"INFRAESTRUCTURAS CRITICAS Y CIBERSEGURIDAD EN LAS FUERZAS ARMADAS DOMINICANAS"

Critical Infrastructures and Cyber Security in the Dominican Armed Forces

Recibido: 02 / 09 / 2019 Aprobado: 31 / 10 / 2019

Coronel
Nelton Baralt Blanco
Ejército de República Dominicana

El autor es Coronel del Ejército República Dominicana es Doctorando en Métodos de Investigación en Ciencias de la Educación en la Universidad de Cordova, España, tiene una Maestría en Seguridad y Defensa de la Universidad Antonio de Nebrija, España, una Maestría en Defensa y Seguridad Nacional de la Universidad Nacional para la Defensa (UNADE), Escuela de Altos Estudios, un Máster Internacional en Gestión Universitaria de la Universidad de Alcalá de Henares, España, Especialidad en Comando y Estado Mayor del Instituto Militar de Estudios Superiores, Licenciado en Administración de Empresas, UTESA, Oficial de Infantería (Cadete) en la Academia Aérea "Gral.de Brigada Piloto Frank Feliz Miranda – FARD, Curso Superior de DDHH y DIH, Instituto Militar de DDHH y DIH, Curso de Altos Estudios Estratégicos para oficiales Iberoamericanos, España; entre otros. Actualmente es el Director de la Escuela de Graduados de Altos Estudios Estratégicos (EGAEE). Escritor de la unidad I: La Inteligencia Militar. (Libro "Inteligencia Aplicada a la Seguridad del SIGLO XXI" julio 2016) con la Universidad Nebrija/INSUDE. neltonbaralt@egae.mil.do, nelton.baralt@gmail.com

RESUMEN

La seguridad siempre ha sido el aspecto clave en la existencia del hombre a partir del uso de la razón y su capacidad cognitiva, como forma de enfrentar las amenazas. El surgimiento de la tecnología como forma de simplificar procesos complejos y ayudar en la solución de problemas cotidianos también trajo consigo el paso de maquinarias inmensas hasta llegar a procesadores minúsculos con capacidad de desarrollar infinidad de operaciones.

Hoy en día la dependencia a los sistemas computarizados hace pensar que resultaría imposible desarrollar actividad alguna actividad por simple que parezca. Es por esto por lo que la exposición a los entornos virtuales ha aumentado el número de amenazas de carácter cibernético en los entornos industriales, laborales o hasta de la vida privada, abriendo nuevos debates en cuanto a la seguridad cibernética entre la exposición o el riesgo asumido.

La misma facilidad con la que se puede acceder a cualquier sistema en tiempo real y sin importar la distancia, también es la misma vía utilizada por ciberdelincuentes, criminales o terroristas para poder acceder a infraestructuras y sistemas consideradas críticas, como forma de emprender acciones en su beneficio o para causar daños, sin que se requiera para ello, equipos de cómputos sofisticados.

La misión de las Fuerzas Armadas de República Dominicana, consagrada por la Constitución, establece que además del resguardo de las fronteras y los intereses de la nación, implica en este nuevo espacio virtual un nuevo escenario donde seguramente se desarrollaran los nuevos combates del futuro. Se requiere entonces repensar las acciones, roles y misiones y por qué no mejorar la capacidad de respuesta ante estos eventos, dada la dependencia en materia de Tecnología de Información y Comunicación, de los sistemas de defensa nacional.

La creación de centros de atención a emergencias o incidentes cibernéticos, mejor conocidos como CERT o CSIRT, para el sector defensa es forma parte de las agendas nacionales e internacionales, como forma de responder de manera oportuna a las amenazas del entorno ciber, y dotar de las capacidades de resiliencia que permitan restaurar los sistemas en el menor tiempo y con el menor nivel de daño.

Palabras clave:
Amenaza, CERT, CSIRT, ciberseguridad, infraestructura critica, riesgo, seguridad, vulnerabilidad.

ABSTRACT

Safety has always been the key aspect of man's existence from the use of reason and cognitive ability, as a way to deal with threats. The emergence of technology as a way of simplifying complex processes and assisting in the solution of everyday problems also led to from huge machinery to small microprocessors with the ability to develop innumerable Operations.

