LA CIBERSEGURIDAD EN EL AMBITO DE LA DEFENSA NACIONAL

Dra. Esc. María José Viega Rodríguez (*)

RESUMEN: Uruguay ha adoptado en su Ley N° 18.650 de Defensa Nacional un concepto amplio de ésta, comprendiendo tanto las acciones civiles como militares. El ciberespacio, considerado como el quinto ámbito de la defensa nacional, está previsto en el Decreto N° 371/020, así como las amenazas que pueden suscitarse dentro de éste. La ciberseguridad se encuentra contemplada en el Objetivo X de la Agenda Uruguay Digital 2025, aprobada por el Decreto N° 134/021 y su ecosistema está coordinado por la Agencia de Gobierno de Gestión electrónica la Sociedad de la Información y el Conocimiento (AGESIC).

PALABRAS CLAVES: ciberseguridad, ciberespacio, amenazas, defensa nacional, Uruguay

1. INTRODUCCIÓN

Uruguay aprobó la Ley de Defensa Nacional N° 18.650 el 19 de febrero de 2010, constituyendo el Marco apara la Defensa Nacional de la República.

El artículo 1° establece que: "La defensa nacional comprende el conjunto de actividades civiles y militares dirigidas a preservar la soberanía y la independencia de nuestro país, a conservar la integridad del territorio y de sus recursos estratégicos, así como la paz de la República, en el marco de la Constitución y las leyes; contribuyendo a generar las condiciones para el bienestar social, presente y futuro de la población".

* **Doctora en Derecho y Ciencias Sociales y Escribana Pública por la Universidad Mayor de la República Oriental del Uruguay (UDELAR). Profesora de Informática Jurídica y Derecho Informático en la UDELAR.** Gerente de la División Derecho Informático en AGESIC. Profesora de Derecho Informático en el Máster de Seguridad de la Información de la Facultad de Ingeniería (UDELAR). Profesora de Ética y Legislación en ORT. Posgrado de Derecho Informático: Contratos Informáticos, Contratos Telemáticos y Outsourcing en la Universidad de Buenos Aires. Experta Universitaria en Protección de Datos, UNED (ESPAÑA). Experta Universitaria en Administración electrónica, Universidad Operta de Cataluña (España). **Cursando Posgrado en Inteligencia Estratégica y la Maestría en Defensa Nacional en CALEN.** mjviega@gmail.com

La ley ha adoptado un concepto amplio de la defensa nacional, comprendiendo tanto acciones de carácter civil como militar, e implica la conservación de la integridad de su territorio.

El artículo 2° establece que la Defensa Nacional constituye un derecho y un deber para la ciudadanía en su conjunto, constituyendo una función del Estado, que a su vez la caracteriza como permanente indelegable e integral.

La Ley N° 19.775 de 26 de julio de 2019, Ley orgánica de las Fuerzas Armadas, en el artículo 8° inciso primero establece: "El ámbito espacial del Estado comprende el territorio continental e insular, incluyendo el subsuelo y las aguas jurisdiccionales, así como el espacio aéreo correspondiente a dichas zonas". Y en su inciso segundo se consigna a texto expreso al ciberespacio, cuando expresa: el ámbito espacial del Estado incluye al ciberespacio y al espectro electromagnético.

Por otra parte, el Decreto N° 371/020 de 23 de diciembre de 2020 que estableció la Política de Defensa Nacional, considera dentro de las amenazas, la violación de nuestra soberanía terrestre, marítima, aeroespacial y del ciberespacio, considerando a los ciberataques como una amenaza que puede suscitarse dentro de éste.

Por tal motivo, la ciberseguridad se encuentra contemplada en el Objetivo X de la Agenda Uruguay Digital 2025, aprobada por el Decreto N° 134/021 de 4 de mayo de 2021 y su ecosistema está coordinado por la Agencia de Gobierno de Gestión electrónica la Sociedad de la Información y el Conocimiento (AGESIC).

Dentro del Ministerio de Defensa Nacional se encuentra el Csirt de Defensa. En el ámbito civil, en el área pública, la Dirección de Seguridad de Agesic que coordina al Centro Nacional de respuestas de incidentes de seguridad informática (CERTuy) y al Centro de operaciones en ciberseguridad (SOC), y también se cuenta con el Csirt de Antel. En el ámbito privado vamos a encontrar los sistemas de ciberseguridad de las empresas y organizaciones privadas, como por ejemplo los sistemas de los bancos.

