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

Maestría en Seguridad Informática

Tesis de Maestría

Ciberseguridad en Infraestructuras Críticas de Información

Autor/a:
Ing. Arsenio Antonio Aguirre Ponce
Tutor/a del Trabajo Final:
Mg. Patricia Prandini

Año de Presentación
2017

Cohorte del Cursante
2014

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y que 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

RESUMEN

El presente Trabajo Final de Maestría analiza la importancia de la ciberseguridad en las infraestructuras críticas de información, las actividades que se han desarrollado en este sentido de manera general en algunos países y el apoyo de las organizaciones internacionales que colaboran en el área de la ciberseguridad. Sobre esta base, propone un modelo para la identificación de los sectores y servicios críticos de una economía y una serie de controles mínimos para su protección.

En efecto, las tecnologías de la información se han esparcido rápidamente en todos los sectores de la sociedad y prácticamente no existen servicios críticos que no dependan de aplicaciones, bases de datos, servidores, redes de comunicaciones, centros de datos, etc.

La falta de controles de ciberseguridad ha ocasionado que algunos servicios se vean afectados a nivel mundial, como lo demuestran los incidentes de ciberseguridad que se describen en el presente trabajo y que impactaron en el funcionamiento de diferentes servicios críticos de tres países.

La mayoría de sectores que están utilizando tecnologías de información, proveen servicios importantes a la población. Sin embargo, debido a la falta de metodologías de clasificación de estos servicios, no se ha podido identificar cuáles son realmente críticos y que por lo tanto, cuáles requieren una protección acorde por parte de los operadores que los proveen.

Un aporte adicional del trabajo es el análisis del estado actual de la ciberseguridad en el Ecuador. En esta sección se analiza la situación de ese país, incluyendo las normativas y regulaciones que ha desarrollado para fortalecer la ciberseguridad en las empresas públicas y a nivel privado.

Palabras claves: ciberseguridad, riesgos, información.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1

INTRODUCCIÓN

El tema propuesto como Trabajo Final de Maestría fue escogido en base a la riesgosa combinación del notable incremento del uso de diversas tecnologías de la información para la provisión de servicios vitales de un país con la escasez de controles de ciberseguridad en las infraestructuras que soportan dichos servicios. En efecto, servicios esenciales tales como las telecomunicaciones o la energía, están utilizando masivamente tecnologías de la información debido a los grandes beneficios que esto acarrea, pero la gestión de la ciberseguridad es una debilidad, a la que se presta poca atención. Se propone en consiguiente, profundizar el estudio de la ciberseguridad, enfocándose en la identificación de servicios críticos y en la protección de las infraestructuras de información que contribuyen a su provisión.

1.1 IDENTIFICACIÓN DEL PROBLEMA

Los ataques que sufren hoy en día las tecnologías de la información que soportan los servicios vitales que sostienen la economía de un país y el bienestar de las personas, son cada vez más sofisticados. Estos ataques se han convertido en una gran preocupación para responsables y proveedores de dichos servicios. Debido a esto, los gobiernos de los países y las instituciones públicas y privadas deben estar preparados ante eventuales ataques o fallas cibernéticas y trabajar coordinadamente para evitar la interrupción de los servicios críticos para los ciudadanos.

Existen variados servicios vitales con infraestructuras físicas originalmente aisladas, que cada vez con mayor asiduidad se están interconectando a redes informáticas compartidas o públicas. Esto genera un mayor perímetro de ataque y facilita diferentes formas para una intrusión. Incluso algunas infraestructuras críticas se encuentran conectadas a Internet para su administración y monitoreo.

Algunos países de Latinoamérica ya están trabajando en políticas y estrategias nacionales de ciberseguridad. Sin embargo, considerando los avances y resultados de los países de la Unión Europea y de los Estados Unidos, Canadá, Australia o algunas naciones del Lejano Oriente, existe una brecha significativa en cuanto a su desarrollo que debe ser cubierta a corto plazo en la región. Latinoamérica no se encuentra exenta a los ciberataques, cuya frecuencia e impacto son cada vez mayores.

El desarrollo de una estrategia nacional de ciberseguridad implica enfrentar varias problemáticas, entre las cuales se encuentran: identificar los servicios críticos, definir mecanismos mínimos de protección y controles de ciberseguridad, determinar el nivel de inversión, crear conciencia en los ciudadanos, establecer cooperación entre instituciones públicas y privadas y con otros países, crear un marco legal y generar capacidades de respuesta a incidentes. Estas acciones tienen como finalidad asegurar proteger la información, en función de su criticidad, y asegurar la provisión de servicios sensibles y el funcionamiento de las infraestructuras críticas de un país. En consiguiente, una estrategia nacional de ciberseguridad debe ser formulada a través de un documento íntegro y conocido por todos los involucrados, adaptado al contexto y la realidad del país.

En este marco, el Trabajo Final de la Maestría apunta a cubrir una parte de esta problemática, para lo cual se determinarán y desarrollarán las principales actividades para la elaboración de una estrategia nacional de ciberseguridad, con especial énfasis en la identificación de los servicios críticos y de los controles necesarios para su protección. Adicionalmente se desarrollará un modelo para su aplicación específica en el campo de las infraestructuras críticas del Ecuador. El documento busca complementar los avances que actualmente está realizando ese país en el campo de la ciberseguridad.

1.2 OBJETIVOS

El Trabajo Final de Maestría plantea los siguientes objetivos, que serán cubiertos a lo largo del desarrollo del documento:

- Presentar y analizar estrategias nacionales de ciberseguridad que están aplicando algunos países avanzados en la materia y su relación con las infraestructuras críticas.
- Desarrollar los pasos para la elaboración de una estrategia nacional de ciberseguridad, que pueda servir de base para la construcción de una estrategia en el Ecuador.
- Desarrollar un marco de referencia que permita identificar servicios críticos de un país, aplicable al Ecuador.
- Definir los mecanismos y controles de seguridad más relevantes que los responsables o proveedores de servicios críticos deben implementar en las infraestructuras críticas, para protegerlas de las amenazas que pudieran afectarlas.

1.3 ALCANCE

El alcance del Trabajo Final de Maestría es específicamente la ciberseguridad en los servicios e infraestructuras críticas, por lo que se descarta analizar temas jurídicos vinculados a la protección de información, tales como el tratamiento del robo de información, los fraudes, etc. Se propone desarrollar las tareas que conforman una estrategia nacional de ciberseguridad, es decir una metodología que permita identificar los servicios críticos en el Ecuador y la definición de los controles de ciberseguridad mínimos a aplicar en infraestructuras críticas de información.

Se descarta asimismo, la revisión y el análisis de los aspectos jurídicos que se deben considerar en una estrategia nacional de ciberseguridad, los que serán sólo enumerados someramente. Queda también fuera del alcance del presente trabajo el establecimiento de un plan de implementación de los controles definidos para proteger las infraestructuras críticas, ya que esto

depende del plan de acción que se establezca en cada país y de los recursos con los que cuente.

1.4 HIPÓTESIS DEL TRABAJO

El Estado ecuatoriano y las instituciones que lo conforman tienen como parte de su responsabilidad: administrar, controlar y regular la prestación de diferentes servicios básicos a los ciudadanos. Muchos de estos servicios son claves para el correcto funcionamiento del Estado, para el desarrollo de la economía del país y para el bienestar de la población. Estas características los convierten en servicios críticos.

Dichos servicios se basan en infraestructuras tecnológicas, que en este marco, se convierten en críticas. Por lo tanto, deben ser protegidas en el mundo digital ante las amenazas internas o externas que se puedan materializar. En efecto, los servicios críticos que se brindan a los habitantes del Ecuador pueden verse afectados si una amenaza impacta una o varias instituciones proveedoras de estos servicios, independientemente de si son públicas o privadas. En consiguiente, sin la generación de una estrategia nacional que considere controles de ciberseguridad para gestionar los riesgos, las infraestructuras críticas pueden volverse vulnerables y al mismo tiempo, objetivos fáciles de los atacantes internos o externos.

Para reforzar los argumentos que justifican la necesidad de contar con una estrategia nacional de ciberseguridad, se plantean los siguientes cuestionamientos, que serán respondidos durante el desarrollo del presente Trabajo Final de Maestría:

- ¿Puede un país funcionar normalmente si una o varias de sus infraestructuras críticas son atacadas simultáneamente y no pueden brindar servicios a los ciudadanos?
- ¿Es posible establecer criterios para identificar los activos más relevantes de una infraestructura crítica?
- ¿Cuáles son los mecanismos de protección y los controles de ciberseguridad a implementar para proteger las infraestructuras críticas?

- ¿Cómo se puede proteger un país de las amenazas internas y externas de ciberseguridad que podrían afectar sus infraestructuras críticas?
- ¿Qué se requiere para que particularmente Ecuador elabore, implemente y monitoree adecuadamente un esquema nacional de ciberseguridad para prevenir amenazas internas y externas?
- Con referencia al mismo país, ¿qué parte de su infraestructura se encuentra en manos privadas y públicas? ¿Qué implica esto en términos de ciberseguridad nacional?

1.5 METODOLOGÍA Y PLAN DE ACTIVIDADES

Los objetivos establecidos para el presente Trabajo Final de Maestría se desarrollarán en cinco capítulos abarcando las siguientes actividades: introducción a la ciberseguridad en infraestructuras críticas, análisis de la situación actual en Ecuador, diseño de un marco de referencia para identificar activos críticos y definición de los controles de ciberseguridad.

El primer capítulo es la presente introducción del tema propuesto. El segundo consta de una sección de desarrollo teórico de la ciberseguridad en infraestructuras críticas, en la que se describen vulnerabilidades y amenazas. Se realiza además un resumen con los aspectos más importantes de algunas estrategias nacionales de ciberseguridad y se mencionan algunos ciberataques reales y de alto impacto ocurridos en los últimos años.

En el tercer capítulo se desarrolla un análisis de la situación actual de la ciberseguridad en infraestructuras críticas en el Ecuador. En esta fase el objetivo es presentar información de tipo pública sobre el tema, obtenida de diferentes sitios oficiales disponibles en Internet. Se agrega asimismo información relevada a partir de una serie de entrevistas e intercambio de información con un funcionario del Estado ecuatoriano, respecto a la situación actual del tema en el país.

En el cuarto capítulo se expondrá el diseño de un marco de referencia que permita identificar si un servicio es crítico. Para este objetivo, se realizará un relevamiento de los servicios que actualmente se prestan a los ciudadanos del Ecuador y se aplicará el modelo elaborado en el marco de referencia antes

referido. Por último, se definirán los controles de ciberseguridad sugeridos para las infraestructuras críticas del país que deberán implementar el gobierno y las instituciones responsables de la ciberseguridad en el Ecuador. Los controles se definirán en base a estándares y buenas prácticas de ciberseguridad, reconocidos y utilizados internacionalmente. El trabajo se cierra con las conclusiones y una serie de recomendaciones sobre el tema.

CAPÍTULO 2

CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS

En el presente capítulo se definen las infraestructuras críticas y se las clasifica de acuerdo a su prestación. Se describen las vulnerabilidades y diferentes amenazas que pueden afectarlas, se define el aporte de la ciberseguridad en su aseguramiento y se profundiza en la importancia de establecer una estrategia nacional de ciberseguridad. A fines ilustrativos, se describen algunos ciberataques que sufrieron infraestructuras críticas a nivel mundial, se menciona a las organizaciones internacionales que trabajan en temas de ciberseguridad para protegerlas y se finaliza describiendo brevemente las estrategias de ciberseguridad de algunos países.

2.1 DEFINICIÓN DE INFRAESTRUCTURAS CRÍTICAS [1]

Una infraestructura crítica de información (en adelante “infraestructuras críticas”) es el conjunto de activos tecnológicos indispensables, que interactúan entre sí para brindar servicios vitales a los habitantes de un país. Los activos pueden ser instalaciones físicas o virtuales, redes de datos, redes industriales, sistemas de información, bases de datos, sistemas de control industrial, procesos automatizados o cualquier otro componente tecnológico que permite la prestación o el monitoreo de un servicio esencial para el bienestar de la población y el sostenimiento de la economía de un país. La falta de controles de ciberseguridad para proteger estos activos origina un grave riesgo para una nación.

La realidad es que los activos no están exentos de sufrir un incidente de ciberseguridad debido al importante número de amenazas que existen en el ciberespacio. El impacto de un incidente puede afectar a diferentes sectores de un país como por ejemplo, el de la salud, la administración pública, el financiero, el de las telecomunicaciones o los proveedores de energía, entre

otros. En este contexto se debe tener en cuenta que los servicios vitales o críticos de un país están respaldados por infraestructuras críticas y que estas infraestructuras críticas están formadas por activos críticos que deben ser protegidos.

Las infraestructuras críticas pueden clasificarse de la siguiente manera, de acuerdo a su prestación:

- De servicio.- Las infraestructuras críticas de servicio proveen servicios vitales a un país y para ellas, la disponibilidad constituye la condición especial. La falta de disponibilidad genera un gran impacto en los ciudadanos. Las mayores amenazas que tienen este tipo de infraestructuras son: los ataques de denegación de servicio distribuidos y el malware que tiene por objetivo alterar el funcionamiento de los sistemas principales.

- De información.- Las infraestructuras críticas de información almacenan, procesan o transfieren información de tipo confidencial o sensible para su propietario. El propietario de la información puede ser una organización proveedora de servicios vitales, instituciones públicas o privadas o un ciudadano. La información es el activo crítico de estas infraestructuras y por lo tanto, se debe garantizar su confidencialidad, integridad y disponibilidad. Las mayores amenazas que tienen estas infraestructuras son: fraudes, robo de información confidencial y malware dedicado a secuestrar la información sensible.

Algunos de los servicios vitales que generalmente tienen activos con infraestructuras críticas son:

- Telecomunicaciones
- Energía
- Servicios financieros
- Transporte
- Comercio
- Agua

- Salud
- Seguridad
- Industria (alimentación, petróleo, etc.)

