ARTÍCULO PROFESIONAL DOI 10.52781/cmm.e008

Como la tecnología controla nuestra infraestructura crítica, los civiles y los militares trabajan juntos para minimizar los ataques cibernéticos

How technology is controlling our critical infrastructure, civilians and military working together to minimize cyberattacks

Resumen: El propósito de este artículo es analizar la influencia del desarrollo tecnológico y cómo este desarrollo aumenta los riesgos en nuestra infraestructura crítica. Cuando estudiamos nuestro Estado, miramos a nuestro alrededor y vemos cómo la tecnología está tomando el control de todos nuestros sistemas importantes y críticos. Por lo tanto, es necesario encontrar una manera de minimizar los ataques cibernéticos a través de todas las formas posibles que tiene nuestro estado, como las unidades cibernéticas militares, la legislación, los protocolos de acción, y la parte más importante: los civiles que trabajan en empresas privadas (bancos, hospitales, Compañía Eléctrica y otros). Este trabajo debe hacerlo con dos objetivos principales: primero, trabajar juntos como una asociación indivisible contra estas amenazas y, segundo, tratar de mantener seguros los sistemas que forman nuestra infraestructura crítica. Para desarrollar este tema, se utilizará el método descriptivo, y la información se recopila de trabajos importantes como la Política de Estrategia Nacional de Seguridad Cibernética (Guatemala, Mingob 2018), libros sobre terrorismo o ciberterrorismo y algunos sitios web que describen el diagnóstico de ataques cibernéticos y cómo estas unidades cibernéticas protegieron su infraestructura crítica.

Palabras Clave: Tecnología. Infraestructura crítica. Ataques cibernéticos.

Abstract: The purpose of this document is to analyze the influence of technological development and how that development increases the risks in our critical infrastructure. When we study our state, we look around and see how technology is taking control of all our important and critical systems. So, It is necessary to find the way of minimizing the cyberattacks through all the possible ways that our state has, such as, the military cyber units, legislation, protocols of act, and the most important part: the civilians that work in private companies (banks, hospitals, the electricity company, and others). This work should do this with two main objectives: first, working together as one indivisible partnership against those threats, and second, trying to maintain the systems that form our critical infrastructure safe and secure. To develop this topic, Will be used the descriptive method, and it is collected the information from important works, such as, The National Cyber Security Strategy Policy (Guatemala, Mingob 2018), books about terrorism or cyber terrorism and some web sites that describe diagnosis of cyber-attacks and how those cyber units have protected their critical infrastructure.

Keywords: Technology. Critical Infrastructure. Cyberattacks.

Aram Albert Jordan Sandoval
Ejército de Guatemala.
Cidade da Guatemala, Guatemala.
jordanaram15@gmail.com

Recibido: 06 de marzo de 2020
Aprobado: 10 de agosto de 2020

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

1 Introducción

Desde las últimas dos décadas, la tecnología se ha convertido en un eje transversal en el desarrollo humano. Las personas utilizan la tecnología en su trabajo diario, la ciencia, la medicina, la ingeniería y la educación, y muchos otros. Se ha convertido en una forma fácil de gestionar todos nuestros servicios en todo el mundo, bancos electrónicos, e-transportation internet de las cosas, y ahora estamos muy cómodos con eso. Estas instalaciones son nuestra infraestructura crítica (CARVALHO, 2016). Todos los países del mundo tienen uno, y tal vez la mayoría de ellos están interconectados entre sí.

Como Paul Shemella en su libro llamado "Fighting Back" explica algo sobre las motivaciones de los actos terroristas, será parafraseado en palabras comprensibles como, la mayoría de los países del primer Mundo se preocupan por cómo mantener sus sistemas seguros y protegidos. Han creado algunas instituciones públicas (unidades cibernéticas), que luchan por minimizar los ataques cibernéticos o luchan contra los hackers que pueden robar información crítica, por dinero, propiedad personal o, peor aún, desestabilizar un país o un grupo de países que tienen relaciones sólidas.

Para comenzar este trabajo, es necesario responder a esta pregunta: ¿Cómo pueden los civiles y los militares trabajar juntos estratégicamente para minimizar estos ataques cibernéticos? Durante el desarrollo de este artículo, es obligatorio averiguar cómo estos actores clave podrían trabajar como un equipo estratégico para combatir las amenazas transnacionales.

En la investigación sobre un nuevo mundo tecnológico, se descubrirá la importancia de las infraestructuras críticas, sus componentes y la importancia de mantener estas infraestructuras seguras para permitir a los ciudadanos contar con sistemas estables y fiables.

Es necesario encontrar una manera de trabajar juntos (civiles y militares) mediante la aplicación de estándares internacionales que incluyen monitoreo de infraestructura 24/7/365, evitando y minimizando ataques y detectando y respondiendo a estas amenazas transnacionales (protocolos de acción).

En este informe de investigación, el lector encontrará información sobre terminología cibernética, infraestructura crítica de generalidades y componentes, estándares internacionales y nacionales de instituciones que se han creado o mejorado, como el Equipo de Respuesta a Emergencias Informáticas (CERTS) [Computer Emergency Response Team] y el Equipo de Respuesta a Incidentes de Seguridad (CSIRTs)[Computer Security Incident Response Team], (URVIO, 2017), que muestran la forma ética de monitorear, combatir y responder a los ataques cibernéticos y cómo pueden afectar nuestra infraestructura crítica.

