	Anomalías y eventos
		DE.CM	Vigilancia continua 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
RC	Recuperar	RC.RP	Planificación de recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

Núcleo del Marco del NIST

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· **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-2: Software platforms and applications within the organization are inventoried	· **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: Organizational communication and data flows are mapped	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	· **CIS CSC** 12 · **COBIT 5** APO02.02, APO10.04, DSS01.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	· **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-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· **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
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	· **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	· **COBIT 5** APO02.06, APO03.01 · **ISO/IEC 27001:2013** Clause 4.1 · **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	· **COBIT 5** APO02.01, APO02.06, APO03.01 · **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 · **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	· **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.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	· **COBIT 5** BAI03.02, DSS04.02 · **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	· **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 controls from all security control families
		ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	· **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-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	· **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 controls from all security control families
		ID.GV-4: Governance and risk management processes address cybersecurity risks	· **COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · **ISO/IEC 27001:2013** Clause 6 · **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	· **CIS CSC** 4 · **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: Cyber threat intelligence is received from information sharing forums and sources	· **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-3: Threats, both internal and external, are identified and documented	· **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** Clause 6.1.2 · **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	· **CIS CSC** 4 · **COBIT 5** DSS04.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11

		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	· **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-6: Risk responses are identified and prioritized	· **CIS CSC** 4 · **COBIT 5** APO12.05, APO13.02 · **ISO/IEC 27001:2013** Clause 6.1.3 · **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	· **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** Clause 6.1.3, Clause 8.3, Clause 9.3 · **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	· **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.2.6.5 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 · **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	· **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 · **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	· **CIS CSC** 4 · **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009** 4.3.4.2 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	· **COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 · **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	· **COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 · **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 · **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	· **COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 · **ISA 62443-2-1:2009** 4.3.2.6.7 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	· **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 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	· **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-2: Physical access to assets is managed and protected	· **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-3: Remote access is managed	· **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-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	· **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-5: Network integrity is protected (e.g., network segregation, network segmentation)	· **CIS CSC** 9, 14, 15, 18 · **COBIT 5** DSS01.05, DSS05.02 · **ISA 62443-2-1:2009** 4.3.3.4 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8 · **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	· **CIS CSC**, 16 · **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 · **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3

			• **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-4:** Backups of information are conducted, maintained, and tested	• **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-5: Policy and regulations regarding the physical operating environment for organizational assets are met	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 • **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Data is destroyed according to policy	• **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-7: Protection processes are improved	• **COBIT 5** APO11.06, APO12.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 • **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared	• **COBIT 5** BAI08.04, DSS03.04 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	• **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-10: Response and recovery plans are tested	• **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-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	• **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-12: A vulnerability management plan is developed and implemented	• **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
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	• **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: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	• **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
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	• **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** AU Family
		PR.PT-2: Removable media is protected and its use restricted according to policy	• **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-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	• **CIS CSC** 3, 11, 14 • **COBIT 5** DSS05.02, DSS05.05, DSS06.06 • **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 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, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 • **ISO/IEC 27001:2013** A.9.1.2 • **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: Communications and control networks are protected	• **CIS CSC** 8, 12, 15 • **COBIT 5** DSS05.02, APO13.01 • **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 • **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 • **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	• **COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 • **ISA 62443-2-1:2009** 4.3.2.5.2 • **ISA 62443-3-3:2013** SR 7.1, SR 7.2 • **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 • **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
		DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	• **CIS CSC** 1, 4, 6, 12, 13, 15, 16 • **COBIT 5** DSS03.01 • **ISA 62443-2-1:2009** 4.4.3.3 • **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
			• **CIS CSC** 3, 6, 13, 15

DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	**DE.AE-2:** Detected events are analyzed to understand attack targets and methods	· **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-3: Event data are collected and correlated from multiple sources and sensors	· **CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 · **COBIT 5** BAI08.02 · **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-4: Impact of events is determined	· **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-5: Incident alert thresholds are established	· **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
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	· **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-2: The physical environment is monitored to detect potential cybersecurity events	· **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-3: Personnel activity is monitored to detect potential cybersecurity events	· **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-4: Malicious code is detected	· **CIS CSC** 4, 7, 8, 12 · **COBIT 5** DSS05.01 · **ISA 62443-2-1:2009** 4.3.4.3.8 · **ISA 62443-3-3:2013** SR 3.2 · **ISO/IEC 27001:2013** A.12.2.1 · **NIST SP 800-53 Rev. 4** SI-3, SI-8
		DE.CM-5: Unauthorized mobile code is detected	· **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-6: External service provider activity is monitored to detect potential cybersecurity events	· **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-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	· **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: Vulnerability scans are performed	· **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
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	· **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-2: Detection activities comply with all applicable requirements	· **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: Detection processes are tested	· **COBIT 5** APO13.02, DSS05.02 · **ISA 62443-2-1:2009** 4.4.3.2 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC 27001:2013** A.14.2.8 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: Event detection information is communicated	· **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-5: Detection processes are continuously improved	· **COBIT 5** APO11.06, APO12.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident	· **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.CO-1: Personnel know their roles and order of operations when a response is needed	· **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

RESPOND (RS)			· **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**RS.CO-2:** Incidents are reported consistent with established criteria	· **CIS CSC** 19 · **COBIT 5** DSS01.03 · **ISA 62443-2-1:2009** 4.3.4.5.5 · **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 · **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	· **CIS CSC** 19 · **COBIT 5** DSS03.04 · **ISA 62443-2-1:2009** 4.3.4.5.2 · **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	· **CIS CSC** 19 · **COBIT 5** DSS03.04 · **ISA 62443-2-1:2009** 4.3.4.5.5 · **ISO/IEC 27001:2013** Clause 7.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	· **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
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	· **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 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	· **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-3: Forensics are performed	· **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: Incidents are categorized consistent with response plans	· **CIS CSC** 19 · **COBIT 5** DSS02.02 · **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	· **CIS CSC** 4, 19 · **COBIT 5** EDM03.02, DSS05.07 · **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained	· **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-2: Incidents are mitigated	· **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: Newly identified vulnerabilities are mitigated or documented as accepted risks	· **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
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	· **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, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	· **COBIT 5** BAI01.13, DSS04.08 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident	· **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
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	· **COBIT 5** APO12.06, BAI05.07, DSS04.08 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	· **COBIT 5** APO12.06, BAI07.08 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed	· **COBIT 5** EDM03.02 · **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4
		RC.CO-2: Reputation is repaired after an incident	· **COBIT 5** MEA03.02 · **ISO/IEC 27001:2013** Clause 7.4
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	· **COBIT 5** APO12.06 · **ISO/IEC 27001:2013** Clause 7.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4