Las estrategias de ciberseguridad plantean, entre otros aspectos, la necesidad de identificar y clasificar los servicios críticos, para luego protegerlos adecuadamente frente a las amenazas. Actualmente las infraestructuras críticas en el campo industrial presentan dos clasificaciones de acuerdo a su arquitectura:

- Aisladas.- Son aquellas infraestructuras críticas que se encuentran organizadas en redes privadas de datos, sin interconexión con redes públicas ni con la red corporativa. Poseen software específico desarrollado para su funcionamiento y procesos complejos para su administración y monitoreo. En algunos casos no se pueden realizar tareas de administración de manera remota. Su mantenimiento es más costoso y realizar un proceso de actualización del software lleva un tiempo considerable. Estas infraestructuras abarcan generalmente solo un área local.

- Digitales.- Son aquellas infraestructuras que utilizan redes de datos privadas y públicas. Tienen sistemas de información y/o procesos automatizados mediante la implementación de *PLC*[1] *(Programmable Logic Controller).* La administración y monitoreo se realiza de manera remota utilizando redes *SCADA*[2] *(Supervisory Control And Data Acquisition).* Se encuentran conectadas a redes corporativas para el análisis de información en tiempo real y para toma de decisiones. Geográficamente estas redes pueden abarcar inmensos territorios.

[1] Se entiende por PLC al dispositivo diseñado para controlar procesos en ambientes industriales. [2]
[2] Se entiende por SCADA a una aplicación de software, diseñada con la finalidad de controlar y supervisar procesos a distancia. Se basa en la adquisición de datos de los procesos remotos. [3]

Dependiendo la legislación interna de un país y de su economía, las infraestructuras críticas pueden ser administradas solo por instituciones públicas o en proporciones variables, por organizaciones públicas y privadas. Sin embargo, en la mayoría de los casos, el Estado a través de las instituciones públicas es el responsable de supervisar y controlar a las instituciones que provean servicios críticos.

2.2 VULNERABILIDADES EN LAS INFRAESTRUCTURAS CRÍTICAS [4]

Las infraestructuras críticas utilizadas específicamente para el control industrial se caracterizaban en el pasado por estar organizadas en redes privadas y con programas dedicados exclusivamente para su funcionamiento. Por lo tanto, la seguridad no era una de las prioridades.

En ese contexto, la protección de estas infraestructuras se garantizaba sobre la base de dos aspectos:

- ✓ en función del software porque se trataba de sistemas propietarios y por lo tanto, el código fuente solo era conocido por los desarrolladores, y
- ✓ porque no tenían conexión con otras redes de datos, por lo cual las amenazas eran sólo locales y era más sencillo gestionarlas adecuadamente.

Debido al incremento en los costos de mantenimiento y la implementación de nuevas actualizaciones de software, así como por el surgimiento de Internet, estas infraestructuras fueron migrando al uso de nuevas tecnologías. Concretamente, con el pasar del tiempo los administradores de infraestructuras críticas comenzaron a reemplazar los sistemas propietarios que tuvieron inicialmente. En efecto, las instituciones públicas y privadas vieron como una oportunidad el hecho de poder contar con información en tiempo real para el análisis de datos y toma de decisiones. Esta posibilidad hizo que las redes de datos aisladas de sistemas industriales

se conectaran con las redes de datos corporativas, facilitándose el acceso remoto para la administración y el monitoreo. Además esta conexión habilitaba que la información de las redes industriales se pudiera compartir con otros sistemas de tipo corporativo, para procesar temas relacionados, como por ejemplo: el inventario, la contabilidad, la facturación, etc.

Como resultado de lo antes mencionado, se genera una evolución en los sistemas *SCADA,* que permiten administrar y monitorear sistemas de control o procesos industriales de manera remota, siempre existieron en el campo industrial pero en una arquitectura aislada. Sin embargo y como ya se explicó en párrafos anteriores, con el advenimiento de Internet comienzan a compartir información con sistemas corporativos, lo cual genera nuevos riesgos. Los sistemas *SCADA* usan *PLC* para la automatización de los diferentes procesos industriales. Por lo antedicho, inicialmente no existían modelos de seguridad para aplicarlos a estos sistemas y por lo tanto, la mayoría de las implementaciones en infraestructuras críticas, fueron realizadas sin considerar controles de ciberseguridad.

Esto llevó a que los sistemas SCADA actualmente en uso, sean menos seguros debido a que muchos emplean sistemas operativos y programas muy antiguos, que carecen de las últimas actualizaciones de seguridad y en la mayoría de casos, son difíciles de actualizar. Desde el punto de vista de seguridad, estas redes necesitan controles adicionales y compensatorios para su protección y para minimizar los riesgos a los que se exponen.

Hoy en día, la mayoría de redes SCADA se encuentran conectadas a redes públicas como Internet, la cual por naturaleza, no es una red segura aun cuando actualmente se la utilice en forma generalizada para aprovechar de sus beneficios. Sin embargo, debido a su naturaleza dual que combina notorias ventajas con mayores riesgos, estas redes de datos han acortado las distancias geográficas entre los atacantes y sus víctimas para realizar un ciberataque.

Frente a este panorama, algunos sectores con infraestructuras críticas como el financiero, el comercio y las telecomunicaciones, se encuentran

alcanzados por regulaciones locales en muchos países, que obligan a implementar políticas y controles de seguridad en los servicios que brindan.

Esta evolución en las infraestructuras críticas ha llevado a que grupos criminales organizados creen armas cibernéticas. Convertir los sistemas de información y programas en armas cibernéticas es el nuevo objetivo de los atacantes. Ya se ha demostrado que las armas cibernéticas se pueden infiltrar en los servicios vitales, afectar su disponibilidad e inclusive, destruirlos completamente.

Por lo tanto, el crecimiento exponencial de las nuevas tecnologías en las infraestructuras críticas genera un incremento también en las amenazas y vulnerabilidades. En este ámbito, cada día se lanzan ciberataques encubiertos con el objetivo de ganar accesos no autorizados y poder manipular su correcto funcionamiento, pudiendo afectar intereses vitales de un país.

Las infraestructuras críticas, especialmente en el sector industrial, están heredando las mismas amenazas y vulnerabilidades de los entornos de tecnologías de la información utilizadas a nivel corporativo. Gestionar correctamente dichas vulnerabilidades y minimizar los riesgos para los servicios críticos, aseguran el uso del ciberespacio por parte de los ciudadanos de un país y minimizan cualquier impacto sobre las economías.

Algunas de las vulnerabilidades que sufren las infraestructuras críticas son:

- Falta de un proceso de aplicación de parches de seguridad.
- Falta de políticas de contraseñas robustas.
- Uso de usuarios por defecto, genéricos o compartidos.
- Uso inadecuado de dispositivos móviles.
- Falta de políticas de acceso de terceros y proveedores a la red.
- Debilidad en la gestión de cambios.
- Conexiones no controladas con otras redes privadas y/ o públicas.
- Falta de una política de respaldo de datos y configuraciones.
- Falta de concienciación del personal en temas de ciberseguridad.
- Inexistencia de un proceso de gestión de incidentes.

- Inexistencia de un plan de continuidad de las operaciones.
- Carencia de profesionales con experiencia en ciberseguridad.
- Falta de entendimiento por parte de la gerencia de la trascendencia de la temática.

2.3 AMENAZAS EN LAS INFRAESTRUCTURAS CRÍTICAS [5]

La adopción de nuevas tecnologías sin considerar los debidos controles de ciberseguridad en las infraestructuras críticas, genera potencialmente nuevos vectores de amenazas, especialmente en los ambientes industriales porque se conectan redes seguras con entornos no seguros como Internet. Las amenazas buscan aprovechar una debilidad o ausencia de controles en los sistemas para explotar una vulnerabilidad.

A continuación podemos identificar algunas fuentes de amenazas:

- Estados extranjeros
- Crimen organizado
- Hacktivistas
- Delincuentes
- Organizaciones terroristas

Estas fuentes pueden originar, entre otros, los siguientes tipos de amenazas:

- Espionaje industrial
- Sabotaje
- Robo de datos
- Indisponibilidad del servicio
- Explotación de código malicioso
- Conflictos entre naciones

2.4 CIBERSEGURIDAD EN LAS INFRAESTRUCTURAS CRÍTICAS

Las infraestructuras críticas están evolucionando con el avance de la tecnología. En efecto, la mayoría están usando redes de datos de gran cobertura, sistemas de información y sistemas de control industrial por sus grandes beneficios, especialmente por sus menores costos, rápida implementación, flexibilidad frente a los cambios y por la posibilidad de su administración y monitoreo de manera remota. Incluso algunos administradores monitorean las infraestructuras críticas directamente a través de Internet.

La conexión de las redes de datos industriales con redes de datos extendidas y públicas, genera un vector de ataque para la proliferación de amenazas. La conexión de sistemas industriales con sistemas corporativos hace que la información y los sistemas necesariamente deban ser protegidos, ya que las redes de datos públicas como Internet, ampliamente utilizadas en las áreas corporativas, facilitan la intrusión y difusión de agentes externos potencialmente destructivos.

Los ciberataques que sufren hoy en día las infraestructuras críticas son cada vez más sofisticados y se han convertido en una gran preocupación para sus responsables y proveedores. Debido a esto, los países a través de instituciones públicas y privadas deben estar preparados para enfrentar a estos ciberataques. Además se necesita trabajar coordinadamente entre países y entre diferentes sectores, para evitar la interrupción de los servicios imprescindibles o críticos para los ciudadanos.

La ciberseguridad aplicada en las infraestructuras críticas permite reducir los riesgos sobre los activos críticos de una nación, mediante la aplicación de políticas, normas, procedimientos, herramientas y/o buenas prácticas de seguridad en el ciberespacio. De acuerdo a la ITU (Unión Internacional de las Telecomunicaciones), el término ciberespacio se utiliza para describir sistemas y servicios conectados directa o indirectamente a Internet o a redes de telecomunicaciones y datos. [6]

En este contexto, es posible afirmar que el proceso de adopción de nuevas tecnologías en infraestructuras críticas es irreversible. Por ello, se debe trabajar sobre el campo de la ciberseguridad para minimizar los riesgos a los que se exponen. Los gobiernos deben promover la creación de una estrategia de ciberseguridad para proteger la información y los servicios vitales de un país, y reconocer la importancia de la protección de las infraestructuras críticas de información.

2.5 CONCEPTO E IMPORTANCIA DE UNA ESTRATEGIA DE CIBERSEGURIDAD

La ciberseguridad puede ser considerada un campo nuevo en la seguridad de la información, que ha surgido con la interconexión de las redes de datos que permiten a los usuarios acceder a la información desde cualquier lugar del mundo. Esta interconexión ha generado lo que se llama ciberespacio o ciberentorno. Si bien, no existe a la fecha un acuerdo mundial para definir a la ciberseguridad, existen organizaciones que la han definido del siguiente modo:

- “La ciberseguridad es la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.” [7]
- "La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios, en el ciberentorno." [8]

Las empresas y los gobiernos tienen una alta preocupación sobre la ciberseguridad, especialmente porque cada día crecen las amenazas, al ritmo que también crecen áreas como: el comercio electrónico, distintas modalidades de comunicaciones a través de Internet, el gobierno digital, etc. En el ciberespacio, existe infinita cantidad de computadores, por lo cual es muy difícil sino imposible encontrar el origen de un ataque cibernético, tanto

para un gobierno, una organización o un usuario. Por otra parte, los países deben garantizar la tranquilidad y seguridad a los ciudadanos en el mundo digital.

Para luchar contra las amenazas cibernéticas, los gobiernos deben establecer a la ciberseguridad entre sus prioridades y desarrollar una estrategia nacional en la materia. Dicha estrategia tiene por objetivo proteger a las personas que utilizan el ciberespacio de distintos modos y mejorar la ciberseguridad de la información y de las infraestructuras críticas del país, mediante diferentes acciones. Se trata de un documento de alto nivel, generalmente público, que establece una serie de objetivos, lineamientos, políticas públicas y prioridades nacionales que deben lograrse para proteger adecuadamente el ciberespacio. En resumen, su objetivo es proporcionar un marco estratégico a nivel nacional para alinear sus acciones en temas de ciberseguridad.

Los principales puntos que cubre una estrategia de ciberseguridad sientan las bases para:

- Definir un marco de gobierno para la ciberseguridad.
- Establecer que la información sensible y/o confidencial debe ser clasificada.
- Definir instancias de cooperación entre instituciones públicas y privadas en temas de ciberseguridad.
- Sentar las bases para la identificación y protección de los servicios e infraestructuras críticas, incluyendo sus interdependencias, contribuyendo a un alto grado de resiliencia.
- Desarrollar planes nacionales de generación de capacidades de respuesta a ciberataques.
- Realizar ciberejercicios controlados con ciberataques a las infraestructuras críticas.
- Crear una cultura de ciberseguridad mediante la concientización de los ciudadanos.
- Generar Recursos Humanos con capacidades técnicas en temas de ciberseguridad.

- Contar con capacidad forense sobre amenazas persistentes avanzadas.
- Definir un marco normativo para la seguridad y particularmente, sobre la gestión de riesgos de ciberseguridad.
- Desarrollar nuevas tecnologías de ciberseguridad.
- Cooperar internacionalmente sobre temas de ciberseguridad, con el fin de contribuir al establecimiento de una política internacional para asegurar el ciberespacio.

Como ya se dijo, las infraestructuras críticas y la información vital de un país deben ser protegidas en el ciberespacio. Un ciberataque podría ser considerado como un atentado contra la soberanía de un país en el ciberespacio. La soberanía en el mundo digital y las nuevas tecnologías están cambiando inclusive, la estructura de las fuerzas militares en diferentes países.

En efecto, por ley los militares estaban dedicados a proteger la soberanía de un país en base a tres ámbitos: tierra, mar y espacio aéreo. En la actualidad, se suma un nuevo ámbito y es el mundo digital o ciberespacio. Debido a esto, en algunos países las estrategias de ciberseguridad son desarrolladas por profesionales que dependen de las fuerzas militares y se está creando comando conjunto de ciberdefensa. [9]

2.6 CIBERATAQUES A INFRAESTRUCTURAS CRÍTICAS [10]

Los ciberataques son los ataques realizados usando una computadora conectada a través de redes de datos o de Internet. También se los puede denominar: ataques informáticos o ataques cibernéticos. Los ciberataques pueden comprometer sitios web, robar o secuestrar información sensible, comprometer bases de datos o impedir el acceso a servicios en infraestructuras críticas, entre otros. En los últimos 10 años se ha visto un incremento notorio de los ciberataques sobre infraestructuras críticas.