Además, esta investigación presenta estudios de caso de dos países que están luchando contra los ataques cibernéticos de la misma manera, y ambos están creando estrategias, leyes específicas sobre cibernética, evaluaciones de riesgo y una cultura de conciencia en sus sociedades con el fin de proteger su soberanía y el honor de su nación. Esta información será una fuente de estudio para minimizar los ataques cibernéticos y sobre cómo prevenir y combatir estos ataques cibernéticos.

Al final de esta investigación, se espera que civiles y militares trabajen como un equipo nacional para compartir experiencias y para que tengan una visión del país sobre las amenazas transnacionales como las amenazas cibernéticas. Al compartir estas experiencias, podrían trabajar en nuevas estrategias de defensa nacional.

2 Características generales

2.1 Defensa Cibernética: "La defensa cibernética es un mecanismo de defensa de redes informáticas que incluye respuestas a acciones y protección de infraestructura crítica y garantía de Información para organizaciones, entidades gubernamentales y otras posibles redes. La defensa cibernética se centra en prevenir, detectar y proporcionar respuestas oportunas a ataques o amenazas para que ninguna infraestructura o información sea manipulada" (CYBER..., 2019, n. p.), computer network defense (CND).

2.2 infraestructura crítica: "La infraestructura crítica es el conjunto de sistemas, redes y recursos que son tan esenciales que su funcionamiento continuo es necesario para garantizar seguridad de una nación dada, su economía y la salud y / o seguridad del público. Aunque la infraestructura crítica es similar en todas las naciones debido a los requisitos básicos de la vida, la infraestructura considerada crítica puede variar de acuerdo con las necesidades, los recursos y el nivel de desarrollo de una nación" (CRITICAL..., 2019, n. p.).

2.3 Ataque cibernético: "[...] es la explotación deliberada de sistemas informáticos, empresas y redes dependientes de la tecnología. Los ataques cibernéticos utilizan código malicioso para alterar el código informático, la lógica o los datos, lo que resulta en consecuencias perturbadoras que pueden comprometer los datos y dar lugar a delitos informáticos, como el robo de información y de identidad. [...] [e] también se conoce como un ataque a la red informática (computer network attack - CNA) (CYBERATTACK, 2019, n.p.).

2.4 Grupo de Respuesta a Emergencias Informáticas (CERT): "[...] es un grupo de expertos que responden a incidentes de ciberseguridad. Estos equipos se ocupan de la evolución de malware, virus y otros ataques cibernéticos (COMPUTER..., 2019a, n.p.).

2.5 Grupo de Respuesta a Incidentes de Seguridad (CSIRT): es un equipo que responde a los incidentes de seguridad informática cuando se producen. Un incidente puede ser una denegación de servicio o el descubrimiento de acceso no autorizado a un sistema informático (COMPUTER..., 2019b, n.p.).

3 Infraestructura crítica

3.1 Generalidades

El concepto de infraestructura comenzó en los años 80. Incluye servicios del sector público como ferrocarriles, puentes, aeropuertos, transporte público, instalaciones de suministro de agua y todos los recursos que los Estados tienen dentro de su territorio. Desempeñaron un papel importante en el desarrollo de todo el país. Proporcionaron lo que la población necesitaba porque en esta parte de la historia el gobierno tenía todo el poder del país. Sin embargo, el concepto cambió en los años 90 a un concepto de Seguridad Nacional, porque los ataques terroristas aumentaron dramáticamente.

La subsistencia de los países y el desarrollo de su población incluían la seguridad nacional, no sólo por el significado de la palabra, sino también porque necesitaban cerrar las brechas entre los ataques terroristas y la seguridad de su infraestructura crítica y estratégica, combinada con información crítica sobre su población y todos los bienes que tienen los Estados.

Son el núcleo de todos los países del mundo. Luego, después de los acontecimientos del 11 de septiembre, el concepto de infraestructura cambia de nuevo y, a pesar de los hechos, ahora aparece incluyendo la palabra "crítica" no solo para el sector público como en los años 80, sino para el nuevo concepto o la nueva forma de hablar de infraestructura.

Uno de los principales desafíos en este concepto es la resiliencia, porque esta palabra va más allá de su significado. Incluye la capacidad de estos países para dar a sus pueblos flexibilidad, adaptabilidad y muchas capacidades para cambiar o redefinir cómo reaccionar cuando la situación requiere este tipo de resiliencia.

Hoy en día, el concepto de infraestructura crítica se convierte en un gran desafío para todos los países del mundo, debido al aumento de la población, las necesidades de comunicación o para realizar más transacciones bancarias electrónicas, y la difusión de tecnología que podría tomar un papel importante en la vida humana, y se ha convertido en un eje transversal en la rutina diaria de todos.

Los estados invertirán mucho dinero en equipos modernos, políticas más estrictas y más capacitación para las personas que manejarán los nuevos sistemas que les ayudarán a mantener estos tres aspectos funcionando como un todo para evitar algo de phishing de información o para evitar algunas intrusiones del sistema.

Mientras tanto, todos los servicios nacionales (públicos y privados) funcionarían adecuadamente y darían a su población todos los materiales y la confianza que necesitan (O'ROURKE, 2007).

3.2 Componentes

Los componentes de infraestructura crítica dirigidos al sector público, el sector privado, los sistemas alimentarios, los sistemas de defensa industrial, los monumentos nacionales, los bancos, los sistemas financieros y muchos otros que participan activamente en todos los países.

Son vitales para un país a fin de proporcionar a su población todos los servicios básicos, manteniendo el proceso de globalización con otros países. Este concepto no es solo para ataques cibernéticos, sino también para desastres naturales, recesiones económicas, falta de servicios vitales o países débiles. Es necesario proteger y mantener seguras todas las partes de esta infraestructura, porque si falta una de ellas, el país colapsará a muy corto plazo (O'ROURKE, 2007).