2. CONCEPTUALIZACION DE LA CIBERSEGURIDAD

El ciberespacio, conceptualizado en sus orígenes como "el lugar sin lugar", en el cual se creía que se podría realizar cualquier tipo de acción sin consecuencias, a lo largo de los años se ha ido

demostrando que no es así. Si bien los temas de la ley aplicable y la jurisdicción competente no dejan de ser una cuestión desafiante, aún hoy, es posible implementar diferentes medidas, frente a las amenazas que sobrevienen en éste.

El ciberespacio se conceptualiza como el espacio virtual que se origina al procesarse, comunicarse y almacenarse información digital por sistemas informáticos (Camps P., 2022).

La ciberseguridad se enmarca en un concepto más amplio que es la seguridad de la información. Esta última puede ser definida como el conjunto de medidas preventivas y reactivas tendientes a resguardar la información buscando mantener su confidencialidad, disponibilidad e integridad (Camps P., 2022).

La importancia de la ciberseguridad crece día a día, el aumento en la utilización de las TIC como consecuencia de la pandemia, disparó los delitos informáticos, así como se han producido diferentes ciberataques en la guerra Rusia – Ucrania.

La ciberseguridad consiste en el conjunto de medidas de carácter preventivo y reactivo para asegurar el uso de las redes y sistemas informáticos propios y negarlo a terceros, manteniendo la integridad, confidencialidad y disponibilidad de la información digital" (Camps P., 2022).

En el ciberespacio hay desaparecido las fronteras físicas, es difícil conocer el origen de un ataque, así como quien lo ha ordenado, por lo que tener una estrategia clara sobre este ámbito es de fundamental importancia.

Yuval Harari (2018, pág. 201) reflexiona acerca de este punto en los siguientes términos: "Pero si ahora Estados Unidos ataca a un país con capacidades para la ciberguerra, incluso moderadas, la contienda podría trasladarse a California o Illinois en cuestión de minutos. Programas malignos y bombas lógicas podrían interrumpir el tráfico aéreo en Dallas, hacer que chocaran trenes en Filadelfia y provocar la caída de la red eléctrica de Michigan. En la gran época de los conquistadores, la guerra era un asunto de daños reducidos y grandes beneficios. En la batalla de Hastings, en 1066, Guillermo el Conquistador se hizo con toda Inglaterra en un solo día al precio de apenas unos pocos miles de muertos. Por el contrario, las armas nucleares y la ciberguerra son tecnologías de daños elevados y pocos beneficios. Se pueden emplear estas herramientas para destruir países enteros, pero en absoluto para construir imperios rentables"

En nuestro país el Decreto N° 134/021 aprueba la Agenda Digital Uruguay 2025, y el Objetivo X refiere a Ciberseguridad, en el que se establece: “Incrementar la ciberseguridad para prevenir y mitigar riesgos en el ciberespacio y avanzar en el cumplimiento del marco nacional de ciberseguridad, basado en la cooperación público y privada, garantizando la disponibilidad de los activos críticos de información”.

Este objetivo se divide en tres aspectos, establecidos en los puntos:

46. Adoptar el Marco de Ciberseguridad en servicios, infraestructura y redes críticas para el país, otorgando mayor seguridad, estandarización y confianza a todos los actores del desarrollo digital.

47. Desarrollar e impulsar trayectorias de formación en ciberseguridad para el desarrollo de capacidades a través de la educación formal y no formal.

48. Mejorar la eficiencia en la detección y respuesta a incidentes cibernéticos, mediante la implementación de nuevas tecnologías que permitan aplicar análisis predictivos y automatización de respuestas, entre otras.

En este sentido, es de destacar que se ha venido trabajando, tanto en la elaboración del Marco de Ciberseguridad realizado por Agesic, como en la Guía para su implementación. Asimismo, el Certuy ha realizado muchas jornadas de capacitación, así como campañas de concientización para niños y adultos.