Today, dependence on computer systems suggests that it would be impossible to develop any activity, however simple it may seem. This is why exposure to virtual environments has increased the number of cyber threats in industrial, work or even private life environments, opening up new debates on cybersecurity between exposure and risk assumed.

The same facility with which you can access any system in real time and regardless of distance, is also the same path used by cybercriminals, criminals or terrorists to be able to access infrastructures and systems considered critical, such as how to take action to your advantage or to cause damage, without requiring sophisticated computing equipment.

The mission of Dominican Republic Armed Forces established in the Constitution, states that in addition to the safeguarding of borders and interests of the nation, it implies in this new virtual space a new scenario where the new fights of the future. It is then necessary to rethink actions, roles and missions and why not, improve the responsiveness to these events, given the dependence on Information and Communication Technology, on national defense systems.

The creation of Cyber Incident or Emergency Care Centers, better known as CERT or CSIRT, for the defense sector is part of national and international agendas, as a way of responding in a timely manner to cyber environment threats, and provide resiliency capabilities to restore systems in the shortest time and with the lowest level of damage.

Keywords:
Threat, CERT, CSIRT, cybersecurity, critical infrastructure, risk, security, vulnerability.

INTRODUCCIÓN

Desde el origen de la humanidad y a partir de lo señalado como la revolución cognitiva donde los seres humanos mediante un proceso de transformación orgánica pudieron diferenciarse del resto de los organismos vivientes en la tierra, surgió como base de este entendimiento la necesidad de sentirse seguros ante las agresiones del ambiente y otros animales, iniciando desde allí nuevas capacidades para enfrentarlas. Esta necesidad de estar seguros para garantizar su propia existencia se ha mantenido hasta nuestros días.

Al hablar de la seguridad en términos integrales, pueden ser asociados algunos conceptos relacionados como: "La ausencia de amenazas", "La reducción del riesgo", o la "reducción de los factores que se asocian a una vulnerabilidad" asumiendo esta última como cualquier persona, actividad o cosa que puede causar un daño.

En estos contextos, la seguridad se asocia a una sensación que, si bien es cierto que se relaciona con el riesgo, las amenazas y la vulnerabilidad, no es menos importante considerar que influyen factores internos en los individuos que valoran indistintamente la sensación de que algo puede afectarlos. Es posiblemente el instinto de supervivencia, lo que más nos ha impulsado a actuar, ante determinadas agresiones, y es por esto por lo que el hombre en sociedad se ha unido para reclamar las garantías que les hagan ser más seguro.

Este enfoque tradicional de la seguridad está relacionado con la propia naturaleza de las fuerzas militares, que en ámbitos de la defensa ha sentado las bases de los planteamientos para generar entornos seguros estableciendo controles de seguridad perimétrica, así como por la fortificación de instalaciones y estructuras como forma de brindar a la sociedad una sensación de seguridad que permita el desarrollo humano.

El diccionario de la Real Academia Española establece que el término Seguridad proviene del latín securĭtas, -ātis, y se asocia a la cualidad de seguro o a la ausencia de amenazas, mientras que el término ciber proviene del inglés cyber-, acort. de cybernetic 'cibernético', y se asocia a las redes informáticas (RAE, 2019), por lo que pudiéramos asociar ambos conceptos y expresar que la Ciberseguridad se refiere a la seguridad en las redes informáticas.
Este modelo tradicional de la seguridad debió transformarse en el momento en que la implementación de medios tecnológicos y la cada vez más marcada influencia de la tecnología en los sistemas funcionales se hizo evidente, complejizo este aspecto al visualizar un mundo físico y su tránsito hacia un mundo lógico, logrando un puente imaginario entre lo tangible y lo intangible.

Esto es algo de lo que nos explica Yuval Noah Harari (sapiens, 2014), cuando establece que a pesar de que en el aspecto orgánico no somos tan diferentes a otros animales, es nuestra capacidad de actuar colectivamente de manera flexible y en masa lo que marca la diferencia.