Ahora, una de las necesidades más importantes es identificar la ubicación de nuestros recursos estratégicos porque representan los activos más valiosos del país. Estos recursos estratégicos se han convertido en una gran parte de la infraestructura crítica y es esencial monitorear, proteger e identificar dónde están y cuán grandes o útiles son. Debemos añadirlos al catálogo de infraestructura nacional.

4 Normas internacionales

La Organización Internacional de Normalización (ISO) desempeña un papel importante en la ciberseguridad y la defensa cibernética al presentar directrices sobre cómo administrar y cómo conectar la seguridad y la defensa. Se refiere a trabajar juntos, civiles y militares. Luego, estos países de todo el mundo necesitan trabajar duro como un equipo nacional para crear escenarios que ayuden y encuentren algunas estrategias nacionales y políticas nacionales para discutir algunos desafíos importantes juntos, los sectores público y privado. Estas normas se han convertido en herramientas invaluables para compartir información, conocimientos y experiencias que contribuyen a mantener segura la infraestructura crítica y a mantener la credibilidad en la tecnología. De esta manera, la población las utilizará de la mejor manera posible para dar un espectro muy claro de ciberseguridad y ciberdefensa.

Las siguientes normas presentarán una guía sobre cómo trabajar en este nuevo mundo cibernético.

4.1 ISO 27032

La ISO 27032 presenta algunas tecnologías de la información (TI), sobre técnicas de seguridad, con el fin de empoderar a un Estado en ciberseguridad, utilizando las técnicas más importantes y puntos estratégicos relacionados con la seguridad de las redes, la seguridad de Internet y la seguridad de las aplicaciones. Esta norma tiene por objeto garantizar el intercambio de información en la red para hacer frente a los delitos informáticos.

La primera área de esta guía aborda los problemas del ciberespacio y la ciberseguridad con el fin de cerrar las brechas en diferentes dominios del ciberespacio y dar orientación para abordar los riesgos comunes de ciberseguridad que incluyen ataques de ingeniería social, piratería, malware, spyware y otro nuevo software malicioso.

Esta guía técnica ha proporcionado algunas habilidades sobre cómo estar preparado para ataques de malware, detección y seguimiento de ataques, y respuestas a estos ataques.

La segunda esfera de interés es la más importante. Se llama "colaboración" porque es necesario ser eficaz y eficiente para compartir e intercambiar información y coordinar cómo se gestionarán los incidentes. Esta colaboración será segura y fiable con el fin de proteger la información de las partes interesadas. La norma incluye integración e interoperabilidad de sistemas en ambas direcciones (JUMBO VIVANCO, 2019).

4.2 ISO 31000

La ISO 31000, según (PALACIOS GUILLEM; GISBERT SOLER; PÉREZ BERNABEU, 2015) describe de manera exhaustiva el significado de gestión de riesgos. Por lo tanto, en este caso, es muy importante aprovechar el proceso de planificación o toma de decisiones, ya que estos Estados deben estar conscientes de los ataques cibernéticos, desastres naturales o cualquier ataque que desestabilice a los países.

Es necesario hacer algunas evaluaciones de riesgo en nuestra infraestructura crítica sin ninguna restricción, pero de manera paralela, es urgente tener un plan que asigne responsabilidades a todos los diferentes sectores incluidos y les proporcione posibles formas de prevenir, mitigar y recuperar diferentes tipos de ataques. También es importante darles la oportunidad de trabajar en el mismo equipo, militar y civil, con el fin de proteger la infraestructura y enfrentar los riesgos juntos, tratando de minimizar el daño, especialmente si se trata de un ciberataque, porque el daño podría ser inmediato y calamitoso. Las consecuencias serían peores, por ejemplo, si el ataque cibernético bloquea el suministro de energía o el sector bancario o provoca el colapso de infraestructuras críticas.

4.3 ISO 27005

Cuando uno de los objetivos principales es proteger la infraestructura crítica, se refiere a la gestión de los riesgos de seguridad de la información que presenta la ISO 27005. Ha sido un marco de referencia sobre la metodología entre la gestión de riesgos y la seguridad de la información, y proporciona cinco pasos importantes:

a) El plan interior y exterior
b) La definición del contexto organizacional (interior y exterior)
c) La valoración de los riesgos tecnológicos
d) El tratamiento de los riesgos tecnológicos
e) El monitoreo y un proceso de gestión de desarrollo continuo

En primer lugar, un plan de comunicación que se difundiría dentro y fuera de la infraestructura crítica del sector público y privado, y a través de este plan, determinar los riesgos y objetivos con el fin de presentar un resumen de los avances en el proceso. La mejor manera de difundir esta información sería utilizando material escrito y capacitando a las personas sobre estos aspectos.

Por otra parte, este plan de comunicación se elaboraría con el fin de crear conciencia y seguridad y, lo que es más importante, para poner de relieve la existencia de riesgos.

Este plan tendría tres aspectos diferentes a considerar: la comunicación primaria, que incluye conceptos generales, implicaciones y ventajas. A continuación, la comunicación en el camino. Este aspecto presenta avances en la gestión del riesgo para tener feedback y apoyo de las personas que están trabajando en el riesgo. Y finalmente, comunicaciones de resultados que intentarán compartir y difundir la información lograda a través de este plan.