La preocupación por la ciberseguridad se debe a que en las relaciones telemáticas que se dan hoy día en todos los ámbitos de la vida humana, las diferentes personas pueden ser tanto atacantes como víctimas.

“En este medio, los atacantes pueden ser de alta complejidad patrocinados por estados o empresas privadas, pueden venir de grupos organizados con fines terroristas o activistas, de organizaciones delictivas o de simples individuos. Pueden ser dirigidos o genéricos y atacar blancos gubernamentales, empresariales o particulares con objetivos dispares según el caso. Lo blanco y lo negro no son norma en este ciberespacio donde priman los grises y no es siempre fácil determinar si un ataque es un delito común, un acto terrorista o un ataque que puede afectar la seguridad nacional, y lo que es peor aún no siempre se puede identificar al atacante” (Camps, 2016, pág. 265).

3. LA DEFENSA NACIONAL EN EL DERECHO URUGUAYO

Como ya hemos hecho mención, la Ley N° 18.650 establece en su artículo primero que la defensa nacional comprende actividades civiles y militares, que deben contribuir a generar condiciones para el bienestar social, presente y futuro de la población. En este sentido, la defensa nacional tiene que generar bienestar.

En el artículo 2° se hace referencia a la ciudadanía en su conjunto, no solamente al ámbito militar, constituyendo la defensa nacional un derecho y un deber de la ciudadanía.

En este ámbito encontramos que defensa y seguridad son dos conceptos inseparables, la defensa es una acción, mientras que la seguridad es una condición. Cuando nos referimos a defensa, en sentido estricto nos referimos al ámbito militar y en un sentido amplio a la defensa nacional. Considerando a la seguridad como condición, la dimensión objetiva está dada por las amenazas.

En lo referente a la soberanía, no se hace mención a texto expreso en la Ley N° 18.650 al ciberespacio, pero es considerado en los Decretos que establecen la Política de Defensa Nacional para los períodos de gobierno, y en ellos, tanto en el Decreto N° 105/014, como en el Decreto N° 371/020, aunque lo hacen en un sentido diferente.

El Decreto N° 105/014 hace referencia al potencial de desarrollo de las nuevas tecnologías y la interconexión de las redes de comunicación, "tornándose una cuestión central para la educación y la información". Considera que estas nuevas herramientas han introducido una nueva dimensión en el ámbito de la seguridad y la defensa, mencionando entre los desafíos actuales los delitos económicos e informáticos.

Al plantearse el escenario futuro hace referencia al ciberespacio: "Las líneas de comunicaciones por las que discurren bienes, servicios e información, particularmente las aguas internacionales y el ciberespacio, se reconfigurarán".

Finalmente, dentro de los objetivos de la defensa nacional, concretamente en los objetivos de carácter estratégico, hace referencia a fortalecer la presencia del Estado en los espacios terrestres, marítimo y aéreo, no haciendo referencia al ciberespacio.

Sí lo considera dentro de los obstáculos que podrían enfrentarse: la materialización y los ataques cibernéticos.

En el Decreto N° 371/020, en el punto III. Situación regional, aparece el ciberespacio como uno de los espacios de interés estratégico, junto al terrestre, marítimo y aeroespacial.

En el punto IX. Amenazas, se consideran los ciberataques como una de las amenazas que afectaría la disponibilidad, integridad o la confidencialidad de la información digital. Hace hincapié en que podrá tener efectos lógicos o físicos, dependiendo del sistema objeto del ataque. Tiene en cuenta también que las amenazas criminales y terroristas tradicionales pueden materializarse en esta modalidad.

Como ya se hizo mención en la introducción, al referirnos al concepto de defensa nacional en sentido estricto, la Ley N° 19.775 en el artículo 8° inciso 2° considera al ciberespacio dentro del ámbito espacial del Estado.

4. INSTITUCIONES CON COMPETENCIA EN CIBERSEGURIDAD

Partiendo de las consideraciones anteriores, teniendo en cuenta el concepto amplio de defensa nacional, vamos a analizar la situación de la ciberseguridad en nuestro país, considerando que no existe al día de hoy una estrategia nacional definida en esta materia.

En la esfera pública, la Agesic coordina el ecosistema de Ciberseguridad, incluyendo al CSIRT en el ámbito del Ministerio de Defensa Nacional, como a los organismos de carácter civil.