Muchos de estos ataques han sido dirigidos contra infraestructuras críticas específicas y en la mayoría de los casos, no fue posible determinar su origen. Pero aún incluso conociendo el origen, no suelen existir acuerdos, protocolos o una legislación entre los distintos países para contrarrestar y eliminar la amenaza, en forma rápida y efectiva.

Algunas de las características de los ciberataques son:

- Relativamente bajo costo
- Ubicuidad
- Fácil ejecución
- Alta efectividad e impacto
- Reducido riesgo para el atacante

A continuación se describe en forma resumida, los casos de tres ciberataques que han sufrido diferentes servicios vitales de Estonia, Irán y Ucrania y que afectaron sus infraestructuras críticas. Las técnicas que se utilizaron en cada ciberataque fueron diferentes. En Estonia se utilizó un ciberataque de Denegación de Servicio Distribuido mediante el Internet, en Irán se usó un malware dedicado mediante la conexión de un dispositivo removible y en Ucrania, se propagó otro malware mediante un correo electrónico, usando una técnica de Ingeniería Social.

2.6.1 Estonia: Ciberataque de Denegación de Servicio Distribuido [11]

Estonia es desde hace ya varios años, uno de los países con mayor acceso a Internet a altas velocidades, que es considerado un derecho humano básico en ese país. Alrededor del 90% de toda la actividad bancaria se realiza por Internet y fue el primer país en votar a través de la gran red. Esto creó el campo propicio para que en el 2007 se enfrentara a un gran ciberataque que amenazó principalmente al gobierno, al sistema financiero y a los medios de comunicación.

Durante dicho año y por decisiones políticas se aprobó un plan para trasladar un importante monumento soviético de la Segunda Guerra Mundial

a una locación diferente, lo que provocó que varios ciudadanos rusos locales se sintieran disconformes.

El mismo día que el gobierno de Estonia trasladó el monumento soviético, el país comenzó inmediatamente a ser víctima de un gran ciberataque, las páginas gubernamentales comenzaron a colapsar y el acceso a los sistemas financieros por Internet fue bloqueado. Las noticias sobre este incidente no se propagaban porque los sitios de los medios de comunicación estaban también fuera de servicio. Ese día Estonia fue víctima de un ciberataque conocido como *DDoS (Distributed Denial of Service)*, es decir que desde algún lugar remoto, una red de computadoras estaban sobrecargando los servidores críticos de Estonia con una gran cantidad de solicitudes de servicio.

La herramienta utilizada para este ciberataque es conocida como *botnet,* definida como el conjunto de computadores que realizan tareas automáticas en base a instrucciones de una computadora central, conocido como centro de comando y control.

Estonia pasó así a enfrentarse con un ciberataque de gran magnitud en el mundo digital. El objetivo fue incomunicar a Estonia del resto del mundo y afectar a sus servicios. Fue la primera vez que se usó Internet como arma para colapsar el funcionamiento de un país en el ciberespacio. Este ciberataque pudo haber sido ocasionado por un grupo de hackers actuando de manera independiente o con el apoyo de un gobierno.

Estonia nunca tuvo claro quiénes fueron los responsables de los ciberataques. Este hecho fue considerado como un acto de ciberguerra porque perturbó la soberanía digital de un país. Aún después de lo ocurrido, no se han establecido claramente aún los protocolos para poder actuar, defenderse y contraatacar en una ciberguerra.

2.6.2 Irán: Ciberataque con malware *Stuxnet* [12]

En el año 2010, el gobierno de Irán confirmó su intención de seguir adelante con el programa nuclear de enriquecimiento de uranio que había iniciado. Anteriormente, los Estados Unidos y algunos países de la *OTAN* (Organización del Tratado del Atlántico Norte) habían expresado su disconformidad, considerando que dicho país estaba desarrollando una carrera armamentista en el campo nuclear.

El programa nuclear instalaba centrifugadoras de enriquecimiento de uranio que se encontraban por debajo de la superficie. Debido a esto, la probabilidad de un impacto con un ataque aéreo tenía menor posibilidad de ser exitosa. Por ese motivo se planeó y logró propagar un virus informático letal mediante una memoria *USB*. Alguien a quien no se pudo identificar conectó un dispositivo de este tipo en un computador de una planta de enriquecimiento de uranio y ayudó a propagar el virus, conocido como *Stuxnet*. El objetivo de este virus era afectar el programa nuclear de Irán.

Stuxnet se infiltró en las computadoras aprovechando vulnerabilidades de día *zero*, es decir vulnerabilidades que no son conocidas o reportadas hasta su descubrimiento y en consiguiente, no tienen actualizaciones de seguridad para su control y prevención. *Stuxnet* había sido desarrollado para buscar *PLC's* específicos relacionados a las centrifugadoras de enriquecimiento de uranio de marca *SIEMENS* y que casualmente, coincidían con los instalados en las plantas del programa nuclear de Irán.

El objetivo de Stuxnet era alterar la velocidad de giro de las centrifugadoras de enriquecimiento de uranio y así ir averiándolas de una en una. De ese modo se las dañaba de manera paulatina y no masivamente, para no levantar sospecha en los administradores de la infraestructura.

Después de algunos meses de detectar varias averías en las centrifugadoras y con ayuda de expertos nucleares e informáticos, los iraníes se dieron cuenta que estaban siendo víctimas de un ciberataque. Pero ya era tarde ya que *Stuxnet* destruyó el programa nuclear de Irán, al infectar los sistemas de enriquecimiento de uranio y dejar físicamente destruidas las centrifugadoras.

Stuxnet fue de algún modo, un arma cibernética perfecta, inteligente y generadora de una gran destrucción. El virus saltaba de una computadora a otra e iba verificando su tipo y el entorno en que trabajaba. El virus fue resultado del uso armamentístico de la programación y se considera que fue originado por una nación con muchos recursos económicos, computacionales y profesionales, ya que su desarrollo está fuera del alcance de un hacker promedio o aún, de un grupo organizado.

Estados Unidos e Israel negaron tener relación con *Stuxnet*. Ningún país se hizo responsable del ataque cibernético y dado lo complejo del virus, es muy probable que nunca se sepa quién estuvo detrás del ataque.

2.6.3 Ucrania: Ciberataque con malware *BlackEnergy* [13]

En diciembre del 2015 Ucrania sufrió un gran apagón de su sistema eléctrico. Un ciberataque coordinado afectó a las infraestructuras críticas, específicamente a las redes de suministro de energía eléctrica. Este ciberataque no fue un incidente aislado sino que impactó en más de una empresa del sector de distribución de energía. Se calcula que afectó alrededor de 600.000 hogares, que no tuvieron electricidad durante algunas horas.

Ucrania y Rusia mantenían en ese momento un conflicto político y el gobierno de Ucrania acusó a Rusia de generar el ciberataque. Esta acusación fue apoyada por profesionales dedicados a la ciberseguridad de los Estados Unidos que analizaron el incidente. Se realizaron entrevistas al personal de tecnologías de la información de las 6 empresas eléctricas afectadas. De acuerdo al historial de ciberataques, este sería el primer ciberataque contra una infraestructura crítica del sector eléctrico.

Los ciberdelincuentes utilizaron una familia de malware llamado *BlackEnergy*. El malware se propagó por un ataque de ingeniería social y usó la técnica llamada *spear phishing*, es decir, correos personalizados con objetivos específicos que tenían adjuntos de Microsoft Office, con código maliciosos.

Como antecedente, este malware ya había sido detectado por el gobierno de los Estados Unidos, cuando intentó infiltrarse en el sistema eléctrico norteamericano, sin registrar un impacto. El objetivo era desconectar las estaciones y subestaciones eléctricas mediante el acceso remoto a las instalaciones.

BlackEnergy fue usado como técnica de acceso inicial para adquirir información de los usuarios, que permitiera realizar conexiones de manera remota. El malware fue detectado en otros sectores con infraestructuras críticas, pero no afectó la operación de los servicios.

Adicionalmente a *BlackEnergy,* también se utilizó el programa de borrado *Killdisk,* que borró archivos importantes del sistema para impedir que se pudieran recuperar los sistemas de suministro de energía. Dicho sistema de energía quedó inutilizado.

El ciberataque fue sincronizado y coordinado por un grupo de hackers, que antes de lanzarlo hicieron una exploración y reconocimiento de la red de las infraestructuras críticas de las empresas proveedoras de energía. Según el personal, los ciberataques a cada empresa ocurrieron con 30 minutos de diferencia e impactaron múltiples estaciones centrales y regionales.

De manera similar a los casos citados anteriormente de Estonia e Irán, nunca se supo quiénes fueron los responsables de este ataque y nadie se atribuyó su autoría. Sin embargo, existen muchas sospechas de que lo pudo haber causado el propio gobierno ruso. Estos ejemplos muestran las dificultades de la atribución, cuando se trata de ataques cibernéticos.

2.6.4 Otros ciberataques a nivel mundial [14]

Algunos países también alertaron a sus centros de respuestas de incidentes, conocidos como CERTs o CSIRTs por sus siglas en inglés, sobre ciberataques que comprometieron sus infraestructuras críticas. De acuerdo a noticias periodísticas, en la mayoría de los casos tampoco se pudo detectar los orígenes. Esto demuestra que las distancias se han reducido y que por

diversos motivos, los grupos criminales organizados están realizando ciberataques. Adicionalmente y como ya se mencionó, las vulnerabilidades presentes en las infraestructuras críticas permiten una fácil ejecución de un ciberataque.

A continuación se mencionan otros casos de ciberataques a nivel mundial:

- Turquía en 2008: Ciberatacantes se infiltraron en sistemas industriales e hicieron explotar tuberías de petróleo.
- Georgia en 2008: Ciberdelincuentes accedieron a redes de datos y cambiaron imágenes de diferentes sitios web del gobierno.
- Israel en 2009: Se registraron ciberataques a sitios gubernamentales mediante el Internet.
- Canadá en 2011: Se registraron ciberataques contra algunas agencias del gobierno que ocasionaron se desconectaran temporalmente de Internet.
- Estados Unidos 2011: Se registró un ciberataque a un proveedor del Departamento de Defensa, que permitió el robo de 24.000 documentos de ese departamento.

Adicionalmente a los mencionados precedentemente, se registraron ciberataques sobre instituciones privadas, especialmente de comercio en línea, que comprometieron información confidencial de los clientes.

A nivel de Latinoamérica no existen reportes fidedignos sobre ciberataques a las infraestructuras críticas. Sin embargo, no por ello se puede confirmar que no hayan existido. Pudieron registrarse casos aislados que no tuvieron repercusión nacional o que no fueron reportados por falta de conocimiento o para no causar temor en la ciudadanía. En este contexto, se genera una oportunidad entre las naciones u organizaciones de la región para crear instancias de colaboración, coordinación y cooperación sobre la ciberseguridad.

En cambio, diferentes países Latinoamericanos han sufrido ciberataques que han comprometido la privacidad y confidencialidad de la información. Estos ciberataques incluso afectaron a algunos países de Europa. A través de filtraciones de información realizados por expertos y trascendidos periodísticos, se pudo confirmar que Estados Unidos a través de sus agencias de servicio secreto estuvo espiando los correos y llamadas telefónicas de los presidentes o autoridades gubernamentales de Latinoamérica y Europa.

Políticamente los países afectados quedaron expuestos en temas de ciberseguridad. Por este motivo muchos de ellos decidieron desarrollar sus estrategias de ciberseguridad para proteger la información confidencial y las infraestructuras críticas. Un rol importante de estas estrategias es desarrollar protocolos para contraatacar un ciberataque y contar con la cooperación entre países y organizaciones que trabajan en ciberseguridad.

2.7 CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS: PANORAMA INTERNACIONAL

Como ya se mencionó, la ciberseguridad en las infraestructuras críticas es una gran preocupación y ocupa un lugar prioritario en la agenda de trabajo de numerosos países y organizaciones internacionales, especialmente en Europa, Estados Unidos y Canadá. La mayoría de estos países ya se encuentra trabajando en un plan de acción, como parte de la implementación de las estrategias nacionales de protección de sus infraestructuras críticas.

2.7.1 Aportes de organizaciones que trabajan en el tema

Varias naciones están protegiendo sus infraestructuras críticas en base a los objetivos y al plan de acción descripto en la estrategia nacional de ciberseguridad. Las organizaciones internacionales juegan un rol importante en esta actividad porque pueden fijar lineamiento y colaborar y asesorar a los países sobre la implementación de dichas estrategias.

A continuación citamos diferentes organizaciones que han desarrollado documentación, publicaciones o normas, desarrollado eventos, etc., para la construcción de estrategias de ciberseguridad y protección de infraestructuras críticas.

2.7.1.1 *ENISA (European Network and Information Security Agency)* [15]

ENISA, que en español significa Agencia Europea de Seguridad de las Redes y de la Información, trabaja para los Estados Miembros de la Unión Europea. Es la entidad responsable de dicho bloque en temas de ciberseguridad. Su objetivo es facilitar que sus Estados Miembros intercambien información, mejores prácticas y conocimiento en el campo de seguridad de la información.

ENISA busca también concientizar en temas de ciberseguridad a los ciudadanos, clientes, negocios y organizaciones del sector público. Ayuda a prevenir problemas de seguridad de la información y a desarrollar una legislación comunitaria en el ámbito de la ciberseguridad. La entidad trabaja sobre muchos sectores dedicados a la seguridad de la información, y cuenta con profesionales expertos que investigan y desarrollan documentación, entre otras, en las siguientes temáticas:

- Seguridad en la nube
- Seguridad en Big Data
- Infraestructuras Críticas de Información
- Gestión de incidentes de seguridad
- Educación y concienciación en ciberseguridad
- Privacidad y protección de datos
- Estrategias Nacionales de Ciberseguridad
- Entrenamiento para especialistas en ciberseguridad
- Gestión de amenazas y riesgos en ciberseguridad

ENISA ha trabajado en analizar el estado de situación en materia de ciberseguridad de cada uno de los Estados Miembros de la Unión Europea.