La segunda etapa de la gestión del riesgo es un contexto organizacional que integra misión, visión, políticas, estrategias, funciones y responsabilidades. La importancia de este contexto es el orden en que se protegerá la infraestructura crítica cuando llegue un ataque cibernético, y encontrar las limitaciones para proteger todos los sistemas de información, y cómo un equipo nacional de respuesta aceptaría el nivel de riesgo y, de esta manera, determinaría el alcance y las limitaciones que tiene la infraestructura crítica.

El tercer aspecto es la valoración del riesgo tecnológico. En esta etapa, se podrían identificar los activos de información nacionales y de esta manera determinar cuál es el más importante

que debe protegerse. También puede establecer las amenazas a las que está expuesta la infraestructura crítica para mitigar los riesgos. Esta valoración puede ser de adquisición de costos, renovación, recuperación o mantenimiento. Por otro lado, es necesario identificar amenazas críticas de infraestructura que puedan ser físicas, lógicas o estratégicas, y según su origen: natural, técnico, accidental o intencional. Esto ayudaría a identificar los riesgos de estas amenazas y determinar el impacto en todas las partes interesadas.

El cuarto aspecto es cómo hacer frente a los riesgos tecnológicos, porque en esta fase es necesaria una evaluación de los daños para mitigar los riesgos y los daños colaterales. Esta acción podría utilizarse para reducir, aceptar y eliminar el daño.

Este plan necesita definir políticas y directrices y crear una unidad de comando y control para realizar tareas de recuperación y llevar la infraestructura crítica a su estado normal. De esta manera, todos los servicios y la confianza serían devueltos a las partes interesadas.

Y por último, la mejora continua. Con esto, se pueden crear controles de cambio de activos, procesos, vulnerabilidades, amenazas y políticas con el fin de establecer las siguientes acciones y mantener actualizada la gestión, con el fin de evaluar los indicadores de acuerdo con los que aparecen en los planes exteriores o interiores (RAMÍREZ CASTRO; ORTIZ BAYONA, 2011).

5 Protección de la infraestructura crítica-estudios de caso: república federativa de Brasil y república de Guatemala

5.1 Estrategia Nacional de Ciberseguridad de Guatemala

Hablando de Guatemala, en 2018, el Ministerio del Interior publicó la Estrategia Nacional de Ciberseguridad con el fin de proporcionar las directrices de las instituciones gubernamentales sobre un tema que solo el Ministerio de Defensa y el Ministerio del Interior han abordado. Es necesario informar al resto del Estado sobre los crecientes problemas de seguridad nacional para crear conciencia social y la responsabilidad que tienen estas instituciones como servidores públicos. También es importante informar a la población guatemalteca sobre los problemas de seguridad nacional que debe combatir y cómo abordarlos.

La estrategia nacional de ciberseguridad, como se menciona en el resumen de esta investigación (GUATEMALA, 2018), incluye:

a) Infraestructura crítica
b) Tecnologías de la información y las comunicaciones
c) Investigación y respuesta ante incidentes cibernéticos
d) Marco legal
e) Gobernanza
f) Misión, visión, objetivos y otros

En primer lugar, esta nueva estrategia se refiere a la Organización de los Estados Americanos (OEA) en su resolución AG / RES 2004 "*Adopción de una estrategia global interamericana para combatir las amenazas de ciberseguridad: un enfoque Multidimensional y Multidisciplinario para crear una cultura de ciberseguridad*". Esta resolución es la punta de lanza del modelo guatemalteco de estrategia de ciberseguridad. Esta estrategia dice literalmente en sus primeros cinco puntos de resolución:

> 1. Adoptar la Estrategia Interamericana de Ciberseguridad Global: un enfoque Multidimensional y Multidisciplinario para crear una cultura de ciberseguridad, adjunto a como Apéndice A.
> 2. Instar a los Estados miembros a que apliquen esta estrategia.
> 3. Instar a los Estados miembros a que establezcan o identifiquen grupos nacionales de "alerta, vigilancia y alerta", también conocidos como "Grupos de Respuesta a Incidentes de Seguridad" (CSIRTs).
> 4. Poner un énfasis renovado en la importancia de lograr sistemas de información seguros en Internet en todo el hemisferio.
> 5. Solicitar al Consejo Permanente, a través de la Comisión de Seguridad Hemisférica, que continúe abordando este tema y a fin de facilitar la coordinación de los esfuerzos en la implementación de la Estrategia, y en particular, los esfuerzos de los expertos del gobierno, el Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL), el Grupo de Expertos Gubernamentales en Delito Cibernético de la Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas (REMJA) y los demás órganos de la OEA, (ORGANIZATION OF AMERICAN STATES, 2004, n. p., enfásis añadida).

Esta resolución de la OEA proporciona directrices sobre cómo América Latina está abordando los problemas de ciberseguridad con una perspectiva multidimensional y multidisciplinaria con el fin de crear una cultura cibernética en los países que forman parte de ella. Esta organización está alentando a los países latinos a implementar esta estrategia como su estrategia nacional con el fin de crear estándares regionales de ciberseguridad. Estos países tienen su propia forma de detectar, prevenir y responder a cualquier ataque cibernético, pero no tienen una estrategia común que les permita trabajar juntos de manera multidimensional. La OEA alienta a estos países a establecer e identificar Grupos de Respuesta a Emergencias Informáticas (CERTs) y Grupos de Respuesta a Incidentes de Seguridad (CSIRTs) con el fin de integrar todos estos equipos nacionales, regionales e internacionales como un equipo grande. Estos equipos tendrán una relación de confianza especial en la forma de compartir información vital contra un ataque cibernético. Finalmente, el Comité Interamericano Contra el Terrorismo (CICTE) trabajará como coordinador de esta estrategia, mientras que los demás departamentos de la OEA participarán en la estrategia cuando sea necesario.