La Agesic fue creada por el artículo 72 de la Ley N° 17.930 de 19 de diciembre de 2006, y tiene el cometido de liderar la estrategia de gobierno electrónico en Uruguay. Desde los inicios se entendió que el proceso de incorporar tecnologías a las instituciones del Estado debía estar centrado en el ciudadano, siendo más eficiente y eficaz en el desarrollo de sus funciones. Con esa consigna se impulsó la Ley de Protección de Datos Personales y Acción de Habeas Data N° 18.331 de 11 de agosto de 2008, entendiendo que la interoperabilidad era uno de los pilares para el desarrollo del gobierno electrónico. Por lo tanto, la comunicación de datos personales de los ciudadanos entre los organismos debía dar garantías de privacidad, sin obstaculizar el objetivo de que las personas no fueran cadetes del Estado, sino que éste solucione internamente aquellos aspectos que faciliten el relacionamiento y permita un mejor desempeño de la función estatal.

Por otra parte, se promueve la confianza y la seguridad en el uso de las TIC y con este objetivo se crea por el artículo 119 de la Ley N° 18.172 de 31 de agosto de 2007 el Consejo de Seguridad de la Información, para apoyar a Agesic en este tema. El Consejo está integrado por representantes de los siguientes organismos: Prosecretaría de la Presidencia de la República, Ministerio de Defensa

Nacional, Ministerio del Interior, Administración Nacional de Telecomunicaciones y Universidad de la República.

Además, el Decreto N° 452/009, de 28 de setiembre de 2009, reglamentó las competencias establecidas por el artículo 55 de la Ley N° 18.046 de 24 de octubre de 2006, en la redacción dada por el artículo 118 de la Ley N° 18.172 de 31 de agosto de 2007, por el que se confiere a la Agesic las facultades para establecer medidas de seguridad que hagan confiable el uso de las tecnologías de la información, concibiendo y desarrollando una política nacional en temas de seguridad de la información, que permita la prevención, detección y respuesta frente a incidentes que puedan afectar los activos críticos del país.

El ecosistema está constituido de la siguiente forma:

a. CERTuy con competencias a nivel nacional.
b. Centro de Operaciones en ciberseguridad (SOC), es un área dentro de la Dirección de Seguridad de la Información de Agesic.
c. CSIRT de Antel a nivel de seguridad en las telecomunicaciones.
d. Delitos informáticos y la Unidad de Cibercrimen, en el Ministerio del Interior, con competencias en delitos informáticos en general la primera y en cibercrimen, en especial casos de hackeos la segunda.
e. Programa Salud.uy, soportado desde el punto de vista técnico por Agesic, el programa nuclea tanto a instituciones de salud públicas como privadas.
f. En la Academia, encontramos el Servicio Central de Informática de la UDELAR (SeCIU), el cual posee entre sus cometidos administrar los nombres de dominio en Uruguay.

En el ámbito público, pero en la esfera del Ministerio de Defensa, y por lo tanto vinculado a la defensa nacional en sentido estricto, es decir la defensa militar encontramos el DCSIRT, con el cometido de la ciberdefensa.

En el ámbito privado, a modo de ejemplo, hallamos los sistemas se ciberseguridad de los bancos privados, los prestadores de servicios de ciberseguridad y los prestadores de servicios de Internet (ISP) privados.

4.1 CERTuy

Según el CERT/CC, un Computer Incident Response Team (CSIRT) es una organización responsable de recibir reportes de incidentes de seguridad, analizarlos y responderlos. Dado que CERT es un término protegido y registrado en Estados Unidos por el CERT-CC, en otros países los equipos suelen tener distintas denominaciones:

- CSIRT (Computer Security Incident Response Team - Equipo de respuesta a incidentes de seguridad informática).
- IRT (Incident Response Team - Equipo de respuesta a incidentes).
- CIRT (Computer Incident Response Team- Equipo de respuesta a incidentes informáticos).
- SERT (Security Emergency Response Team - Equipo de respuesta a emergencias de seguridad).
- ISIRT (Information Security Incident Response Team - Equipo de respuesta a incidentes de seguridad de la información), (Sitio web CERTuy, 2022).