Con su aporte, veinte países europeos ya cuentan con estrategias de ciberseguridad y actualmente se encuentran en la fase de implementación.

Los documentos más relevantes que desarrolló ENISA y que contribuyen a la ciberseguridad de las infraestructuras críticas y a las estrategias de los Estados Miembros son:

- Estrategia Nacional de Ciberseguridad: Una guía de implementación
- Marco de evaluación de una Estrategia Nacional de Ciberseguridad
- Metodología para la identificación de activos de Infraestructuras Críticas de Información.
- Protegiendo los Sistemas de Control Industrial
- Plan de cooperación ante una cibercrisis
- Ejercicios de cibercrisis

2.7.1.2 *NIST (National Institute of Standards and Technology)* [16]

En español NIST significa Instituto Nacional de Normas y Tecnología. Se trata de la Agencia Federal del Departamento de Comercio de los Estados Unidos, cuya misión es promover la innovación y la competitividad industrial de los Estados Unidos mediante el desarrollo de la ciencia de la medición, normas y tecnología, para mejorar la seguridad económica y la calidad de vida de los estadounidenses. Su accionar parte de la base de que la seguridad nacional y económica de los Estados Unidos depende del funcionamiento seguro de sus infraestructuras críticas. Organizacionalmente, el NIST se encuentra dividido en diferentes laboratorios que trabajan en áreas diversas, entre las cuales se encuentran la de las Tecnologías de la Información.

En dicho laboratorio existe una división específica para trabajar en temas de ciberseguridad, que provee normas y tecnologías para proteger los sistemas y servicios de información contra amenazas a su confidencialidad, integridad y disponibilidad. Esta dependencia provee publicaciones especiales en temas de ciberseguridad bajo la serie SP 800 y SP 1800. La primera está conformada por guías, recomendaciones y material de referencia

sobre ciberseguridad. La segunda es una nueva serie de publicaciones creadas a partir de la serie SP 800, que se enfoca en los nuevos desafíos de ciberseguridad, específicamente en los sectores público y privado.

En el año 2013 la división de ciberseguridad publicó el documento SP 800 - 53 Rev. 4 “Controles de seguridad y privacidad para las Organizaciones y Sistemas Federales de Información”. El documento provee una guía para la implementación de controles mínimos de seguridad de la información para proteger las operaciones, activos e individuos de todas las organizaciones y a los Estados Unidos de un conjunto de amenazas. Las amenazas incluyen: ciberataques, desastres naturales, fallos estructurales y errores humanos, y son de aplicación obligatoria a todas las dependencias del gobierno y a las infraestructuras críticas.

Como resultado de la publicación del SP 800 - 53 Rev. 4, la división de ciberseguridad elaboró un marco para mejorar la ciberseguridad de las infraestructuras críticas. El objetivo de dicho marco es mejorar su ciberseguridad y resiliencia con el objetivo de mantener un ciberespacio seguro.

2.7.1.3 *LACNIC (Latin America & Caribbean Network Information Centre)* [17]

LACNIC, el Registro de Direcciones de Internet para América Latina y el Caribe, es una organización no gubernamental internacional establecida en Uruguay en el año 2002. Es responsable de la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), y de los Números Autónomos y Resolución Inversa, entre otros recursos, para la región. Es uno de los 5 Registros Regionales de Internet del mundo.

LACNIC contribuye al desarrollo de Internet en la región mediante una política activa de cooperación, promoviendo y defendiendo los intereses de la comunidad regional y colaborando en generar las condiciones para que Internet sea un instrumento efectivo de inclusión social y desarrollo económico para todos los países y ciudadanos de América Latina y el Caribe.

La organización se encuentra trabajando en temas de ciberseguridad desde hace varios años, con el objetivo de tener un ciberespacio seguro. Considerando que la mayoría de las infraestructuras críticas usan Internet, LACNIC apunta a la construcción de una Red abierta, estable y segura, al servicio del desarrollo económico, social y cultural de América Latina y el Caribe.

Para cumplir tal fin, genera documentación, publicaciones y eventos sobre tecnologías de la información y ciberseguridad. Actualmente se encuentra trabajando en el proyecto AMPARO, con el objetivo de fortalecer la Capacidad Regional en Ciberseguridad. Gracias a su accionar se han desarrollado numerosos grupos de respuesta a incidentes en la región.

Este proyecto propone además fortalecer la difusión, conocimiento y atención de la problemática de ciberseguridad en los países latinoamericanos, fundamentalmente en el ámbito privado de las empresas y organizaciones sociales. El enfoque principal es promover la difusión y capacitación en ciberseguridad, aunque también ha desarrollado algunas actividades de investigación en la materia.

2.7.1.4 *OEA* (Organización de Estados Americanos) [18]

La Organización de Estados Americanos ha desarrollado una iniciativa muy robusta, a través de la cual se asesora en temas de ciberseguridad a los Estados Miembros del continente americano, especialmente a países de Latinoamérica. Cuenta con un grupo de profesionales que genera información, publicaciones, eventos, etc, sobre la temática. El trabajo que realiza la OEA se orienta a que los gobiernos de Latinoamérica incorporen en sus agendas de trabajo el desarrollo de estrategias de ciberseguridad y específicamente, la protección de las infraestructuras críticas.

La OEA reconoce que la responsabilidad nacional y regional para la ciberseguridad cae sobre una amplia gama de instituciones, tanto del sector público como el privado. Estas instituciones deben trabajar en aspectos políticos y técnicos para asegurar el ciberespacio.

Entre los principales objetivos de grupo de ciberseguridad de la OEA se encuentran:

- Establecer grupos nacionales de "alerta, vigilancia y prevención", conocidos como Equipos de Respuesta a Incidentes (CSIRT Nacionales) en cada país.
- Crear una red para proporcionar formación técnica al personal que trabaja en ciberseguridad en los gobiernos de las Américas.
- Promover el desarrollo de Estrategias Nacionales de Ciberseguridad.
- Fomentar el desarrollo de una cultura que permita el fortalecimiento de la ciberseguridad en los Estados Miembros.

Mediante la Resolución AG/RES (XXXIV-O/04), la OEA estableció una estrategia integral para combatir las amenazas a la ciberseguridad con base en un enfoque multidimensional y multidisciplinario para la creación de una cultura de ciberseguridad. Esta estrategia estipula tres vías de acción con sus responsables [19]:

- Creación de una Red Hemisférica de Equipos Nacionales de Respuesta a Incidentes de Seguridad de Computadores - CSIRT. Este cometido fue asignado al Comité Interamericano Contra el Terrorismo - CICTE.
- Identificación y adopción de normas técnicas para una arquitectura segura de Internet. Esta labor es desarrollada por la Comisión Interamericana de Telecomunicaciones - CITEL.
- Adopción y/o adecuación de los instrumentos jurídicos necesarios para proteger a los usuarios de Internet y las redes de información frente a delincuentes y grupos delictivos organizados que utilizan estos medios, a cargo de las Reuniones de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas - REMJA.

2.7.1.5 *UIT* (Unión Internacional de Telecomunicaciones) [20]

La UIT es el organismo especializado de las Naciones Unidas para el desarrollo de las Tecnologías de la Información y Comunicación - TIC. Elaboran normas técnicas que garantizan la interconexión continua de redes y las diferentes tecnologías asociadas. Esta organización está comprometida en desarrollar normas que conecten a toda la población mundial, dondequiera que viva y a través de cualquier medio que disponga.

La UIT organizacionalmente está compuesta por diferentes sectores de trabajo y tiene una división específica dedicada a la ciberseguridad. Esta división refleja un papel fundamental del UIT, en base a la orientación de la Cumbre Mundial sobre la Sociedad de la Información, dirigido a la construcción de confianza y seguridad en el uso de las Tecnologías de la Información. En este marco, durante el año 2007 lanzó la Agenda sobre Ciberseguridad Global (ACG), como un marco para la cooperación internacional en ciberseguridad.

La Agenda sobre Ciberseguridad Global se basa en los siguientes cinco pilares estratégicos:

- Medidas legales
- Medidas técnicas y de procedimientos
- Estructura organizacional
- Capacidad de las infraestructuras
- Cooperación internacional

En el 2009 la UIT desarrolló una herramienta para realizar una autoevaluación de la ciberseguridad nacional y la protección a las infraestructuras críticas de información (CIIP). Esta herramienta estaba dirigida a los Estados Miembros para examinar los temas relacionados a políticas, normas, instituciones y relaciones sobre la ciberseguridad y la protección a las infraestructuras críticas de información, y asistirlos en la creación de una estrategia nacional de ciberseguridad. La herramienta considera los siguientes ítems como parte de dicha estrategia:

- Identificar una política nacional en ciberseguridad.

- Identificar las agencias y organizaciones claves del gobierno con responsabilidades de liderazgo en ciberseguridad y describir sus roles.
- Identificar las estructuras organizacionales que se usarán para el desarrollo de la política de ciberseguridad.
- Identificar las estructuras organizacionales a las que se le asignarán las tareas vinculadas a las operaciones de ciberseguridad.
- Identificar los objetivos y estructuras organizacionales para la colaboración entre el gobierno y el sector privado.
- Identificar la ubicación dentro del gobierno de la función de gestión de incidentes.
- Identificar objetivos para la actualización del marco legal relacionado con los delitos informáticos.
- Identificar y priorizar objetivos para construir una cultura nacional de ciberseguridad.
- Revisar los requisitos y las fuentes de financiación para cada elemento de la estrategia nacional.
- Identificar los plazos de ejecución.
- Identificar las métricas y objetivos de re-evaluación.

Actualmente, esta organización internacional se encuentra desarrollando una nueva versión del documento, en colaboración con organizaciones como: ENISA, Universidad de Oxford, Microsoft, *OTAN*, *CCDCOE (Cooperative Cyber Defence Centre of Excellence)*, la OEA y el Banco Mundial, entre otros. La UIT cuenta con un repositorio en línea sobre las estrategias nacionales de ciberseguridad de 72 países, de un total de 193 Estados Miembros.

2.7.1.6 *APEC (Asia-Pacific Economic Cooperation)* [21]

La Cooperación Económica Asia-Pacífico (APEC) es un foro económico regional establecido en 1989 para aprovechar la creciente

interdependencia de la región de Asia y el Pacífico. APEC está formada por veintiún Estados Miembros que tienen como objetivo crear una mayor prosperidad para los pueblos de la región mediante la promoción de un crecimiento equilibrado, inclusivo, sostenible, innovador y seguro y mediante la aceleración de la integración económica regional.

APEC tiene un grupo de trabajo en Telecomunicaciones e Información, que tiene como objetivo mejorar las infraestructuras de las telecomunicaciones y la información en la región. Para cumplir su función, desarrolla e implementa políticas de telecomunicaciones y de información y realiza eventos. Algunos de sus enfoques para el tema son: protección de la información, infraestructura de comunicaciones y ciberseguridad.

El grupo de trabajo propone, implementa y monitorea proyectos y actividades para cumplir con las metas de APEC.

Algunos de los proyectos de ciberseguridad elaborados son:

- Estrategia de Ciberseguridad de APEC
- Principios para autenticación electrónica basada en una *PKI.*
- Principios de APEC contra el SPAM
- Estrategia para asegurar el entorno on-line (ciberespacio).
- Aspectos de ciberseguridad para infraestructuras críticas

2.8 ESTRATEGIAS DE CIBERSEGURIDAD

La primera estrategia de ciberseguridad fue publicada por los Estados Unidos en el 2003. Fue parte de una estrategia nacional de seguridad como consecuencia de los atentados terroristas en septiembre del 2001. En el 2005 Alemania adoptó el “Plan Nacional para la Protección de Infraestructuras de Información”. En el 2006 Suecia desarrolló una “Estrategia para mejorar la seguridad en internet en Suecia”. Debido a los fuertes ciberataques que sufrió Estonia en el 2007, el país fue el primer miembro de la Unión Europea que publicó una extensa estrategia nacional de ciberseguridad en el 2008. Desde

entonces algunos países han realizado esfuerzos considerables para publicar una estrategia nacional de ciberseguridad.

España junto a la ya mencionada Estonia, son dos de los países que más desarrolladas tienen sus estrategias de ciberseguridad. Estos gobiernos han tomado en serio el tema de la ciberseguridad en sus agendas. A nivel estratégico y operacional cuentan con las capacidades y conocimientos para gestionar los riesgos de una ciberamenaza.

Algunos países de Latinoamérica ya se encuentran trabajando en la elaboración de políticas y estrategias nacionales de ciberseguridad, como son los casos de Colombia, Chile y Costa Rica. Colombia en particular publicó un documento con lineamientos para establecer una estrategia de ciberseguridad.

Sin embargo, considerando los avances y resultados de los países miembros de la Unión Europea y Estados Unidos, existe una brecha significativa debido a que estos países ya se encuentran en la implementación de sus estrategias de ciberseguridad y están preparados para gestionar un ciberataque. La brecha debe ser cubierta a corto plazo por los países de Latinoamérica porque el rol de las tecnologías de información en los servicios críticos se está incrementando en la región.

A continuación se desarrollarán los aspectos más importantes de las estrategias de ciberseguridad de España, Estonia y Colombia. Esta información fue encontrada en sitios oficiales de ciberseguridad que tienen publicadas todas las estrategias de ciberseguridad a nivel mundial.

2.8.1 España [22]

El Consejo de Seguridad Nacional impulsó la elaboración de la Estrategia de Ciberseguridad Nacional, con el fin de brindar respuesta al gran desafío de proteger el ciberespacio de los riesgos y amenazas a los que se encuentra expuesto. Esta Estrategia de Ciberseguridad forma parte de la Estrategia de Seguridad Nacional de España y señala que asegurar el

ciberespacio contribuye a incrementar el potencial económico, porque promueve un ciberespacio más seguro para la inversión, la generación de empleo y la competitividad.