Esta estrategia es de la mayor importancia para el modelo guatemalteco de ciberseguridad, porque las amenazas transnacionales y los ataques cibernéticos evolucionan, y las actividades

electrónicas diarias participan en la zona digital, y los sistemas nacionales están interconectados. Será necesario contar con una estrategia que brinde a todos los sectores guatemaltecos la oportunidad de crear marcos técnicos y legales para fortalecer la ciberseguridad nacional y global. Esta estrategia presenta un componente importante y de gran valor, la resiliencia. Será necesario restablecer lo antes posible todos los servicios, evitando con esta recuperación, la pérdida de información y daños colaterales con el fin de proteger el activo más valioso del país, su población.

Esta estrategia fue creada al inicio de un proceso que involucró a más de un centenar de factores clave nacionales y regionales de los diferentes sectores de la sociedad guatemalteca (militar y civil) de acuerdo con el Plan Estratégico de Seguridad Nacional (2016-2020), la agenda Nacional de riesgos y amenazas y la agenda estratégica de seguridad de la nación. Esta estrategia analiza el escenario que Guatemala necesita para mitigar los riesgos y amenazas que provienen del ciberespacio.

Los objetivos que muestra esta estrategia están orientados a fortalecer las capacidades y protocolos de acción de las instituciones que forman parte del sistema de seguridad nacional en Guatemala, asignándoles responsabilidades para actuar sobre la base de un marco jurídico con el fin de mantener el estado de derecho en Guatemala.

Guatemala está involucrada en hitos internacionales que regulan la cooperación en materia de infraestructura crítica y, por supuesto, están liderados por Estados Unidos, que es el primer país en crear un documento relacionado con la protección de la infraestructura crítica. Este documento explica la necesidad de crear un comité. Este comité evaluaría las vulnerabilidades de los ataques terroristas con el fin de proteger esta infraestructura en una dimensión transnacional. Guatemala tiene muchas infraestructuras públicas y otras del sector privado, pero no hay manera de articularlas todas y cómo trabajar con las mejores prácticas en procedimientos de seguridad de la información.

Como corolario de esta estrategia, Guatemala creó dos cosas después de publicar esto. El primero fue un comité técnico que incluye al sector gubernamental, el sector privado, las academias, las infraestructuras críticas, el sector financiero y el sector de TI, con el fin de fortalecer las relaciones de colaboración, cooperación y coordinación entre ellos, promoviendo análisis e iniciativas que aumenten el ecosistema de ciberseguridad en Guatemala.

El segundo, según el acuerdo del gobierno guatemalteco 65-2019, el Comando de Informática y Tecnología fue creado por el Ministerio de Defensa. Este comando es responsable de coordinar todos los temas de defensa cibernética, trabajando con las instituciones nacionales e internacionales que manejan estos temas y formando parte de este esfuerzo nacional e internacional.

5.2 Amenazas cibernéticas brasileñas

En 2005, después de un largo tiempo sin una política de defensa en Brasil, el gobierno brasileño emitió un Plan de Defensa Nacional (PND). El objetivo principal de este plan es crear conciencia en todos los sectores del país para defender a la nación, y establecer la importancia estratégica del sector cibernético. Este sector debería ser más fuerte porque Brasil tiene

muchos sistemas con vulnerabilidades y necesitan crear más capacidades para evitar estas vulnerabilidades y recuperar, lo antes posible, todas sus TICs (tecnologías de la información y comunicación). Este plan incluye todas las acciones de seguridad de la infraestructura crítica y aplica todos los dispositivos y procedimientos que ayudan a reducir o minimizar las vulnerabilidades cuando afectan a sus sistemas de defensa nacional de ataques cibernéticos. Hay instituciones a cargo de este importante desafío. Estas instituciones son: la Casa Civil o Presidencia, el Ministerio de Defensa, el Ministerio de Comunicaciones, el Ministerio de Ciencia y Tecnología y la Oficina de Seguridad Institucional (AMARAL, 2014).

La información anterior es prueba de que el gobierno brasileño está trabajando con civiles y militares, a través de su política estratégica nacional, para proteger los sistemas de defensa de ataques cibernéticos, y este trabajo incluye la protección de su infraestructura crítica.

El plan está poniendo a todos los sectores nacionales en la misma dirección, ya sean privados o públicos, y generarán más capacidades para obtener mucho conocimiento cibernético. Están siendo entrenados para prevenir, proteger y responder a cualquier amenaza nacional o internacional que pueda llevar a Brasil a una situación crítica que podría causar la pérdida de su hegemonía y liderazgo en ciberseguridad y defensa cibernética en América del Sur.

La Oficina de Seguridad Institucional desarrolló en 2010 el Libro Verde sobre Ciberseguridad, con el objetivo principal de crear un entorno de ciberseguridad para proteger a la sociedad brasileña y a la nación. Este libro verde se hizo para abordar los nuevos retos y las agendas mutuas en el sector privado, público, las academias y el "tercer sector" refiriéndose a las instituciones privadas, pero sin ánimo de lucro según (what is the third sector) (¿QUÉ ES..., 2018)?

Es un esfuerzo conjunto de civiles y militares para crear un pensamiento común y construir juntos las directrices de ciberseguridad con estos vectores: político-estratégico, económico, medio ambiente, comunicaciones, tecnología, educación, marco legal, cooperación internacional, transporte, suministro de agua, financiamiento y suministro de energía, y cuando estos vectores se ubican en la misma olla, crean su infraestructura crítica.