Este tipo de acciones ha permitido que sea desarrollada una actualización de los conceptos de seguridad y defensa debido a la modificación de los conceptos de riesgo amenaza y vulnerabilidad, además de la aparición de nuevos actores estatales o no, vinculados al ambiente militar o no, así como la multiplicidad de afectados, seres humanos, maquinarias, infraestructuras y softwares (Gamón, 2017).

De lo anterior se entiende que nos mantenemos ante una disyuntiva del modelo tradicional de la Defensa y la Seguridad frente a un nuevo modelo que debe aceptar algunos riesgos y que debe operar en un entorno vulnerable, pero que se asocia también al crecimiento de nuevas amenazas en un entorno virtual e intangible.

PARADIGMAS DE SEGURIDAD Y DEFENSA FRENTE A LA TECNOLOGÍA

Amparados bajo el principio de la legítima defensa y de la búsqueda, protección y preservación de los intereses nacionales, y habiendo sigo testigos de los eventos del 11 de septiembre del 2001 en los Estados Unidos de Norteamérica y el 11 de marzo del 2004 en Madrid, España, evidenciaron nuevos elementos a ser considerados como amenazas y como las actividades cotidianas, podían colapsar, lo cual hizo posible un cambio en las estrategias de Defensa y Seguridad de todos los organismos. Este Siglo XXI promete estar plagado de una serie de acciones o ataques desde diferentes lugares, incluso aprovechando los entornos virtuales lo que ha obligado a la creación de los Cibercomandos.

Conforme a la legislación europea las infraestructuras críticas son definidas como:

"Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados miembros. http://europa.eu/scadplus/leg/es/lvb/l33259.htm (CCNSTIC-401:2007)".

Con esto se destaca que las infraestructuras estratégicas del estado son las que garantizan el desarrollo de las actividades cotidianas y mantiene un equilibrio entre el desarrollo, el uso aplicado de la tecnología y el estado, brindando estabilidad y paz a sus ciudadanos.

Constituye un grave problema de Defensa y Seguridad de los países, poder contar con una organización con las competencias necesarias para garantizar la protección de las infraestructuras críticas y su clasificación, sean estas vistas del modo estratégico, vitales, operativas, funcionales, de defensa y seguridad o de transporte. Así como los correspondientes elementos, instituciones, agencias y marcos legales o de acción para poder actuar en momento determinado. Esto último porque algunas instalaciones pueden formar parte de la iniciativa privada o de empresas, pero pueden afectar a la colectividad de la nación en caso de fallas, así como estas pudieran cambiar de clasificación en un momento determinado, lo cual implicaría un cambio en los roles de control, dirección o administración del recurso.

De acuerdo a un artículo del Dr. Vicente Pons Gamón, publicado en la Revista URVIO (Gamón, 2017), se afirma que el incremento de usuarios de internet es uno de los mayores fenómenos, que ha dado pasos agigantados desde el 1969 hasta la fecha, donde existe una dependencia casi total de los sistemas informáticos, se atribuye junto al crecimiento del internet a un nuevo espacio delictivo, para criminales y terroristas.

Es por esto, que podemos identificar que esto produjo dos cambios significativos en cuanto a los países a partir del marco legal regulatorio para perseguir estos delitos, crímenes y acciones terroristas vinculadas al ciberespacio, y la creación de nuevas estructuras o cuerpos de seguridad para enfrentarlas, perseguirlas o prevenir sus acciones.

Basado en estos criterios se ha podido observar como el desarrollo tecnológico de la humanidad, ha provocado cambios que se asocian a la naturaleza de la guerra. En nuestra intervención durante el Simposio Ciber Seguridad/Defensa 2019 celebrado por el Instituto Superior para la Defensa (INSUDE) se pudo ponderar que asumiendo los cambios paradigmáticos en ciclos de cada 20 años a partir de la Segunda Guerra Mundial (1945) y con ello fueron identificadas acciones militares desarrolladas a gran escala frente a los adelantos y usos de nuevas tecnologías, dejando abierto este esquema para el año 2025, donde con el Big Data, la Inteligencia artificial, las tecnologías disruptivas y exponenciales, sumado a la investigación y desarrollo de equipos cada vez más rápidos y mejores vías de interconexión, no cabe dudas que estaremos frente a nuevos eventos. (Baralt, 2019).