El CERTuy es el Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay y fue creado por el artículo 73 de la Ley N° 18.362 de 6 de octubre de 2008, con el objetivo de regular los activos de información críticos del Estado, de acuerdo a los criterios que sugiera el Consejo de Seguridad de la Información.

Este artículo fue reglamentado por el Decreto N° 451/009 de 28 de setiembre de 2009, regulando el funcionamiento, cometidos, potestades, obligaciones y organización del CERTuy. En el artículo 3° se definen aspectos como: activos de información, activos de información críticos del Estado, evento de seguridad informática, incidente de seguridad informática, servicios vitales para la operación del gobierno y la economía del país, y sistema informático (VIEGA M., Otra, 2018, pág. 66).

El CERTuy está conformado por un grupo de expertos responsables del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información. Sus principales objetivos son: centralizar, coordinar y optimizar los procesos de respuesta a incidentes en seguridad de la información; difundir mejores prácticas en seguridad de la información y realizar tareas preventivas (Sitio web, 2022).

4.2 Centro de Operaciones de Ciberseguridad (SOC)

El SOC tiene como objetivo principal detectar en tiempo real eventos e incidentes de ciberseguridad en los Activos de Información Críticos del Estado. Colectar y analizar información de ciberseguridad para prevenir y detectar incidentes de ciberseguridad.

En el sitio web se detallan como cometidos sustantivos:

a. Asesorar en la definición de políticas, metodologías y buenas prácticas en operaciones de ciberseguridad.

b. Monitorear los sistemas informáticos que soporten activos de información críticos del Estado, así como los sistemas circundantes a éstos.

c. Operar infraestructura de ciberseguridad del Estado.

d. Colectar y analizar información histórica de ciberseguridad.

e. Coordinar espacios de relacionamiento de múltiples partes interesadas en ciberseguridad de Seguridad de la Información.

f. Interactuar con CERTuy y otros CSIRTs para intercambiar información y coordinar operaciones de ciberseguridad.

g. Interactuar con otros SOC, locales e internacionales para el intercambio y procesamiento de información y alertas de ciberseguridad.

4.3 CSIRT de ANTEL

“El CSIRT de ANTEL es un Centro de Respuesta a Incidentes orientado a nuestra Comunidad Objetivo, la cual está integrada por ANTEL (la corporación y subsidiarias) y los clientes de ANTEL. Cuando ocurren incidentes de seguridad, es crítico que nuestra comunidad tenga un modo efectivo y coordinado de responder. La velocidad con la cual la organización pueda reconocer, analizar y responder a un incidente de seguridad limitará los daños y disminuirá los costos de recuperación. El CSIRT de ANTEL tiene como servicio central realizar una gestión de incidentes de seguridad eficaz y eficiente. Para ello, sus integrantes buscan, en el contexto de su Código de Conducta, relacionarse con equipos pares y con su comunidad, capacitarse permanentemente, estar al día tecnológicamente y así mejorar de manera continua todos los servicios brindados” (Sitio Web, 2022).

El Csirt de Antel realiza diferentes servicios:

a. Reactivos: alertas y manejo de incidentes.
b. Proactivos: anuncios, detección de incidentes y desarrollo de técnicas y herramientas.
c. Valor Agregado: capacitación y entrenamiento, análisis de riesgo, consultoría en seguridad y concientización de la comunidad en temas de seguridad

4.4 Departamento de Delitos Tecnológicos y Unidad de Cibercrimen - Ministerio del Interior

El Decreto N° 94/2019 de 25 de marzo de 2019 reglamenta el artículo 93 de la Ley N° 19.670 de 15 de octubre de 2018, relativo a la creación de la Dirección de Investigaciones de la Policía Nacional.

A esta Dirección le compete la dirección, supervisión técnico-estratégica y coordinación de la Dirección General de Lucha contra el Crimen Organizado e INTERPOL y es la encargada, de acuerdo al artículo 2° inciso 4° de proteger a la República de, entre otros, la ciberdelincuencia.

Por lo tanto, el Departamento de delitos tecnológicos de la Jefatura de Montevideo integra la Dirección General de Lucha contra el Crimen Organizado e INTERPOL trabaja para combatir la delincuencia virtual, es decir los llamados delitos informáticos.