España mediante la estrategia de ciberseguridad se compromete a desarrollar políticas que mejoren la seguridad de los Sistemas de Información y Telecomunicaciones que emplean los ciudadanos, las administraciones públicas, los profesionales y las empresas, preservando los derechos fundamentales consagrados en la Constitución y en instrumentos internacionales, tales como: la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos o el Convenio Europeo para la protección de los Derechos Humanos y las Libertades Fundamentales.

- **Objetivos de la ciberseguridad**

Objetivo General

- Lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques.

Objetivos específicos

- Garantizar que los Sistemas de Información y Telecomunicaciones que utilizan las Administraciones Públicas poseen el adecuado nivel de ciberseguridad y resiliencia.
- Impulsar la seguridad y resiliencia de los Sistemas de Información y Telecomunicaciones usados por el sector empresarial en general y los operadores de Infraestructuras Críticas en particular.
- Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades de terrorismo y la delincuencia en el ciberespacio.
- Sensibilizar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio.

- Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad.
- Contribuir a la mejora de la ciberseguridad en el ámbito internacional.

Líneas de acción de la ciberseguridad nacional

- Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas.

  Incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las ciberamenazas, haciendo énfasis en las Administraciones Públicas, las Infraestructuras Críticas, las capacidades militares y de Defensa y otros sistemas de interés nacional.
- Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas.

  Garantizar la implantación del Esquema Nacional de Seguridad, reforzar las capacidades de detección y mejorar la defensa de los sistemas clasificados.
- Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas.

  Impulsar la implantación de la normativa sobre Protección de Infraestructuras Críticas y de las capacidades necesarias para la protección de los servicios esenciales.
- Capacidad de investigación y persecución del ciberterrorismo y ciberdelincuencia.

  Potenciar las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio, sobre la base de un marco jurídico y operativo eficaz.
- Seguridad y resiliencia de las TIC en el Sector Privado.

  Impulsar la seguridad y la resiliencia de las infraestructuras, redes, productos y servicios empleando instrumentos de cooperación público-privada.

- Conocimientos, Competencias e I+D+i (Investigación, desarrollo e innovación).

  Promover la capacitación de profesionales, impulsar el desarrollo industrial y reforzar el sistema de I+D+i en materia de ciberseguridad
- Cultura de ciberseguridad

  Concienciar a los ciudadanos, profesionales y empresas de la importancia de la ciberseguridad y del uso responsable de las nuevas tecnologías y de los servicios de la Sociedad de la Información.
- Compromiso Internacional

  Promover un ciberespacio internacional seguro y confiable, en apoyo a los intereses nacionales.

- **La Ciberseguridad en el Sistema de Seguridad Nacional**

Define la estructura orgánica para cumplir con los principios que sustentan el Sistema de Seguridad Nacional. Esta estructura se encuentra bajo la dirección del Presidente de Gobierno español. Los componentes de la estructura son los siguientes:

- Consejo de Seguridad Nacional
- Comité Especializado de Ciberseguridad
- Comité Especializado de Situación

España como parte de su estrategia de ciberseguridad, tiene un centro de mando para ciberguerra. Este centro es administrado por el alto mando militar y controla todas las plataformas de telecomunicaciones del ejército. Si se realiza un ciberataque, dicha fuerza despliega un programa militar contra las amenazas, riesgos y vulnerabilidades que se vayan presentando en los distintos sistemas que están en operación. El ejército dispone de una red propia desconectada del Internet. Como aporte a la ciberseguridad en infraestructuras críticas, España ya cuenta con legislación referente del más alto nivel para la protección de dichas infraestructuras y ha desarrollado una serie de documentos referidos a la seguridad de sistemas SCADA.

2.8.2 Estonia [23]

La estrategia de ciberseguridad es el documento básico para la planificación de la ciberseguridad en Estonia y forma parte de la estrategia nacional de seguridad. El documento destaca los últimos acontecimientos importantes, evalúa las amenazas a la ciberseguridad de Estonia y presenta medidas para gestionar las amenazas.

Organizacionalmente, el país tiene varias agencias trabajando en temas como la cooperación entre el sector público y privado, la protección de infraestructuras críticas de información, los servicios de evidencia digital, la persecución a la ciberdelincuencia y la capacitación relacionada a la protección frente a ciberamenazas, entre otros.

En este sentido, establece que las crecientes amenazas a la ciberseguridad deben ser revisadas al considerar el papel importante que las tecnologías de la información y las comunicaciones tendrán en el futuro, impulsando el crecimiento de las economías y las sociedades. Mediante su estrategia de ciberseguridad, Estonia tiene identificados los servicios vitales y los requerimientos de seguridad que deben aplicarse. A continuación revisamos los temas más importantes de la estrategia de ciberseguridad de Estonia:

Principios para garantizar la ciberseguridad

- La ciberseguridad es una parte integral de la seguridad nacional, ayuda al funcionamiento del Estado y la sociedad, a aumentar la competitividad de la economía y a desarrollar la innovación.
- La ciberseguridad es garantizada mediante el respeto de los derechos y las libertades fundamentales, así como mediante la protección de las libertades individuales, información personal y su identidad.
- La ciberseguridad es afianzada sobre la base del principio de proporcionalidad, teniendo en cuenta riesgos y recursos existentes y potenciales.

- La ciberseguridad es garantizada de manera coordinada a través de la cooperación entre los sectores público y privado y con el denominado “tercer sector”, teniendo en cuenta la interconexión e interdependencia de la infraestructura y los servicios existentes en el ciberespacio.
- La ciberseguridad se basa primariamente en la responsabilidad individual para el uso seguro de las herramientas de tecnologías de la información y comunicación.
- Una de las principales prioridades para garantizar la ciberseguridad es anticipando y previniendo las potenciales amenazas y respondiendo eficazmente a las amenazas que se materializan.
- La ciberseguridad es apoyada por la investigación y desarrollo.
- La ciberseguridad es garantizada a través de la cooperación internacional con aliados y socios. A través de la cooperación, Estonia promueve la ciberseguridad global y mejora su propio desempeño.

Objetivo general

- Aumentar las capacidades de ciberseguridad y la conciencia de la población sobre las ciberamenazas, garantizando así la continua confianza en el ciberespacio.

Objetivos específicos

- Garantizar la protección de los sistemas de información que brinden servicios vitales.
  - Garantizar soluciones alternativas para servicios esenciales.
  - Gestionar interdependencias entre servicios esenciales.
  - Garantizar la seguridad de las infraestructuras y servicios de tecnologías de la información y comunicación.
  - Gestionar ciberamenazas para el sector público y privado.
  - Introducir un sistema nacional de monitoreo para la ciberseguridad.
  - Garantizar la continuidad del Estado en el ciberespacio.
  - Promocionar una cooperación internacional en la protección de infraestructuras críticas de información.
- Mejorar la lucha contra la ciberdelincuencia.

    - Mejorar la detección de la ciberdelincuencia.
    - Aumentar la concienciación a los ciudadanos sobre los riesgos.
    - Promocionar la cooperación internacional contra la ciberdelincuencia.
- Desarrollar capacidades nacionales de ciberdefensa.
    - Sincronizar planes y preparación militar para emergencias civiles.
    - Desarrollar ciberdefensa colectiva y colaboración internacional.
    - Desarrollar capacidades militares de ciberdefensa.
    - Garantizar un alto nivel de concienciación sobre el papel de la ciberseguridad en la defensa nacional
- Gestionar la evolución de las amenaza en ciberseguridad.
    - Garantizar la siguiente generación de profesionales en ciberseguridad.
    - Desarrollar contrataciones inteligentes para soluciones de ciberseguridad.
    - Apoyar el desarrollo de empresas que provean ciberseguridad y soluciones nacionales de ciberseguridad.
    - Evitar riesgos de ciberseguridad en nuevas soluciones.
- Desarrollar actividades intersectoriales.
    - Desarrollar un marco legal para apoyar la ciberseguridad.
    - Desarrollar políticas internacionales de ciberseguridad
    - Impulsar una cooperación más estrecha con aliados y socios.
    - Mejorar la capacidad de la Unión Europea.

2.8.3 Colombia [24]

Colombia creó en el año 2011 el documento CONPES (Consejo Nacional de Política Económica y Social) 3701 con el auspicio de algunos ministerios y departamentos del Gobierno. Este documento busca generar lineamientos en temas de ciberseguridad y ciberdefensa orientados a elaborar una estrategia nacional de ciberseguridad para proteger los recursos informáticos del país. En el 2016 este documento fue actualizado para considerar la gestión de riesgos en el entorno digital.

CONPES 3701 es lo más cercano que tiene Colombia a una estrategia de ciberseguridad. A continuación se destaca los puntos importantes del documento:

Problema Central

Colombia identificó que la capacidad actual del Estado para enfrentar las amenazas informáticas presenta grandes debilidades. Las principales debilidades fueron:

- Iniciativas y operaciones en ciberseguridad y ciberdefensa sin una adecuada coordinación.
- Debilidad en la oferta y cobertura de capacitación especializada en ciberseguridad y ciberdefensa.
- Debilidad en regulación y legislación de la protección de la información y de los datos.

Objetivo general

- Fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético, creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio.

Objetivos específicos

- Implementar instancias apropiadas para prevenir, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional. Con este objetivo se crean los siguientes organismos:
    - Comisión Intersectorial, encargada de fijar la visión estratégica de la gestión de la información, así como de establecer los

lineamientos respecto a la gestión de las infraestructuras tecnológicas, información pública y ciberseguridad y ciberdefensa. Esta Comisión está encabezada por el Presidente de la República.

  - El Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT, encargado de coordinar a nivel nacional en aspectos de ciberseguridad y ciberdefensa.

  - Comando Conjunto Cibernético de las Fuerzas Militares, encargado de prevenir y contrarrestar toda amenaza o ataque de naturaleza cibernética que afecte los valores e intereses nacionales.

  - Centro Cibernético Policial, encargado de la ciberseguridad del territorio colombiano, ofreciendo información, apoyo y protección antes los delitos cibernéticos.

- Brindar capacitación especializada en seguridad de la información y ampliar líneas de investigación en ciberseguridad y ciberdefensa.

- Fortalecer la legislación en materia de ciberseguridad y ciberdefensa, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales en esta temática.

Al igual que la estrategia de ciberseguridad de España, se establece un plan de acción para lograr los objetivos. Este plan de acción presenta un mayor nivel de detalle porque provee información como: acciones concretas, entidad responsable, dependencia del Estado y fechas de inicio y finalización de la acción.

El documento también aporta las leyes y resoluciones que Colombia ha promulgado en el tema de ciberseguridad, entre las cuales menciona:

- Ley 527 de 1999 COMERCIO ELECTRÓNICO
  Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.

- Ley 599 de 2000

  Tipifica el acceso abusivo a un sistema informático y la violación ilícita de comunicaciones.
- Ley 1273 de 2009

  Impulsa la protección de la información y de los datos.
- Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009

  Obliga a los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet a implementar modelos de seguridad de acuerdo con los marcos definidos por la UIT.
- Circular 052 de 2007 (Superintendencia Financiera de Colombia)

  Establece requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios.

Adicionalmente diferentes sectores del Gobierno han aportado diferentes iniciativas y documentos para la elaboración del documento CONPES. Colombia ha recibido ayuda de la OEA mediante la realización de talleres de concienciación en temas de ciberseguridad. El Ministerio de Defensa de Colombia es el organismo encargado de posicionar el tema de ciberseguridad y ciberdefensa dentro de la agenda nacional.

2.8.4 Otros países de América Latina [25]

Brasil publicó en febrero de 2008 en *Diário Oficial da União* Nº 27, la importancia de sus infraestructuras críticas y ha elaborado una Guía de Referencia para gestionar la ciberseguridad en infraestructuras críticas.

Argentina ha generado el "Programa Nacional de Infraestructuras Críticas de información y ciberseguridad", el cual en la actualidad, depende de la Dirección Nacional de Infraestructuras de Información y Ciberseguridad, del Ministerio de Modernización.

CAPÍTULO 3

CIBERSEGURIDAD EN ECUADOR

El presente capítulo detalla los diferentes avances en ciberseguridad que han desarrollado las instituciones públicas del Ecuador. Se mencionará algunas normativas y acciones y su aporte en el campo de la ciberseguridad.

3.1 Situación Actual

Ecuador no ha desarrollado aún una estrategia nacional de ciberseguridad para establecer los lineamientos, objetivos y plan de acción que permita proteger los servicios, la información, las infraestructuras críticas y a los ciudadanos frente a ciberamenazas en el ciberespacio.

Sin embargo, diferentes instituciones públicas han realizado actividades de manera independiente y están contribuyendo a mejorar la ciberseguridad a nivel nacional. Entre los aportes realizados por estas instituciones en materia de ciberseguridad se encuentran los siguientes:

- **Ley de comercio electrónico, firmas electrónicas y mensajes de datos aprobada por el Congreso Nacional en el 2002.**

  Establece la validez a la información en el mundo digital, es decir: que los mensajes de datos, correos electrónicos, etc, son válidos, considerando los principios de confidencialidad y reserva de la información. Además establece la validez de la firma electrónica para garantizar la autenticidad e integridad de la documentación digital. Considerando los beneficios de la firma electrónica, esta se puede utilizar para cifrar la información sensible y mantener la confidencialidad e integridad de los datos en el mundo digital, además de proveer evidencia indubitable del origen o autor. Adicionalmente, esta ley establece sanciones sobre infracciones informáticas. Entre ellas se encuentra:

- Robo de claves o alteración en sistemas de seguridad para acceder u obtener información sensible en sistemas de información.
- Alteración de mensajes de datos o información incluida en éstos.
- Destrucción, eliminación, alteración de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica.
- Destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos.

- **Acuerdo Ministerial 166 - EGSI (Esquema Gubernamental de Seguridad de la Información).**

  Desarrollado por la Secretaría Nacional de la Administración Pública en el 2013. Este acuerdo fue elaborado en la base a la norma NTE INEN-ISO/IEC 27002 “Código de Práctica para la Gestión de la Seguridad de la Información”. Entre los objetivos de este acuerdo destacamos:

  - Mantener la seguridad en la información en diferentes medios y formatos de las entidades de la Administración Pública Central, que dependen de la Función Ejecutiva.
  - Minimizar los riesgos a los que está expuesta la información.
  - Proteger la infraestructura gubernamental de los ciberataques.