NUEVOS ESQUEMAS PARA LA DEFENSA Y LA SEGURIDAD

La seguridad Informática había sido tratada en un principio sobre la base de mecanismos de restricciones físicas, murallas o controles de acceso, sin embargo, con la proliferación de los equipos informáticos y la mejora de la tecnología, que propiciaron su cambio de tamaño, estos equipos fueron más accesibles, con más capacidad y mejor desempeño que los equipos tradicionales lo que hizo posible que los empleados utilizaran sus propios equipos o desde su hogar.

La protección de las infraestructuras criticas abarca no solo la protección física o material contra posibles ataques, sino otras vin-

culadas con el entorno virtual, además de definir las respuestas correspondientes, así como la normativa de coordinación entre las agencias o instituciones actuantes.

Factores como el terrorismo, la delincuencia organizada, la interconexión de los sistemas críticos, y cada vez más dependientes de la interconexión a través de sistemas de cómputos o instalaciones de carácter privado que no están bajo el control del estado, son algunos de los potenciadores de esta identificación de las infraestructuras, así como los protocolos de acción y marco regulatorio para cada uno de los casos.

Existen tres aspectos se asocian a que la seguridad de información basada en la norma ISO2700 (Glosario de términos) consiste en la preservación de la confidencialidad, integridad y la disponibilidad de la información.

La seguridad Informática como una disciplina que involucra técnicas, aplicaciones y dispositivos que aseguran la autenticidad y privacidad de las informaciones contenidas en los sistemas informáticos, dividiendo está en dos tipos: a) seguridad lógica: De las herramientas informáticas de control de acceso a los sistemas informáticos y b) La seguridad física: Aquella que se especializa en proteger los dispositivos del ambiente externo a causa de factores externos (ataques, incendios, inundaciones etc.).

Las infraestructuras críticas están expuestas a las amenazas internas y externas que pueden afectar no solo a los ambientes lógicos, sino que además pueden afectar los ambientes físicos o una combinación de ambos. A esto se suma el factor humano, que bien puede además afectar ambos ambientes en función al daño provocado con intencionalidad o no, pero que al final tiene un costo similar.

Las infraestructuras deben ser clasificadas y para ello existen diferentes métodos para evaluar las infraestructuras, y para esto se precisa establecer un listado que bien puede estar relacionado con las siguientes categorías:

Energía	*Industria Nuclear Y manufacturera*	*Tecnología de información y comunicaciones*	*Recursos Hídricos*
Alimentación	Salud	Sistema financiero	Transporte
Industria química	Espacio	Investigación	Administración

Tabla 1: Tomado de: Sectores estratégicos conforme a la Ley 8/2011 de Infraestructuras Críticas de España.

De esta lista son consideradas para su evaluación en función de:

- Cantidad de personas afectadas en función del número de víctimas mortales o heridos o consecuencias para la salud pública.
- Impacto económico de las perdidas.
- Impacto medioambiental.
- Impacto público y social (alteración de la vida cotidiana o perdida de los servicios esenciales).

La Constitución de República Dominicana establece las garantías en cuanto al respeto a la dignidad humana y los derechos fundamentales, así como la protección efectiva de su persona, su dignidad a la vez que proporciona los medios para que los ciudadanos puedan perfeccionarse de modo equitativo y progresista lo cual se evidencia en los artículos 7 y 8. (República Dominicana, 2015).

Artículo 7.- Estado Social y Democrático de Derecho. La República Dominicana es un Estado Social y Democrático de Derecho, organizado en forma de República unitaria, fundado en el respeto de la dignidad humana, los derechos fundamentales, el trabajo, la soberanía popular y la separación e independencia de los poderes públicos.

Artículo 8.- Función esencial del Estado. Es la protección efectiva de los derechos de la persona, el respeto de su dignidad y la obtención de los medios que le permitan perfeccionarse de forma igualitaria, equitativa y progresiva, dentro de un marco de libertad individual y de justicia social, compatible con el orden público, el bienestar general y los derechos de todos y todas.