Lo más importante para el sector cibernético fue asignar esta enorme responsabilidad a una fuerza armada a través del Ministerio de Defensa, y después de eso, crearon un Comando de Defensa Cibernética. Esta unidad tiene la misión de contribuir a aumentar el nivel de ciberseguridad. Esta unidad Cibernética tiene el conocimiento para trabajar con diferentes sectores y con la sociedad brasileña. Esta unidad militar está tratando de centrarse en la creación de recursos humanos, la doctrina y la aplicación de la seguridad con el objetivo de ofrecer a la población una respuesta rápida a los incidentes, las lecciones aprendidas y la protección contra los ataques cibernéticos (AMARAL, 2014).

En 2012, el Ministerio de Defensa publicó un documento que contenía una nueva política de defensa cibernética. Ella estableció la manera de ejecutar un sistema de defensa cibernética militar. Este documento fue escrito para definir las tareas de la fuerza armada con el fin de evitar que Internet y otras redes de uso delictivo, y para proteger todos los datos de información y comunicaciones esenciales. Con esta política, el ejército brasileño fue entrenado y se hizo cargo de todo el control cibernético en todo el país. Este control incluye la responsabilidad de reunir a todos los sectores dándoles sus propios deberes en este tema de seguridad nacional.

También incluyó instrucciones sobre cómo compartir información, protocolos de acción y la forma inmediata de responder en caso de un ataque cibernético, construyendo con este control relaciones confiables entre estos sectores y el ejército para dar la primera alerta nacional y hacer continuar el plan de ciberseguridad.

Inmediatamente después de un ataque cibernético, un equipo nacional de respuesta se pondrá en contacto con todos sus miembros para proporcionar información específica del campo con el fin de encontrarlos lo antes posible, dependiendo del tipo del ataque cibernético, la ubicación de los eventos, los daños mayores y determinar cuáles podrían ser las primeras decisiones a tomar. Uno de los principales desafíos es mitigar el daño y tratar de resolver el problema de inmediato. Con esta reacción, la unidad de defensa cibernética se coordinará con otras instituciones que tienen la responsabilidad de investigar y criminalizar este ataque de acuerdo con su marco legal.

Esta breve descripción explica las primeras acciones contra un ataque cibernético, cómo activar el plan de ciberseguridad, y cómo criminalizar el cibercrimen si existe, o si este ataque es parte de un problema de ciberterrorismo, con el fin de alertar a los países vecinos brasileños o países de todo el mundo.

Hoy en día, Brasil tiene un paso por delante en comparación con sus vecinos. Está muy cerca de consolidar su sistema de ciberseguridad y defensa cibernética del más alto nivel político, con cobertura nacional, representado por la Oficina de Seguridad Nacional, la Administración Pública Federal y el Ministerio de Defensa, que construye el vínculo político-estratégico, a los niveles más bajos de unidades del ejército. Estas unidades trabajan a nivel operativo y táctico en el sistema de ciberseguridad y ciberdefensa, incluyendo en este nivel a civiles que trabajan a nivel medio y bajo en todo tipo de sectores con el fin de defender sus intereses cibernéticos nacionales.

En el sistema de ciberseguridad y defensa cibernética, la oficina mencionada en el último párrafo tiene la tarea de coordinar todas las acciones que afectan a la sociedad, por ejemplo, las cuestiones de ciberseguridad, información y comunicación, y la seguridad nacional de las infraestructuras críticas.

El Ministerio de Defensa supervisa todos los asuntos relacionados con la defensa cibernética y ha recibido las siguientes órdenes:

(a) nivel estratégico: El Ministerio de Defensa será responsable de crear protocolos que les permitan formar parte del marco legal de acuerdo con sus leyes nacionales y sus acuerdos internacionales de acciones que los involucren en situaciones de crisis o conflictos armados y operaciones de mantenimiento de la paz.

(b) nivel Operacional: Aquí, el Ministerio de Defensa, como todos los ejércitos del mundo, debe estar preparado para llevar a cabo operaciones militares defensivas u ofensivas con el fin de preservar su soberanía y el honor de la nación. En este concepto, el Ejército brasileño también incluye todos los problemas que afectan su entorno cibernético (AMARAL, 2014).

Con esta importante política, el Ministerio de Defensa y el Ejército Brasileño están tomando el control de toda la infraestructura crítica en todo el país. Son el vínculo entre las instituciones nacionales y las empresas privadas que se interconectan e intercambian información

clasificada de personas que viven en Brasil o personas que realizan transacciones electrónicas, dentro o fuera de las fronteras brasileñas. Esperan que el gobierno brasileño les proporcione un alto nivel de seguridad de sus informaciones personales para no sean blancos de un ataque cibernético, o para que no tengan sus informaciones robadas (phishing), o para no sean víctimas de extorsión del crimen organizado.

El nivel de seguridad debe ofrecerse a estas personas con el fin de aumentar los inversores extranjeros y hacer que el entorno empresarial sea más fiable. De esta manera, el comercio internacional brasileño será más confiable.

Por otro lado, el gobierno brasileño tiene una infraestructura crítica más fuerte para conservar sus recursos naturales en lugares seguros y también protege sus áreas estratégicas.

Hoy en día, estas áreas estratégicas están siendo afectadas por el crimen organizado y las amenazas transnacionales que necesitan contar con estas áreas para aumentar su riqueza.

Es por eso que el equipo de seguridad nacional y el equipo de defensa nacional, combinando sus recursos y capacidades, necesitan trabajar juntos para ser más poderosos, y de esta manera, detectarán, prevendrán y responderán a todos los actos que puedan afectar su infraestructura nacional crítica y los sistemas que administran esa infraestructura.