  Se dispuso en todas las entidades públicas el uso obligatorio de este acuerdo, por lo cual se garantiza que se implementen adecuados niveles de seguridad en los sistemas de información utilizados por el sector público.

- **Resolución JB-2010-2148 Libro I "Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero".**

  Elaborado por la Superintendencia de Bancos y Seguros en el 2012 con la finalidad de gestionar el riesgo operativo ante el uso inseguro de las tecnologías de la información y comunicación. Esta resolución obliga a que todas las instituciones del sistema financiero implementen algunos controles de seguridad para mitigar los diferentes riesgos relacionados al fraude que se puede llevar a cabo por el mal uso de las tecnologías de información y comunicación. Estos controles de seguridad permitirán a las instituciones financieras entregar servicios seguros y confiables a los clientes y reducir posibles pérdidas económicas y daños a la reputación.

  Esta resolución se enfoca principalmente en la seguridad de:

  - Tarjetas de débito y crédito
  - Cajeros automáticos
  - Puntos de venta (POS y PIN Pad)
  - Banca electrónica
  - Banca móvil
  - Sistemas de audio respuestas (IVR)

- **Creación del EcuCERT**

  Es el Centro de Respuestas a Incidentes Informáticos de la Agencia de Regulación y Control de las Telecomunicaciones del Ecuador. Su objetivo principal es apoyar en la prevención y resolución de incidentes de seguridad informática del sector de las telecomunicaciones, las Instituciones del Estado ecuatoriano y las instituciones privadas que demanden los servicios que el EcuCERT brinda. Adicionalmente contribuye en la seguridad de las redes de telecomunicaciones de todo territorio nacional y del uso de Internet.

Algunos de los propósitos del EcuCERT son:

- Ser el punto de contacto entre el Estado Ecuatoriano y otros equipos de respuesta internacionales.
- Asesorar en el cumplimiento de la Normativa de Seguridad de la Información de aplicación vigente en el Ecuador.
- Promover la adopción de Políticas de Seguridad de la Información en las Instituciones públicas y el sector de las telecomunicaciones.
- Promover la creación de Equipos de Respuesta a Incidentes de Seguridad Informática en sectores con infraestructuras críticas nacionales, sector privado y sociedad civil.
- Impulsar la conformación de un Comité de Ciberseguridad.

- **Creación del Comando Conjunto de Ciberdefensa**

  Se crea con Acuerdo Ministerial 281 en septiembre del 2014, siendo un ente que debe implementar la capacidad de ciberdefensa bajo el Comando Conjunto de las Fuerzas Armadas. Es el responsable de proteger la infraestructura crítica del Estado en el ámbito digital y tecnológico, con prioridad a las Fuerzas Armadas y minimizar o bloquear los sistemas de información del enemigo a fin de contribuir a la defensa de la soberanía nacional.

3.2 Ciberseguridad en Infraestructuras Críticas

En base al análisis realizado en la sección anterior podemos decir que a nivel normativo las instituciones públicas del Ecuador han realizado un gran esfuerzo para elevar el nivel de ciberseguridad en diferentes sectores con servicios vitales y que aportan a establecer un ciberespacio seguro para los ciudadanos, sobre la premisa de que los servicios vitales pueden funcionar correctamente en un ciberespacio seguro, libre de amenazas y con los riesgos debidamente gestionados.

Los sectores vitales en Ecuador que se encuentran trabajando en temas de ciberseguridad son los siguientes:

- Financiero
- Gobierno
- Telecomunicaciones
- Defensa

Sin embargo, el Ecuador debe continuar reforzando los temas relacionados a la ciberseguridad, con el objetivo de cubrir la mayoría de sectores y en especial, los que brindan servicios vitales a los ciudadanos, teniendo en cuenta las siguientes cuestiones:

- La mayoría de servicios vitales son brindados por instituciones públicas. Si estas instituciones públicas cumplen con el Acuerdo Ministerial 166, sin duda elevarán sus niveles de ciberseguridad. Sin embargo, para brindar un servicio realmente seguro, deben implementar controles adicionales, relacionados con la protección de las Infraestructuras Críticas y que no se encuentran completamente cubiertos por el mencionado acuerdo. Esto es así debido a que el Acuerdo Ministerial no cubre en forma integral todos los controles de ciberseguridad. Adicionalmente, se omiten temas importantes como: la cooperación público-privada, la capacidad forense ante incidentes, la gestión de riesgos, la investigación en temas de ciberseguridad y el desarrollo de herramientas de ciberseguridad, entre otros.

- Si bien como se dijo en el punto anterior, la mayor parte de los servicios vitales en Ecuador son brindados por entidades públicas, algunos son provistos por instituciones privadas, que no se encuentran alcanzadas por normativas o controles de ciberseguridad específicos. Es por esto que debe existir una estrategia para requerir que las instituciones privadas eleven también sus niveles de ciberseguridad y que exista una adecuada cooperación con las instituciones públicas. En este sentido, los

organismos estatales que regulan los servicios ofrecidos por las empresas privadas deben poner en su agenda los temas de ciberseguridad y establecer requerimientos en este sentido.

- Debido al lento crecimiento de las tecnologías de la información en el Ecuador, existe actualmente una importante carencia en cuanto a recursos humanos calificados en el área de ciberseguridad, capaces de gestionar correctamente los riesgos ante nuevas amenazas. La escasa capacitación de técnicos y profesionales está siendo liderada por empresas privadas dedicadas la ciberseguridad y no por las instituciones académicas o de formación técnica.

- Adicionalmente, el gobierno debe trabajar en un plan de concienciación para los ciudadanos, con el fin de prevenirlos frente a las amenazas informáticas. Este plan debe tener la impronta de otras campañas de difusión, como las utilizadas para enfrentar los problemas de drogadicción, delincuencia, corrupción o alcoholismo, en el sentido de alcanzar a toda la población, especialmente a la más vulnerable (en este caso, los niños, niñas y adolescentes) y presentarse en un lenguaje sencillo y no técnico, alertando de los riesgos que se corren si se hace un uso inseguro de las tecnologías de la información.

- Finalmente, el gobierno debe estar dispuesto a cooperar internacionalmente con otros países y organizaciones en el campo de la ciberseguridad, lo cual beneficiará a organizaciones y profesionales del campo. En este sentido, se deberán analizar y eventualmente, adherir a los tratados internacionales en la materia.

CAPÍTULO 4

MODELO PARA IDENTIFICAR SERVICIOS CRÍTICOS

El presente capítulo desarrolla un modelo para categorizar como crítico un servicio provisto por una infraestructura de información, basado en la utilización de una serie variables que permiten determinar su nivel de criticidad. Provee además una herramienta para que los responsables de la protección de infraestructuras críticas de un país puedan identificarlas. La base utilizada para su desarrollo es una publicación de diciembre del 2016 elaborada por ENISA para la clasificación de servicios, bajo el título "Metodologías para la identificación de servicios y activos de Infraestructuras Críticas de Información". [26]

Este modelo es una herramienta de fácil aplicación, una vez obtenida la información y los conocimientos sobre el funcionamiento de todos los servicios sobre los que se aplicará y la manera en que éstos interaccionan entre sí.

4.1 Desarrollo del modelo

El modelo se desarrolla a través de una secuencia de tareas que se despliegan con el objetivo de categorizar servicios como críticos. Para facilitar su aplicación, se han agrupado los diferentes servicios por sectores. La información presentada en algunas tareas es ilustrativa, y se introduce con el fin de validar la aplicabilidad del modelo. Se aclara que el resultado de cada tarea variará según el país ya que cada uno presenta un escenario diferente.

Las tareas que conforman el modelo son las siguientes:

- Identificación de servicios.
- Interdependencia de servicios
- Definición de las variables
- Categorización de los servicios

A continuación se describe cada una de ellas y su resultado esperado.

4.1.1 Identificación de servicios

El objetivo de esta tarea es identificar todos los servicios que se ofrecen a la población de un país, agrupándolos por sectores. A manera de ejemplo: el sector telecomunicaciones tiene los siguientes servicios: telefonía fija, telefonía y redes de datos. La definición de dichos sectores es una tarea que generalmente recae en los gobiernos nacionales, de acuerdo a las actividades que se realicen en sus respectivas economías. Se utilizarán en este caso 18 sectores, con fines ejemplificativos.

Se deja aclarado que conceptualmente se puede usar sectores o servicios en el modelo y el resultado de su aplicación, no se verá afectado si bien en el segundo caso presentará un mayor detalle pero también, una mayor complejidad en su aplicación.

Por otro lado, es importante destacar que dichos servicios pueden ser brindados por instituciones públicas o privadas, si bien esta tarea es independiente del tipo de prestador. Tampoco está relacionada con el nivel de tecnologías de información que utiliza un servicio determinado para su funcionamiento. Como resultado se obtiene la información presentada en la Tabla 4.1.

Para facilidad en la aplicación del modelo, se recomienda asignar un código a cada sector, según surge de la primera columna de la Tabla.

Listado de sectores		
Código	**Sector**	**Servicios**
S1	Agua	Almacenamiento, distribución y tratamiento del agua.
S2	Alimentación	Producción, suministro y distribución de alimentos.
S3	Comercio	Compras, negocios, entretenimiento y alojamiento.
S4	Defensa	Defensa / Soberanía nacional.
S5	Energía	Suminstro de energía eléctrica.
S6	Gas Natural	Extracción, transporte, distribución y almacenamiento de gas.
S7	Gobierno	Servicios públicos que rigen en la Constitución.
S8	Industria	Servicios de manufactura.
S9	Manejo de Residuos	Recoger y tratar aguas residuales.
S10	Petróleo	Extracción, refinamiento, transporte y almacenamiento de petróleo y derivados.

S11	Protección civil	Servicios de emergencia y rescate.
S12	Químico	Gestión, almacenamiento y eliminación de materiales peligrosos.
S13	Salud	Hospitales y control de infecciones y epidemias.
S14	Seguridad y Orden público	Orden público y seguridad en los ciudadanos.
S15	Servicios Financieros	Bancos, transacciones de pagos y banca online.
S16	Tecnologías de la información	Servicios web y centros de datos.
S17	Telecomunicaciones	Redes de voz (Telefonía móvil y fija) y datos (Internet).
S18	Transporte	Servicios de movilización aérea, terrestre y marítima.

Tabla 4.1 – Listado de servicios brindados a la población, agrupados por sector

4.1.2 Interdependencia de servicios

Esta tarea busca identificar las posibles interdependencias que existen entre los distintos servicios. Para realizar esta actividad se utiliza la siguiente premisa: ¿un evento o incidente de ciberseguridad que interrumpe total o parcialmente o degrada la disponibilidad de uno o varios de los servicios del sector Sx afecta el funcionamiento de los servicios del sector Sy?

Para realizar esta tarea es importante conocer el funcionamiento de cada servicio y sus dependencias de otros servicios para su normal funcionamiento. Como resultado de esta tarea se podrá determinar qué servicios son cruciales para la operación de uno o varios de los sectores identificados y cómo impacta la ocurrencia de un incidente de ciberseguridad en ellos.

Para entender el concepto de interdependencias entre los diferentes sectores, se presenta el Gráfico 4.1, con su respectiva explicación a manera de ejemplo.

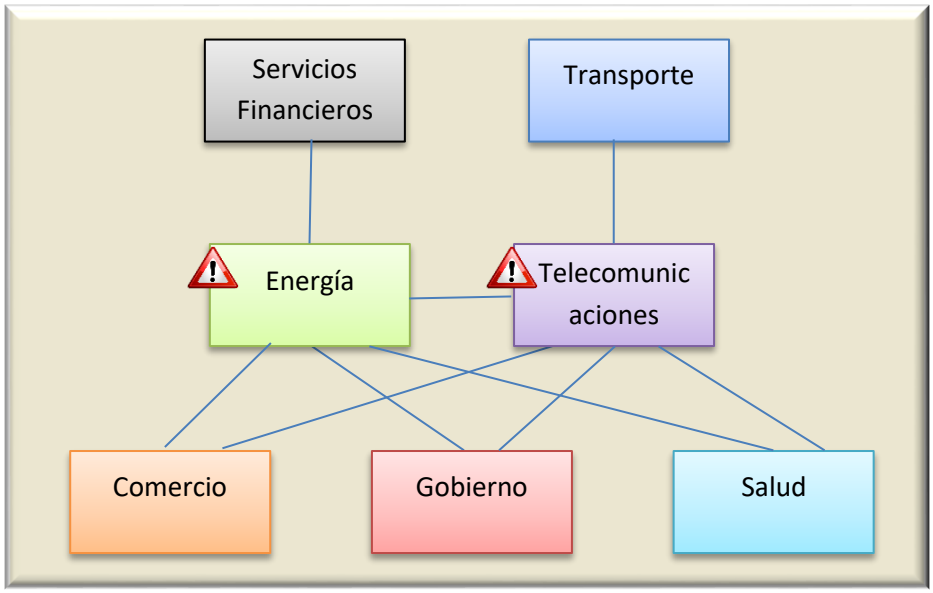

Gráfico 4.1 – Ejemplo de interdependencia de servicios [27]

En el Gráfico bajo análisis, se identifican 8 sectores existentes en la mayoría de las economías. Si los servicios del sector energía se vieran afectados por un incidente de ciberseguridad, provocando la indisponibilidad total o parcial de sus servicios en un área geográfica determinada, se podrían plantear los siguientes escenarios:

- En cuanto al sector financiero: uno o varios bancos que no pueden brindar servicios, cajeros automáticos no operativos, limitaciones en la aprobación de transacciones bancarias, etc.

- En cuanto al sector de telecomunicaciones: los servicios de telefonía fija o móvil e Internet podrían no estar disponibles a los usuarios. Los proveedores de servicios tendrán inconvenientes que podrían proyectarse en las redes de datos corporativas.

- En cuanto al sector del comercio: los negocios no van a poder usar los sistemas de facturación y medios de pago y los clientes podrían verse impedidos de comprar en línea.

- En cuanto al funcionamiento del Estado: los servicios asociados a las funciones ejecutiva, legislativa y judicial podrían no estar disponibles para brindar servicios a los habitantes y organizaciones del país.