Con el Decreto Presidencial número 230-18, de la Estrategia Nacional de Ciberseguridad la República Dominicana asume su compromiso de garantizar la seguridad de los sistemas de información, así como de las infraestructuras críticas (Gobierno dominicano, 2018).

El objeto de su creación persigue establecer y regular la estrategia nacional de Ciberseguridad del 2018-2021, con la misión de establecer los mecanismos necesarios para la protección del estado, sus habitantes y el aseguramiento del desarrollo y seguridad nacional, además de procurar en su visión, establecerse al 2021 como un país más seguro en cuanto al ciberespacio y las actividades de sus ciudadanos.

Distribuido su accionar a través de 4 pilares, se plantea brindar respuesta en los ámbitos de: 1.- Marco legal y fortalecimiento institucional, 2.- Protección de infraestructuras Críticas e Infraestructuras TI del Estado, 3.- Educación y cultura nacional en ciberseguridad, 4.- Alianzas nacionales e internacionales.

Las Fuerzas Armadas dominicanas, como parte de la estructura del estado, deben emplear sus recursos para provocar un cambio en la naturaleza de las funciones y roles tradicionales, y sumar sus propias iniciativas que permitan ayudar a completar las acciones de esta directiva, y promover la creación de entornos sectoriales seguros.

Nota: Las líneas de acción y objetivos superan los dispuestos, aquí fueron señalados los que afectan al Ministerio de Defensa y la Policía Nacional como instituciones encargadas de preservar la Defensa y la Seguridad Nacional.

PILAR	Objetivo especifico	Lineas de acción
I Marco legal y fortalecimiento institucional	1: Fortalecer el marco jurídico que facilite un ciberespacio seguro en RD.	1.1 Desarrollar un plan de actualización y reforma del marco jurídico. 1.2 Establecer un plan de actualización del marco regulatorio dados los cambios.
	2: Fortalecer las capacidades de los órganos de investigación de crímenes y delitos de alta tecnología.	2.1. Realizar una evaluación de las capacidades de los cuerpos de investigación. 2.2. Incluir en el plan de estudios programas de investigación y seguimiento a evidencias. 2.3 Fortalecer la relación de la policía con la ciudadanía en la mejora de la confianza para hacer denuncias.
2.- Protección de Infraestructuras Criticas e Infraestructuras TI del Estado	1.- Identificar las infraestructuras criticas y de TI de la nación.	1.- Establecer los criterios para la evaluación. 2.- Catalogar las Infraestructuras Criticas y de TI. 3.- Efectuar el análisis de riesgo de las infraestructuras criticas y de TI e identificar su vulnerabilidad.
	2.- Elaborar y poner en ejecución un plan para robustecer la seguridad de la infraestructura crítica.	1.- Considerará las mejores prácticas en ciberseguridad. 2.- Analizar y mejorar las normas emitidas en ciberseguridad.
	3.- Mejorar la Coordinación intersectorial	1.- Establecer un equipo se respuesta ante incidentes cibernéticos (CSIRT-RD) 2.- Promover la creación de equipos sectoriales de respuestas a incidentes cibernéticos y ayudar al CSIRT-RD. 3.- Definir y aplicar un protocolo de comunicación entre los equipos sectoriales y el CSIRT-RD 4.- Hacer cumplir los requisitos mínimos de seguridad y recuperación de las infraestructuras criticas y de TI del Estado.
	4.- Elaborar un plan de respuesta ante incidentes	1.- Identificar las entidades relevantes para la actuación. 2.- Definir el protocolo de activación y actuación de las instituciones ante incidentes de ciberseguridad. 3.- Coordinar y monitorear las actividades de recuperación de incidentes hasta la normalidad. 4.- Crear un plan de ejercicios periódicos y prácticas en incidencias cibernéticas del estado y del sector privado.
Pilar 3: Educación y cultura nacional en ciberseguridad	1.- Incorporar el manejo de los temas fundamentales en seguridad informática.	1.- Incluir planes de capacitación en materia de ciberseguridad al personal docente del nivel básico y media escuela públicas. 2.- Adecuar los planes de estudio de educación básica y media.
	2.-Adecuar los planes de estudio básica, grado y postgrado a ciberseguridad y cibercivismo.	1.- Planes de capacitación a docentes de grado y posgrado en ciberseguridad.
	3.- Crear un marco de coordinación académica en ciberseguridad.	1.- Propiciar la investigación en ciberseguridad. 2.- Desarrollar un programa de caza talentos en ciberseguridad. 3.- Establecer un programa de formación continua para los servidores públicos. 4.- Sensibilizar a la población civil.
Pilar 4: Alianzas Nacionales e Internacionales	Fomentar mecanismos de cooperación nacional con los sectores público, privado y sociedad civil.	1.- Establecer alianzas para la creación de una plataforma de seguimiento conjunta. 2.- Asegurar la participación de República Dominicana en foros y eventos internacionales en materia de ciberseguridad. 3.- Fomentar el intercambio de información nacional e internacional.