6 Conclusiones

Para sacar conclusiones, es obligatorio considerar cómo la tecnología se está convirtiendo en una parte importante de la vida de las personas en todo el mundo. La tecnología ha aumentado más del 50% de todos los hallazgos durante el último siglo. Ayuda en todas las actividades diarias como eje transversal en ciencia, tareas domésticas, acciones militares y muchas otras que incluyen infraestructura crítica en todos los países.

Los seres humanos han encontrado un conjunto de cosas que han hecho sus actividades e incluso sus vidas más fáciles con el fin de ganar más tiempo para hacer otras actividades. Es por eso que estas actividades son el alcance de esta investigación porque necesitan una forma de proporcionar más herramientas tecnológicas a personas de todo el mundo. Los desarrolladores de software y hardware o las empresas que administraban los sistemas no se dieron cuenta de lo peligrosos que eran estos hallazgos no solo por las herramientas, sino también por la forma en que las personas usan estas herramientas.

El desarrollo tecnológico debe continuar, además de ello, con un gran componente de seguridad a fin de proporcionar conexiones fiables y mantener el nivel de seguridad nacional al más alto nivel en todos los países y la seguridad colectiva en su región.

Después de decir esto, es necesario referirse a los gobiernos que han creado muchas instituciones que tienen la responsabilidad de establecer pautas para proporcionar ciberseguridad para asuntos internos, y equipos de ciberdefensa para resolver problemas internos, externos, regionales y continentales. Estas instituciones están combinando sus mejores esfuerzos para trabajar juntas, civiles y militares, y ahora el nuevo desafío es trabajar con muchas agencias diferentes no solo para compartir información, sino también para construir una estrategia común para combatir y minimizar los ataques cibernéticos. Estos ataques pueden afectar la estabilidad de

todo el país y, por lo tanto, la estabilidad de cualquier región, ya que la mayoría de sus sistemas están interconectados para proporcionar servicios de banca electrónica, operaciones financieras, suministro de luz eléctrica y muchos otros, por ejemplo, que deben garantizarse a través de un nivel de seguridad nacional, y como parte del gobierno, esto debe hacerse dentro del país.

Además, es necesario hablar de los equipos de seguridad nacional que juegan un papel importante en este tema de seguridad, porque el Grupo de Respuesta a Emergencias Informáticas y el Grupo de Respuesta a Incidentes de Seguridad son herramientas estratégicas para los gobiernos. Son la primera línea de defensa cuando ocurre un ataque cibernético. Estos grupos tienen la capacidad de combatir un ataque o muchos ataques con el fin de prevenir, combatir y responder a las tareas para las que están entrenados.

Estos grupos trabajan juntos en los sectores público y privado. Aprovechando su experiencia, mitigarán los daños colaterales después de un ataque en cualquier área de infraestructura crítica, y tienen la responsabilidad de detener el ataque, y también la responsabilidad de llevar las cosas a un estado normal en un período mínimo de tiempo. Estos fueron los objetivos más importantes cuando se crearon estos grupos.

Por otro lado, los grupos que están creando estándares internacionales deben ser tomados en cuenta para seguir las reglas de evaluación de riesgos que son una parte importante de este instrumento, porque, antes de estas evaluaciones de riesgo, estos gobiernos no sabían cuáles eran sus amenazas, o cómo se componía la infraestructura crítica, o cuál era su nivel de seguridad nacional. Después de realizar evaluaciones de riesgos, las normas internacionales les brindan una guía precisa para elaborar un plan estratégico sobre cómo prevenir, combatir y responder a un ataque cibernético, y cómo recuperar la estabilidad después del ocurrido.

Cuando se trata de infraestructura crítica, no se puede eliminar sus componentes. Estos componentes son la razón de la nación y sus participantes, porque no tienen riesgo por separado, pero cuando trabajan juntos, como un engranaje en un país, se convierten en una infraestructura importante que necesita ser protegida para proporcionar en primer lugar confianza para las personas y también confianza para una región con el fin de invertir y aumentar las transacciones tecnológicas en el comercio, las finanzas, la banca y otros aspectos. Como se demuestra en el cuerpo de esta investigación, cada país tiene su propia infraestructura crítica, pero en algún momento, estos países necesitan estar interconectados con los sistemas de otros países y, de esta manera, se convierte en un objetivo a proteger por la seguridad colectiva.

Es importante decir que es necesario revisar periódicamente el plan de infraestructura crítica para que el nivel político-estratégico del país mantenga el control sobre qué instituciones se han creado, y verifique si necesitan ingresar a su infraestructura crítica y, de esta manera, puedan mantener actualizado su plan de evaluación de riesgos.

Para seguir el orden lógico en esta investigación, se han incluido dos países que tienen casi los mismos problemas y los mismos esfuerzos para combatir los ataques cibernéticos. Estos países son la República de Guatemala y la República Federativa del Brasil. Cada uno de ellos tiene problemas, pero está asumiendo la difícil tarea de trabajar juntos, civiles y militares, sectores privados y públicos, como un equipo contra los problemas que necesitan combatir.

Están trabajando juntos en el trabajo interinstitucional con el fin de minimizar los ataques cibernéticos mediante la protección de su infraestructura crítica.

Al final de esta investigación, es necesario resaltar la necesidad de que los países proporcionen una estrategia especial para trabajar juntos contra las amenazas cibernéticas, pero también es necesario crear una cultura de conciencia en todas las sociedades, porque las personas son los ojos de la nación en las calles y en las redes sociales. Dado que las personas y las redes sociales están en contacto todos los días, podrían proporcionar información importante para impulsar los Sistemas Nacionales de Inteligencia. Todos los países deben investigar a fondo a las personas que administran los sistemas de infraestructura crítica para tener equipos con un alto nivel de confidencialidad, honestidad y transparencia.