La Unidad de Cibercrimen fue creada por Resolución del Ministro del Interior Luis Alberto Heber el 30 de agosto de 2021, la que funciona en el órbita de la Dirección de Investigaciones de la Policía Nacional.

La unidad tendrá como principales cometidos la "detección, investigación, persecución y represión de las conductas y acciones antijurídicas de amenazas, hackeo, ataque o daño contra la seguridad, confidencialidad y la integridad de sistemas informáticos", detalla la resolución del Ministerio del Interior. Y agrega: "Actividades que busquen comprometer sistemas informáticos, bancos o bases de datos y redes, sabotaje y espionaje informático" (Diario El País, 2021).

4.5 Programa Salud.uy

La Agesic entendió prioritario abordar el área de la Salud –como uno de los desafíos del gobierno electrónico- con el fin de modernizar los procesos y viabilizar mejoras en la calidad de las prestaciones de salud recibidas por los usuarios del sistema.

El Decreto N° 405/011 de 23 de noviembre de 2011, aprobó la Agenda Digital Uruguay 2011-2015, entre cuyos objetivos se encontraba la creación de redes avanzadas para la salud y una Historia Clínica Electrónica (HCE) integrada a nivel nacional, en el entendido que las Tecnologías de la Información y Comunicaciones tienen un gran potencial para la mejora de la gestión de los servicios de salud (Viega, 2021).

En el año 2012 se firmó un convenio para llevar adelante la estrategia, entre el Ministerio de Salud Pública (MSP), el Ministerio de Economía y Finanzas (MEF) y la AGESIC, creándose el Programa Salud.uy para implementar dicha iniciativa. El Programa está constituido por un Comité de Dirección, que comenzó a funcionar el 8 de marzo de 2013. Consta, además, de un Consejo Asesor representado por todos los actores del sistema, teniendo su primera reunión el 25 de junio de 2013. Han existido también diferentes grupos asesores especializados a lo largo del proyecto, con representantes de las principales áreas involucradas en cada caso (Viega, 2021, pág. 394).

En este ámbito, se creó la Historia Clínica Electrónica Nacional (HCEN), en el cual la Historia Clínica Electrónica funciona como un sistema federado entre los distintos prestadores de salud, el intercambio de información clínica se convierte en el principal desafío, desde dos puntos de vista: técnico y jurídico. Desde el punto de vista técnico se creó la Red Salud y la Plataforma de Salud, como infraestructura segura que permitiera la conexión de los distintos prestadores, tanto públicos como privados, a los efectos de permitir subir la información y habilitar los accesos.

El artículo 12 del Decreto N° 242/2017 de 31 de agosto de 2017 refiere a la seguridad de las HCE, estableciendo que será responsabilidad de cada Institución dotar de los mecanismos y procedimientos de administración e identificación electrónica a quienes accedan a la HCE. Todo acceso a la HCE debe quedar debidamente registrado y disponible. La información no podrá ser alterada o eliminada sin que quede registrada la modificación de que se trate.

Además, cada prestador es responsable de la gestión de la seguridad de su información. Por tanto, cada prestador va a gerenciar sus accesos. Es importante que la información sea confidencial, pero también que la información sea íntegra y que esté disponible cuando se necesite.

El artículo 17 establece a texto expreso, entre otras obligaciones de las instituciones, las de garantizar el acceso y adoptar medidas de seguridad.

Por el Decreto N° 122/019 de 29 de abril de 2019 se empoderó a los usuarios del Sistema Nacional Integrado de Salud (SNIS), de forma tal que pudieran controlar los accesos a su HCE, a través de la plataforma.

En este contexto, el artículo 2° reguló la seguridad en los procesos, disponiendo que las instituciones de salud, públicas y privadas, que interactúen con la plataforma de HCEN, así como las personas para la gestión de sus accesos y la consulta de su HCE, deberán encontrarse debidamente identificadas a través de los instrumentos establecidos en la Ley N° 18.600, de 21 setiembre de 2009 y sus modificativas.