Tabla 2: Identificación por pilares de las vinculaciones de las FFAA a la Estrategia de Ciberseguridad RD 2018-2021. Elaboración propia.

Al producirse los cambios en este mundo global en cuanto a este espacio virtual intangible surgen nuevas actividades como la Cibercriminalidad y la Ciberguerra. Ambos conceptos se definen de acuerdo al Diccionario LID de Inteligencia y Seguridad, (Díaz, Cabré, Marcelino, Gómez, 2013) del modo siguiente:

Cibercriminalidad: Modalidad delictiva contra la confidencialidad, la integridad, y la disponibilidad de los datos y los sistemas informáticos. Incluye aquellos delitos relacionados con fraudes informáticos o falsificaciones informáticas, delitos relacionados con la venta o distribución de pornografía infantil a través de internet y delitos que infringen el derecho de la propiedad intelectual o derechos afines. La práctica de actividades relacionadas con la cibercriminalidad ha crecido desde el mismo momento en que apareció internet. Muchos ciberdelitos son perpetrados por delincuentes aislados, pero otros son obra de grupos criminales internacionales.

Por su parte la ciberguerra ha sido definida en el referido diccionario como:

Acción ejecutada por un Estado con la finalidad de penetrar en los ordenadores o redes informáticas de otro, con el objeto de causar daños o interrupción de servicios. El Pentágono reconoció, en 2009, al espacio cibernético como un potencial territorio donde podría librarse un ataque de otros Estados, que podría ir dirigido a infraestructuras críticas, pudiendo así bloquear servicios esenciales como agua, electricidad o transporte; causar daños económicos importantes, e interrumpir actividades cotidianas de ciudadanos, empresas y administraciones. Tras los ciberataques que sufrió Estonia en 2007, muchos países han establecido departamentos de guerra electrónica y han reforzado la protección de sus infraestructuras críticas.

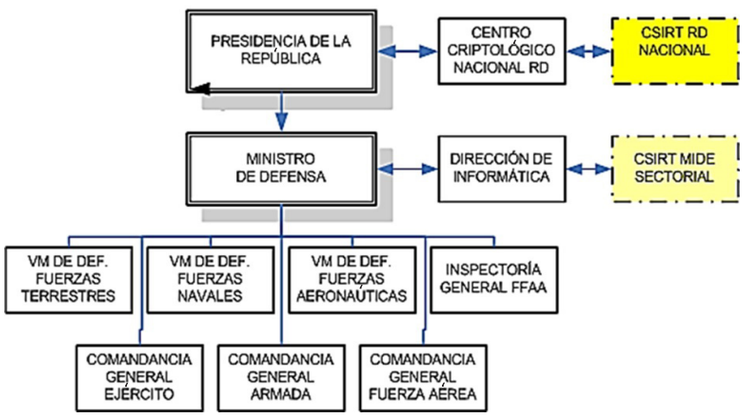
En todas estas definiciones, arrojan nuevamente la necesidad de los estados de generar las estructuras y los instrumentos necesarios para la protección de la vida y bienes de sus ciudadanos, así como la inminente implicación de que los países podían ser afectados por otros a través del espacio cibernético, dirigiendo ataques a las infraestructuras críticas, así como a recursos vitales de cada nación. Esto demanda una estructura defensiva que permita responder a una crisis y que por demás permita restaurar los sistemas en la brevedad posible para su funcionamiento.