Referencias

AMARAL, A. C. La amenaza cibernética para la seguridad y defensa de Brasil. **Revista Visión Conjunta**, Buenos Aires, n. 10, p. 19-22, 2014. Disponible en: http://cefadigital.edu.ar/bitstream/1847939/32/3/VC%2010-2014%20AMARAL.pdf. Accesado el: 19 de abril de 2020.

CARVALHO, P. S. M. de. A defesa cibernética e as infraestruturas críticas nacionais. In: EXÉRCITO. Comando Militar do Sul. Núcleo de Estudos Estratégicos. **Biblioteca do NEE**. Porto Alegre: Núcleo de Estudos Estratégicos, 2016. Disponible en: http://www.nee.cms.eb.mil.br/attachments/article/101/cibernetica.pdf. Accesado el: 19 de abril de 2020.

COMPUTER emergency response team (CERT). In: TECHNOPEDIA. Dictionary. **Cybersecurity**. Edmonton: Techopedia Inc., 2019a. Disponible en: https://www.techopedia.com/definition/31003/computer-emergency-response-team-cert. Accesado el: 10 de noviembre de 2019.

COMPUTER security incident response team (CSIRT). In: TECHNOPEDIA. Dictionary. **Cybersecurity**. Edmonton: Techopedia Inc., 2019b. Disponible en: https://www.techopedia.com/definition/24837/computer-security-incident- equipo de respuesta-csirt. Accesado el: 10 de noviembre de 2019.

CYBER defense. In: TECHNOPEDIA. Dictionary. **Cybersecurity**. Edmonton: Techopedia Inc., 2019. Disponible en: https://www.techopedia.com/definition/6705/cyber-defense. Accesado el: 10 de noviembre de 2019.

CYBERATTACK. In: TECHNOPEDIA. Dictionary. **Cybersecurity**. Edmonton: Techopedia Inc., 2019. Disponible en: https://www.techopedia.com/definition/24748/cyberattack. Accesado el: 10 de noviembre de 2019.

Infraestructura crítica. In: WHATLS.COM. Newton, MA: Tech Target, 2019. Disponible en: https://whatis.techtarget.com/definition/critical-infrastructure. Accesado el: 10 de noviembre de 2019.

GUATEMALA. Ministerio de Gobernación. **Estrategia nacional de seguridad cibernética**. Guatemala de la Asunción: Ministerio de Gobernación, mar 2018. E-book. (Documento técnico, n. 1). Disponible en: https://uip.mingob.gob.gt/wp-content/uploads/2019/03/Estrategia-Nacional-de-Seguridad-Cibern%C3%A9tica.pdf. Accesado el: 19 de abril de 2020.

JUMBO VIVANCO, P. L. **Implementación de un siem para el comando de ciberdefensa utilizando herramientas de código abierto bajo el estándar ISO 27032**. 2019. Thesis (Ingeniero en Sistemas Informáticos) – Universidad Tecnlógica Israel, Quito, Ecuador, 2019. Disponible en: http://repositorio.uisrael.edu.ec/bitstream/47000/2000/1/UISRAEL-EC-SIS-378.242-2019-033.pdf. Accesado el: 19 de abril de 2020.

O'ROURKE, T. D. Critical infrastructure, interdependencies, and resilience. **The Bridge**, Washington, DC, v. 37, n. 1, p. 22-29, 2007.

ORGANIZATION OF AMERICAN STATES. The General Assembly. **AG/RES 2004 (XXXIV-O/04)**: Adoption of a comprehensive inter-american strategy to combat threats to cybersecurity: a multidimensional and multidisciplinary approach to creating a culture of cybersecurity. [Washington, DC]: June 8, 2004. (Adopted at the fourth plenary session held on June 8, 2004). Disponible en: https://2009-2017.state.gov/p/wha/rls/59284.htm. Accesado el: 22 de abril de 2020.

PALACIOS GUILLEM, M.; GISBERT SOLER, V.; PÉREZ BERNABEU, E. Sistemas de gestión de la calidad: lean manufacturing, kaizen, gestión de riesgos (UNE-ISO 31000) e ISO 9001. **3C Tecnología**: Glosas de Innovación Aplicadas a La Pyme, [Alicante], v. 4, n. 4, p. 175-188, 2015. Disponible en: https://ojs.3ciencias.com/index.php/3c-tecnologia/article/view/324. Accesado el: 22 de abril de 2020.

¿QUE ES el tercer sector?. In: AYUDA EN ACCION, Madrid, 7 feb 2018. Disponible en: https://ayudaenaccion.org/ong/blog/solidaridad/que-es-el-tercer-sector/. Accesado el: 19 de noviembre de 2019.

SHEMELLA, P. (ed.). **Fighting back**: what government can do about terrorism. California: Stanford University Press, 2011.

RAMIREZ CASTRO, A.; ORTIZ BAYONA, Z. Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. **Ingeniería**, Bogotá, v. 16, n. 2, p. 56-66, Jul/Dic 2011. Disponible en: https://revistas.udistrital.edu.co/index.php/reving/article/view/3833. Accesado el: 26 de abril de 2021.

URVIO: Revista Latinoamericana de Estudios de Seguridad. Quito, Ecuador: FLACSO, n. 20, jun./nov. 2017. Disponible en: https://revistas.flacsoandes.edu.ec/urvio/issue/view/150. Accesado el: 19 de abril de 2020.