- En cuanto a los servicios de salud: los hospitales y clínicas podrían ver limitadas sus posibilidades de atender pacientes, realizar

estudios, trasladar personal o personas con necesidades sanitarias, etc.

Si los casos anteriores fueran factibles, se puede afirmar que existe interdependencia entre los sectores listados y el sector energía y en consiguiente, se deben adoptar medidas urgentes para efectivizar los controles preventivos, detectivos y correctivos pertinentes.

Para efectuar el análisis de las interdependencias, debe tenerse en cuenta que al hacerlo, no se consideran los controles de ciberseguridad que un sector haya implementado. Esto es porque si bien la ciberseguridad permite adoptar los mecanismos para gestionar adecuadamente los riesgos, siempre existe la probabilidad de que una nueva amenaza explote una vulnerabilidad en los activos de información de infraestructuras críticas bajo análisis. Por ejemplo: el sector financiero puede cumplir con todas las normativas, regulaciones, etc., para proteger sus servicios pero eso no garantiza que un incidente pueda afectar el comercio, los servicios del gobierno, etc. y esto tenga un efecto indirecto sobre el sector. En otras palabras, se toma en cuenta el riesgo inherente a cada servicio, sin considerar los controles ya implementados.

Por lo tanto, y como resultado del análisis de interdependencias, se obtiene una tabla que las identifica, en la que las columnas representan los sectores efectivamente afectados por un incidente de ciberseguridad y las filas, los que pueden sufrir consecuencias, debido a una interdependencia.

Con esta lógica, las “x” en la siguiente Tabla 4.2 reflejan cuando se evalúa el mismo servicio tanto en las columnas como en las filas y su efecto sobre el resto. Por ejemplo, si un incidente de ciberseguridad en el sector S1 afecta al sector S3, S7 y S10 se debe marcar con una x, mientras que los casilleros en blanco se entiende que no generan una interdependencia.

En el modelo propuesto, la Tabla 4.2 es muy importante porque forma parte de las variables que se definirán en el siguiente paso, ya que en función del número de interdependencias, los criterios a considerar producirán diferentes valores.

La “x” de la siguiente tabla refleja un efecto sobre el mismo sector. Cabe acotar al respecto, que en este modelo no se toman en cuenta las interdependencias intra-sector (por ejemplo, de un proveedor de energía respecto a otro), con el fin de no agregar complejidad. No obstante este aspecto debe ser también tenido en cuenta al establecer un plan de acción de protección de infraestructuras críticas a nivel nacional.

	Interdependencia de los sectores																	
Sector	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**	**S8**	**S9**	**S10**	**S11**	**S12**	**S13**	**S14**	**S15**	**S16**	**S17**	**S18**
S1	X																	
S2		X																
S3			X															
S4				X														
S5					X													
S6						X												
S7							X											
S8								X										
S9									X									
S10										X								
S11											X							
S12												X						
S13													X					
S14														X				
S15															X			
S16																X		
S17																	X	
S18																		X

Tabla 4.2 – Tabla de las interdependencias entre sectores

4.1.3 Definición de las variables

Esta tarea consiste en la identificación de los criterios, denominados variables, que permitirán categorizar la criticidad de los servicios, usando para ello distintas perspectivas. Estas variables consideran el impacto que puede tener la interrupción de un servicio en un país. El objetivo de este paso es valorar todos los servicios a través de cada una de las variables.

A los fines de esta tarea, la interrupción se considera como la afectación de la provisión del servicio que incluso puede abarcar su destrucción total o parcial e incluye cualquier tipo de indisponibilidad ocasionada por una

amenaza cibernética que explota una vulnerabilidad en la infraestructura afectada.

A cada variable se le pueden asignar tres posibles calificadores respecto a su alcance y gravedad, que son: ALTO, MEDIO y BAJO. En esta tarea se califican todos los sectores por cada variable.

A continuación se definen y describen las variables seleccionadas para este modelo, teniendo en cuenta que a partir de su enunciación y definición se podrá escoger correctamente su valoración. Se aclara que en razón de ser una calificación valorativa, pueden presentarse variaciones de criterio entre quienes realizan la tarea. Por ello se recomienda efectuar esta tarea en equipos conformado por un número no muy grande de especialistas, en los que se pueda analizar en profundidad cada variable y calificación seleccionada.

- Legislación Nacional.- Si el sector se encuentra descrito como básico en la legislación nacional y debe ser brindado a los habitantes del país, el impacto se considera:
    - ALTO.- Si un servicio se encuentra definido como tal en la legislación nacional.
    - MEDIO.- Si un servicio que no se encuentra definido como básico en la legislación nacional pero sí en una legislación local, por ejemplo de una provincia, territorio, ciudad, etc.
    - BAJO.- Si un servicio no se encuentra definido como básico en la legislación nacional, regional o provincial.
- Salud Pública.- Si la salud de la población puede verse afectada por la interrupción o afectación de un servicio. No debe confundirse con el Sector Salud que es uno de los agrupamientos posibles de servicios, sino a la probabilidad que un incidente de ciberseguridad en cualquier sector genere consecuencias en la salud de los habitantes. Por ejemplo, un incidente de ciberseguridad que afecta

al Sector Químico podría tener un impacto ALTO en esta variable. El impacto se considera:

  - ALTO.- Si la interrupción de un servicio genera daños graves e irreparables en la población.

  - MEDIO.- Si la interrupción de un servicio genera daños leves en la población, afectando solo a determinados rangos etarios (ancianos, menores de un año, etc.).

  - BAJO.- Si la interrupción de un servicio no afecta la salud de la población.

- Medio ambiente.- Si las fallas o la interrupción en la prestación de los servicios del sector afectan el medio ambiente. Esta variable hace referencia a los impactos que puede tener sobre la naturaleza ante alguna interrupción o falla registrada en una entidad perteneciente a un sector. El impacto se considera:

  - ALTO.- Si se afectan recursos NO RENOVABLES.

  - MEDIO.- Si se afectan recursos RENOVABLES.

  - BAJO.- Si la interrupción del sector no afecta al medio ambiente.

- Impacto en la población.- Esta variable se refiere al número de habitantes sobre los que impacta la interrupción o falla de un servicio. El impacto se considera:

  - ALTO.- Si el servicio afecta a más del 10% de la población de una nación.

  - MEDIO.- Si el servicio afecta a más del 5% de la población.

  - BAJO.- Si el servicio afecta a un grupo reducido de la población.

- Económico-financiero.- Esta variable se refiere al impacto económico-financiero de una interrupción de un servicio en un país. El impacto se considera:

    - ALTO.- Si el servicio impacta sobre los servicios vinculados a los ingresos que forman parte del presupuesto del Estado, se inhabilitan las transferencias externas e internas de dinero en un país o evento similar y existe un alto costo para restablecerlo nuevamente.

    - MEDIO.- Si el servicio inhabilita las transferencias de dinero internas en un país o el sistema de cuentas públicas y existe un costo para ponerlo a funcionar nuevamente.

    - BAJO.- Si el restablecimiento del servicio sólo representa un costo y es posible restablecerlo rápidamente.

- Orden Público.- Esta variable se refiere al caos que puede ocasionar en la sociedad la interrupción parcial o total o falla de algún servicio. El impacto se considera:

    - ALTO.- Si el servicio interrumpido genera un caos a nivel nacional que afecta la propiedad pública y privada e implica desplazar y utilizar en forma masiva las fuerzas del orden para controlarlo.

    - MEDIO.- Si el servicio interrumpido genera un caos sin afectación de las propiedades públicas y privadas, por lo cual solo es necesario desplegar fuerzas del orden locales para controlarlo.

    - BAJO.- Si la interrupción del servicio no genera caos en el orden público.

- Interdependencia.- Esta variable se relaciona con el resultado de la tarea realizada en el punto anterior. Cabe acotar que los siguientes valores dependerán de la cantidad de sectores identificados en una

economía. A los fines del ejemplo presentado, el impacto se considera:

- ALTO.- Cuando tiene de 10 a 18 interdependencias.
- MEDIO.- Cuando tiene de 6 a 10 interdependencias.
- BAJO.- Cuando tiene de 1 a 5 interdependencias.

Como resultado de esta tarea se obtiene una matriz con todos los servicios y su valoración para cada variable de acuerdo, como ya se explicó, a: ALTO, MEDIO y BAJO. Las columnas de la matriz hacen referencia a los servicios y las filas a las diferentes variables indicadas en esta tarea. Esta matriz servirá para después identificar la criticidad de un servicio.

Variables por sector							
Sector	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**
S1							
S2							
S3							
S4							
S5							
S6							
S7							
S8							
S9							
S10							
S11							
S12							
S13							
S14							
S15							
S16							
S17							
S18							

Tabla 4.3 – Variables por cada sector

4.1.4 Categorización de los servicios

Como se explicó, para identificar si un servicio es crítico, es necesario evaluarlo en base a una serie de criterios, denominadas variables a los fines de este modelo. En esta tarea, con la que finaliza el desarrollo del modelo, se

van a establecer los criterios para categorizar un servicio como crítico. Como primer punto se va a cuantificar el impacto en base a la siguiente Tabla 4.4, de tal manera que tengamos una matriz con valores numéricos:

IMPACTO	VALOR
ALTO	3
MEDIO	2
BAJO	1

Tabla 4.4 – Cuantificar el impacto

Una vez que está cuantificada la matriz, se procede a sumar los valores de impacto de cada sector y con estos resultados, se aplican las siguientes conclusiones:

- Considerando que un sector tiene impacto ALTO en todas las variables, tendrá un máximo valor de impacto igual a 21.
- Considerando que un sector tiene impacto BAJO en todas las variables tendrá un máximo valor de impacto igual a 7.
- Un servicio es crítico cuando la sumatoria del impacto es mayor a 15. Los servicios que no entran dentro de ese rango no se los considera como críticos.

La matriz final quedará de la siguiente manera. En la columna se encuentran todos los sectores y en las filas se encuentran las variables, el valor cuantificado y la criticidad. El campo criticidad identifica si un sector es categorizado como crítico.

Criticidad de los servicios									
Sector	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**Valor**	**Criticidad**
S1									
S2									
S3									
S4									
S5									
S6									
S7									
S8									

S9	
S10	
S11	
S12	
S13	
S14	
S15	
S16	
S17	
S18	

Tabla 4.5 – Criticidad de los servicios

Sobre la base de los resultados de la Tabla 4.4, se pueden efectuar las siguientes derivaciones:

- Los esfuerzos destinados a proteger las infraestructuras críticas deben formularse y priorizarse en base al nivel de criticidad de los sectores resultantes de la matriz.

- El modelo permite realizar una categorización de sectores en críticos. Sin embargo existen parámetros que pueden ser modificados en las diferentes etapas de acuerdo a criterios del o los profesionales que apliquen el modelo.

- Para los profesionales de ciberseguridad encargados de proteger infraestructuras críticas de un país, que necesiten identificar los sectores con servicios críticos, este modelo puede resultar de gran ayuda para ordenar criterios y fijar prioridades y cursos de acción, Además les permite enfocar sus esfuerzos en los sectores con mayor exposición y prepararse mejor. Incluso, al avanzar el plan de acción, las medidas de protección que utilicen para los sectores más críticos pueden ser adaptados y reutilizados para los sectores que presenten un menor nivel de criticidad.

CAPÍTULO 5

CONTROLES BÁSICOS DE CIBERSEGURIDAD PARA LAS INFRAESTRUCTURAS CRÍTICAS

En el presente capítulo se definen los controles básicos de ciberseguridad sugeridos para implementar en las infraestructuras críticas. Para agrupar los controles de seguridad se ha utilizado la publicación del NIST “Marco de referencia para mejorar la ciberseguridad en las infraestructuras críticas” y para definir los controles, se han seleccionado los 20 controles críticos de ciberseguridad del Centro de Seguridad en Internet, organización que se describe brevemente más abajo.

Los controles de ciberseguridad seleccionados ayudan a minimizar y gestionar los riesgos de amenazas que pueden explotar una o varias vulnerabilidades y que afecten la disponibilidad de los servicios esenciales que se brinda a la población y son base de la economía de un país.

El cumplimiento de estos controles deberá ser exigido por las instituciones responsables de la ciberseguridad a nivel nacional y en este caso bajo revisión, en el Ecuador, a los operadores que sean propietarios de activos utilizados para proveer servicios esenciales, ya sea empresas privadas o entidades públicas. El gobierno juega un rol muy importante en esta tarea porque debe velar por el cumplimiento de los controles, asegurando de este modo, la provisión de los servicios. Como ya se mencionó, los controles que siguen han sido definidos en base a estándares y buenas prácticas de ciberseguridad y son reconocidos y utilizados internacionalmente.

5.1 Categorías de los controles de ciberseguridad [28]

El marco para mejorar la ciberseguridad en las infraestructuras críticas del NIST tiene un enfoque basado en riesgos. Puede ser usado para ayudar a identificar y priorizar acciones para reducir los riesgos de seguridad. Está compuesto por un conjunto de actividades que son comunes en los servicios

críticos. Utiliza 5 categorías para proveer una vista estratégica de la gestión de los riesgos de ciberseguridad en infraestructuras críticas.

Las categorías de los controles que establece el NIST organizan actividades básicas de ciberseguridad de alto nivel, las que se alinean con metodologías existentes para la gestión de incidentes y ayudan a mostrar el impacto de las inversiones en ciberseguridad. Estas categorías son: identificar, proteger, detectar, responder y recuperar.

Gráfico 5.1 – Categorías de los controles de ciberseguridad

Las categorías serán desarrolladas brevemente a continuación:

- **Identificar.-** Concientizar en la organización sobre la importancia de gestionar los riesgos de ciberseguridad que pudieran afectar los sistemas, los activos y la información. Las actividades de la categoría de identificación son fundamentales para el uso efectivo del marco. Entender el contexto organizacional, los recursos que soportan servicios críticos y los riesgos relacionados con la ciberseguridad, permite a una organización centrarse y priorizar sus esfuerzos.

- **Proteger.-** Desarrollar e implementar mecanismos apropiados para asegurar la provisión de servicios críticos. La categoría de protección es compatible con la capacidad de limitar o contener el impacto de un posible evento de ciberseguridad.