LA CREACIÓN DE UN CERT O CSIRT SECTORIAL PARA EL MINISTERIO DE DEFENSA DE REPÚBLICA DOMINICANA

En atención a la Estrategia Nacional de Ciberseguridad las instituciones del estado tendrán CSIRT Sectoriales, los cuales obedecen a instituciones afines. El MIDE puede transformar su Dirección de Informática en el CSIRT-MIDE.

Ante estos nuevos roles que afectarán a las FFAA se propone la creación de un CERT o CSIRT del Ministerio de Defensa de la República Dominicana, utilizando para ello en vista de la experiencia favorable de otros países como el Reino de España, de donde fueron tomados como ejemplos los documentos fundamentales para su diseño y configuración el Producto WP2006/5.1 (CERT-D1/D2) titulado "Cómo crear un CSIRT paso a paso" de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA, 2019) y la Guía de Creación de un CERT/CSIRT (CCN-STIC-810) del Centro Criptográfico Nacional del Ministerio de Defensa de España.

Cabe destacar que el proceso de creación de los CERT o CSIRT, se refiere en primera instancia a que la organización ya cuenta con un Sistema de Seguridad de la Información, que ha cumplido con el proceso prudente para su maduración y cuenta ya con la estructura básica de recursos humanos, económicos, instalaciones, infraestructura, protocolos de actuación, un marco legal regulatorio y competencias, aprovechando para ello la estructura existente en la Dirección de Informática en un nuevo esquema.



Propuesta para la creación de un CSIRT para el Ministerio de Defensa de República Dominicana. (Elaboración propia).

Tomando en cuenta los servicios que ofrecería el mismo, dado que cada país tiene sus propias capacidades, recursos y necesidades, para prestar los mismos servicios conforme a la lista de los servicios de los CSIRT del CERT/CC: recuperado de: http://www.cert.org/csirts/services.html, estos pueden ser identificados de acuerdo a su naturaleza, alcance, tamaño y disponibilidad de recursos (ENISA, 2019).

De lo anterior se describen las actividades que el CERT o CSIRT del MIDE deberá ofrecer como servicios de donde los reactivos y proactivos, reflejan una gama importante en cuanto a las actividades, los primeros para responder y mitigar los incidentes y los segundos para prevenir la ocurrencia de incidentes. Todas estas acciones deberán conectar con el accionar del CSIRT-RD o Nacional.

Este, al estar conectado con el Centro Nacional de Ciberseguridad podrá proveer capacidades de información, prevención, mitigación y respuesta adecuada ante cualquier incidencia de carácter cibernético, así como las capacidades de resiliencia ante eventos que puedan ser catastróficos o que afecten las infraestructuras críticas.

Servicios reactivos	Servicios proactivos
✓ Alertas y advertencias	✓ Comunicados
✓ Tratamiento de incidentes	✓ Observatorio de tecnología
✓ Análisis de incidentes	✓ Evaluaciones o auditorías de la seguridad
✓ Apoyo a la respuesta a incidentes	✓ Configuración y mantenimiento de la seguridad
✓ Coordinación de la respuesta a incidentes	✓ Desarrollo de herramientas de seguridad
✓ Respuesta a incidentes in situ	✓ Servicios de detección de intrusos
✓ Tratamiento, análisis y respuesta a la vulnerabilidad	✓ Difusión de información relacionada con la seguridad

Gráfica servicios a ofrecer en el CSIRT del MIDE. (Elaboración propia basado en el documento fuente).

NUEVO PARADIGMA HACIA EL AÑO 2030 DE LAS INFRAESTRUCTURAS CRÍTICAS EN CUANTO A LA SEGURIDAD Y DEFENSA

Los escenarios actuales permiten evidenciar que estaremos en el 2030, en un aumento de la tecnología en cuanto a la cantidad, calidad y uso, por lo tanto se precisa establecer que para las Fuerzas Armadas serán nuevos roles a emplear y nuevos escenarios que dan sentido a la guerra vista no solo desde el punto de vista militar, sino de cómo enfrentar las acciones que puedan generar daños contra la vida y bienes de los ciudadanos.

Visto así la Ciberguerra y los conflictos en escenarios virtuales son una realidad, solo basta definir como la enfrentaremos, y como serán empleadas las medidas para adaptarnos cuando esto ocurra. El desarrollo de políticas públicas para garantizar la ciberseguridad y las infraestructuras críticas, sumado a la educación y concientización en temas ciber, deberán ser la prioridad para los próximos años, en virtud del aumento de la dependencia de los sistemas informáticos y los efectos domino o cascada que pueden producirse en algún momento al colapsar uno de los sistemas prioritarios.

En pocas palabras tendremos que adaptarnos, desaprender, aprender y reaprender, porque cada día van en aumento los sistemas y cambian nuestras capacidades de reacción y no existen las de prevención ante eventos de nueva aparición.

Peor aún, las máquinas dotadas de inteligencia artificial y los programas que pueden tener estas capacidades, permiten evidenciar que nos enfrentaremos a un nuevo enemigo que ha aprendido con nosotros, que podrá anticipar las respuestas y contramedidas, o que de algún modo podrá condicionar nuestra respuesta ante estos eventos.

CONCLUSIÓN

• Estamos frente a un nuevo paradigma que debe ser enfrentado y al que debemos adaptarnos. ¿Estamos preparados para ello?

• Debemos dejar atrás el pasado y estar listos a desaprender para aprender lo nuevo.

• Las amenazas no solo están dentro o fuera de nuestras oficinas o en nuestros hogares, están en todas partes, en todo lo que hacemos o pretendemos hacer.

• Se requiere una formación especializada, cambiante y retadora, que cada día sufre mutaciones y hace muchas cosas.

• Los individuos y las instituciones solos no pueden avanzar, se necesita la cooperación en la sociedad, instituciones públicas y privadas, así como la cooperación internacional y especializada.

• Pero sobre todo, prepararnos no para no caer, sino prepararnos para levantarnos y restaurar los sistemas y servicios que brindan nuestras infraestructuras, cuando por razón de cualquier naturaleza.

REFERENCIAS

Centro Criptológico Nacional. (2015). *Guía de seguridad (ccn-stic-401) glosario y abreviaturas.* Madrid, España: Centro Criptológico Nacional.

Constitución de la República Dominicana. (2015). Santo Domingo, República Dominicana: Congreso Nacional.

Decreto 230-18. (2018). *Estrategia nacional de ciberseguridad 2018-2021.* Santo Domingo, República Dominicana: Presidencia de la República.

Díaz Fernández, A., Cabré, M.T., Elosa, M. y Gómez Enterria, J. (2013). *Diccionario LID de inteligencia y seguridad.* Madrid: LID Editorial Empresarial.

ENISA. (2019). *Como crear un CSIRT paso a paso. Producto WP2006/5.1* (CERT-D1/D2). ENISA. Recuperado de https://www.enisa.europa.eu/publications#c5=2009&c5=2019&c5=-false&c2=publicationDate&reversed=on&b_start=20&c10=C-SIRTs+in+Europe&c8=CSIRTs

Gamón, V. P. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *Urvio: Revista Latinoamericana de Estudios de Seguridad,* 15. doi: dx.doi.org/10.17141/urvio.20.2017.2563

Gobierno de España_CCN. (2019). *Guía de seguridad (CCN-STIC-810). Guía de creación de un CERT / CSIRT.* Recuperado de https://www.ccncert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf

Obama, B. (2008). *La iniciativa nacional de seguridad cibernética integral.* Recuperado de https://obamawhitehouse.archives.gov/issues/foreignpolicy/cybersecurity/national-initiative

RAE. (2019). *Seguridad.* Diccionario de la Real Academia Española. Recuperado de https://dle.rae.es/