- **Detectar.-** Desarrollar e implementar apropiadas actividades para identificar la ocurrencia de un evento de ciberseguridad. La categoría de detección permite el descubrimiento oportuno de eventos de ciberseguridad.

- **Responder.-** Desarrollar e implementar apropiadas actividades para tomar medidas con respecto a un evento de ciberseguridad

detectado. La categoría de respuesta apoya la capacidad de contener el impacto de un posible evento de ciberseguridad.

- **Recuperar.-** Desarrollar e implementar apropiadas actividades para mantener los planes de resiliencia y restaurar las capacidades o servicios que se vieron afectados debido a un evento de ciberseguridad. La categoría recuperar soporta la recuperación oportuna a las operaciones normales para reducir el impacto de un evento de ciberseguridad.

5.2 Controles críticos de ciberseguridad [29]

El Centro de Seguridad en Internet es una organización sin fines de lucro que aporta conocimientos y experiencia para identificar, desarrollar, validar, promover y sostener la adopción de las mejores prácticas de ciberseguridad. Se encuentra localizado en New York y está compuesto aproximadamente de 180 miembros de 17 diferentes países. Un gran aporte ha sido el desarrollo de los 20 controles críticos de seguridad, que han sido adoptados como buenas prácticas. En efecto, las empresas públicas y privadas usan estos controles para medir el nivel de madurez en ciberseguridad.

A continuación se van a identificar los controles de ciberseguridad que deben implementarse en las categorías definidas en el “Marco para mejorar la ciberseguridad en las infraestructuras críticas” del NIST mencionado en el punto anterior.

- **Identificar**
    - Control 1 - Inventariar dispositivos autorizados y no autorizados
    - Control 2 - Inventariar programas autorizados y no autorizados

    - Control 17 - Evaluar y capacitar al personal en ciberseguridad

- **Proteger**

    - Control 3 – Configurar en forma segura el hardware y el software
    - Control 5 - Controlar el uso de los privilegios administrativos
    - Control 7 - Proteger los servicios de navegación web y correo electrónico
    - Control 8 - Defender contra el código malicioso
    - Control 9 - Limitar y controlar los puertos de red
    - Control 11 – Configurar en forma segura los dispositivos de red
    - Control 12 - Defender el perímetro
    - Control 13 - Proteger de datos
    - Control 14 – Otorgar accesos en base al principio del menor privilegio
    - Control 15 - Controlar el acceso a redes inalámbricas
    - Control 18 – Incorporar prácticas de desarrollo seguro en las aplicaciones
    - Control 20 – Realizar ejercicios de test de penetración

- **Detectar**

    - Control 4 - Evaluar y remediar en forma continua las vulnerabilidades
    - Control 6 - Mantener, monitorear y analizar los registros de auditoría

    - Control 16 - Controlar y monitorear cuentas.

- **Responder**

    - Control 19 - Gestionar y responder ante incidentes.

- **Recuperar**

    - Control 10 – Incorporar capacidades de recuperación de datos.

A partir de la definición de estos controles de ciberseguridad, los países y especialmente el Ecuador, deben establecer un plan para difundir y exigir su implementación a los proveedores u operadores de servicios críticos. El Ecuador ya tiene experiencia para gestionar este tipo de actividades, ya que en el 2013 solicitó la implementación del Acuerdo Ministerial 166 a todas las instituciones públicas. Este acuerdo requería la implementación de un Sistema de Gestión de la Seguridad de la Información.

Si bien el alcance de esta exigencia es más limitado, marca un posible camino a seguir. Adicionalmente se deben establecer instancias de auditoría, monitoreo y supervisión de la efectiva aplicación de controles, llevadas a cabo por organismos del gobierno responsables de la ciberseguridad, por organismos reguladores o por entidades privadas.

Adicionalmente, los países deben desarrollar una metodología para evaluar la implementación de los controles y medir el nivel de madurez de la ciberseguridad en los proveedores u operadores de servicios catalogados como críticos.

CAPÍTULO 6

RECOMENDACIONES

A partir de la realización del presente Trabajo Final de Maestría, se pueden formular las siguientes recomendaciones:

- Los gobiernos deben tomar conciencia sobre la importancia de incluir a la ciberseguridad como prioridad en su agenda.

- En esta línea, deben asignar a una entidad pública de alcance nacional las responsabilidades de establecer una estrategia nacional, generar normas, lineamientos y guías y brindar soporte para la implementación de los controles de ciberseguridad en todos los servicios críticos que se brindan a los habitantes.

- Todas las entidades que proveen servicios críticos, independientemente de su carácter público o privado, deben ser debidamente controladas por el Estado, ya sea a través de la entidad responsable de la ciberseguridad o de los organismos reguladores, en cuanto a la efectiva aplicación de controles para la protección de las infraestructuras críticas de información. Actualmente, en la mayoría de los países, el único sector realmente controlado por los gobiernos es el sistema bancario, posiblemente a raíz de las exigencias internacionales en materia de regulación bancaria.

- Los proveedores de servicios críticos deben utilizar la metodología de modelo de análisis de amenazas, con la finalidad de determinar los riesgos de ciberseguridad que pueden afectar sus servicios.

- Se debe tener en cuenta las características específicas de los distintos sectores al aplicar el modelo de amenazas, ya que cada uno tiene diferentes procesos, tecnologías, aplicaciones, etc., y por ende sus riesgos son diferentes.

- Los proveedores de servicios críticos deben realizar un relevamiento de activos de tecnologías de la información y operación y mantenerlo

actualizado, para asignar recursos en función de la criticidad y establecer prioridades para brindar un servicio más seguro.

- Los profesionales y especialistas en ciberseguridad deben utilizar un lenguaje comprensible para establecer una comunicación efectiva, teniendo en cuenta que los interlocutores no suelen dominar la jerga técnica.

- La estrategia nacional de ciberseguridad no debe basarse sólo en la perspectiva militar, sino integrar la mirada de diversos profesionales para cubrir cuestiones legales, de gestión, de concienciación, de protección del comercio electrónico y de generación de una industria de la ciberseguridad, entre otros.

- Las interdependencias entre sectores deben ser consideradas al analizar el impacto ante la falta de disponibilidad de un sector. La mayoría de los sectores son inter-dependientes entre sí.

- Los modelos son representaciones simplificadas de la realidad. Por lo tanto, al momento de poner en práctica el modelo aquí desarrollado, debe validarse su funcionamiento, en cada una de sus tareas, y hacer las correcciones que sean necesarias. Se trata de un proceso continuo, que va a ir variando en función del panorama de amenazas y de la evolución tecnológica, cuya aplicación debe ser debidamente monitoreada.

CAPÍTULO 7

CONCLUSIONES

La ciberseguridad en la mayoría de los países y especialmente en el Ecuador, se está desarrollando de manera aislada e independiente en cada sector de la economía. Tampoco existe una coordinación por parte del Estado que vele por la ciberseguridad a nivel nacional. Este escenario implica una duplicación de esfuerzos por parte de los diferentes sectores en la implementación de controles para la provisión de servicios confiables.

Para que esto no suceda, es necesaria la creación de una estrategia nacional de ciberseguridad, documento a través del cual los países alinean sus objetivos a nivel nacional en la materia y que abarca también la identificación y protección de las infraestructuras críticas de información utilizadas para brindar servicios esenciales a la población. Cada Estado es responsable de establecer un plan para proteger sus infraestructuras críticas, el que debe ser auditado en cada sector y medido y mejorado continuamente. Esto se justifica en el hecho de que las amenazas son cada vez más sofisticadas y cambiantes y deben ser identificadas en forma oportuna.

Lamentablemente, la brecha en materia de ciberseguridad que existe entre Latinoamérica y otros países más avanzados como EEUU, Canadá y aquellos ubicados en Europa, es aún muy amplia. Parte de la responsabilidad recae sobre los Estados que no han podido o sabido darle un carácter prioritario a este tema, lo cual es fundamental para elevar los niveles de ciberseguridad en un país y proteger a la población.

Si bien esta problemática ha sido afrontada en ciertos sectores como el bancario, el comercio electrónico y las telecomunicaciones, se detecta un nivel de concientización bajo en otras verticales esenciales de la economía y por lo tanto, se vislumbra un largo camino a recorrer para lograr un adecuado nivel de protección del ciberespacio.

El modelo o marco de referencia elaborado en este Trabajo Final de Maestría intenta aportar en la creación de estrategias nacionales de

ciberseguridad, ubicando esta temática en un lugar prioritario sobre la base del análisis de experiencias internacionales y publicaciones reconocidas en la materia y ayudando a identificar servicios críticos. Si bien el modelo fue pensado en el contexto de Ecuador, puede ser aplicado en cualquier otro país ya que no se encuentra asociado a una política o normativa específica que restrinja su uso a un área geográfica en particular.

El modelo desarrollado representa el primer paso para proteger los servicios críticos de un país. Su aplicación debe integrar múltiples miradas e identificar las interdependencias entre sectores para determinar los impactos directos e indirectos.

Como queda evidenciado, en la actualidad, ante un incidente de ciberseguridad que afecte un servicio crítico, la mayoría de los países de la región no cuenta con protocolos de respuesta para saber cómo proceder. Es un desafío para los gobiernos generar marcos legales, protocolos o acuerdos internacionales que faciliten la solución de tales eventos.

De acuerdo a lo analizado, Ecuador se encuentra trabajando en el campo de la ciberseguridad y ha desarrollado algunas normativas para proteger la información y los servicios de los habitantes. Sin embargo, es necesario que el siguiente paso sea la generación de una estrategia nacional de ciberseguridad. De ese modo se proporcionará un marco para la protección del ciberespacio que garantice el aprovechamiento de las tecnologías, en un entorno seguro.

Finalmente, hay muchas actividades que se deben reforzar para tener un alto grado de madurez en ciberseguridad a nivel nacional. La tecnología está avanzando exponencialmente y las organizaciones y los usuarios están adoptando estas tecnologías, sin conocer los riesgos que conllevan. La generación de una cultura de ciberseguridad es un paso ineludible para el progreso de una sociedad moderna. Aquí también el Estado debe ponerse a la cabeza por su rol fundamental como generador de conciencia en sus habitantes.

BIBLIOGRAFÍA

[1] Methodologies for the identification of Critical Information Infrastructure assets and services

https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis (Consultada el 28/02/2017)

[2] Definición PLC

http://recursostic.educacion.es/observatorio/web/gl/component/content/article/502-monografico-lenguajes-de-programacion?start=2 (Consultada el 06/02/2017)

[3] Definición SCADA

http://www.automatas.org/redes/scadas.htm (Consultada el 06/02/2017)

[4] Protección de Infraestructuras Críticas

https://s2grupo.es/wp-content/uploads/2017/01/PROTECCI%C3%93N-DE-INFRAESTRUCTURAS-CR%C3%8DTICAS-4%C2%BA-INFORME-T%C3%89CNICO-WEB..pdf (Consultada el 06/02/2017)

[5] Riesgos y Amenazas para la Seguridad Nacional

http://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-es-seguridad-nacional/riesgos-amenazas-para-seguridad-nacional (Consultada el 19/05/2017)

[6] THE ITU NATIONAL CYBERSECURITY STRATEGY GUIDE

http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf (Consultada el 06/02/2017)

[7] Definición de ciberseguridad

ISO 27032:2012

[8] Definición de ciberseguridad

Recomendación UIT-T X.1205

[9] An evaluation framework for Cyber Security Strategies

https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies/at_download/fullReport (Consultada el 19/05/2017)

[10] Ciberataques a Infraestructuras Críticas

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ES_NCSS.pdf (Consultada el 19/05/2017)

[11] Ataque de DDoS a Estonia

http://www.iar-gwu.org/node/65 (Consultada el 19/05/2017)

[12] Ataque con malware Stuxnet a Irán

https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf (Consultada el 19/05/2017)

[13] Ataque a servicio eléctrico de Ucrania

https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf (Consultada el 19/05/2017)

[14] Cronología de ciberataques

http://www.nato.int/docu/review/2013/Cyber/timeline/ES/index.htm (Consultada el 19/05/2017)

[15] ENISA - Resilience of Networks and Services and Critical Information Infrastructure Protection
https://www.enisa.europa.eu/activities/Resilience-and-CIIP (Consultada el 15/02/2016)

[16] NIST Computer Security Resource Center
http://csrc.nist.gov/ (Consultada el 20/02/2016)

[17] LACNIC – Proyecto Amparo
http://www.proyectoamparo.net/ (Consultada el 22/02/2016)

[18] Organización de Estados Americanos – Seguridad Cibernética https://www.sites.oas.org/cyber (Consultada el 25/02/2016)

[19] OEA - Estrategia Interamericana Integral http://www.innovacion.gob.pa/descargas/ESTRATEGIA%20INTERAMERICANA%20INTEGRAL.pdf (Consultada el 06/02/2017)

[20] ITU Cybersecurity http://www.itu.int/en/action/cybersecurity/Pages/default.aspx (Consultada el 27/02/2016)

[21] APEC TEL WORKING GROUP http://www.apectelwg.org/ (Consultada el 27/03/2016)

[22] Estrategia de ciberseguridad de España

http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf (Consultada el 27/04/2016)

[23] Estrategia de ciberseguridad de Estonia

https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf (Consultada el 28/04/2016)

[24] Actualización CONPES 3701

https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf (Consultada el 06/02/2017)

[25] Ciberseguridad en países de América Latina

http://www.segu-info.com.ar/articulos/116-proteger-infraestructuras-criticas.htm (Consultada el 06/02/2017)

[26] Methodologies for the identification of Critical Information Infrastructure assets and services

https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis (Consultada el 28/02/2017)

[27] Common Threats and Vulnerabilities of Critical Infrastructures

https://pdfs.semanticscholar.org/7098/a29a404f8561c7f3c66801b6e1f36f88b7b7.pdf (Consultada el 07/02/2017)

[28] Framework for Improving Critical Infrastructure Cybersecurity

https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (Consultada el 13/07/2017)

[29] AuditScripts CIS Controls v6.0 Mappings

http://www.auditscripts.com/free-resources/critical-security-controls/ (Consultada 13/07/2017)