El artículo 4° reguló la solicitud de acceso y estableció que en el caso que una Institución de salud, pública o privada, requiera acceder a la información disponible en la plataforma de HCEN, debe realizarlo mediante una identificación única (orden de servicio), la que será registrada en la plataforma. Las instituciones de salud deberán garantizar mediante mecanismos informáticos seguros la autenticación de las personas cuyo acceso autorizan.

La normativa establece que Agesic podrá acceder a la HCEN con la finalidad de proporcionar soporte técnico.

4.6 SeCIU

El SeCIU es el Servicio Central de Informática Universitaria, perteneciente a la Universidad de la República (UDELAR), siendo el responsable de asesorar a las autoridades universitarias sobre esta temática, así como de desarrollar y gestionar la infraestructura informática de la Udelar relacionada con los emprendimientos institucionales y de brindar asesoramiento y apoyo informático a todos los servicios universitarios. También es responsable de la administración del .UY en Internet, y es por ello que lo consideramos en el presente trabajo.

El Decreto N° 92/014 de 7 de abril de 2014 reglamenta el artículo 149 de la Ley N° 18719 relativo a la Estandarización de los nombres de dominio de la Administración Central, para todos los servicios vinculados con Internet. El decreto pretende garantizar a los organismos y a los funcionarios correos electrónicos institucionales seguros, por lo que se establecen lineamientos mínimos se seguridad para su intercambio. También establece lineamientos de seguridad para los centros de datos, considerándolo un elemento fundamental para el desarrollo del gobierno electrónico. Establece que los activos críticos de información deberán encontrarse en centros de datos existentes en el territorio nacional.

4.7 Respuesta a Incidentes de Seguridad Informática de Defensa (D-CSIRT)

El D-CSIRT es el Equipo de Respuesta a Incidentes de Seguridad Informática de Defensa, creado por el Decreto N° 36/015 de 27 de enero de 2015.

"Su creación representa la primera organización en el ámbito específico de la Defensa Nacional encargada de atender asuntos de ciberdefensa. La comunidad objetivo a la que dirige su acción son las organizaciones dependientes de dicho Ministerio, entre las que se encuentran las fuerzas armadas. El centro además de atender los incidentes comunes a cualquier organismo se especializará en los incidentes específicos en materia de Defensa que ocurrieran" (Camps, 2016).

El visto del Decreto desataca: la importancia de prevenir, atender y gestionar incidentes de seguridad cibernética que se puedan presentar en el marco de la defensa nacional;

Su misión es la de participar de forma eficaz y eficiente en la respuesta a incidentes cibernéticos sobre infraestructuras críticas y servicios esenciales de la comunidad objetivo, así como desarrollar capacidades de prevención y detección temprana de incidentes de seguridad informática en dicha comunidad (Sitio web, 2022).

En los artículos 4° y 5° del Decreto se establecen los objetivos generales y los específicos, señalándose en el artículo 8° que los servicios que se prestarán serán de carácter reactivo y proactivo, los que se encuentran especificados en los artículos 9° y 10.

Fuera de fronteras el DCSIRT para cumplir con su cometido integra igualmente con múltiples redes y equipos de respuestas como el Comité Interamericano Contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (Camps, 2016).

5. CONCLUSIONES

Con relación a la capacitación en este tema, además de las campañas mencionadas, realizadas por el CERTuy, es de destacar la labor que realiza desde el año 2014 el Centro de Altos Estudios Nacionales (C.A.L.E.N.) brindando cursos de extensión en Ciberseguridad, estando además incluida la materia en la Maestría en Estrategia Nacional y en el Postgrado de Inteligencia Estratégica, concientizando y capacitando tanto a civiles con interés en la materia, como a militares.

Por otra parte, en el Reporte 2020 de la OEA y el BID sobre Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe, se ubica a Uruguay en un lugar muy favorable.

Este documento analiza la situación en que se encuentran los diferentes países de América Latina y realiza una comparación con el estudio anterior elaborado en 2016. Luego analiza cada uno de los países, considerando diferentes aspectos (Viega, 2020).

“De acuerdo al informe Uruguay ha progresado en todas las dimensiones desde el 2016 -cuando se realizó el primer reporte de ciberseguridad- y se encuentra liderando en cuatro de las cinco dimensiones a nivel de América Latina y el Caribe: Política y Estrategia de Seguridad Cibernética, Cultura Cibernética y Sociedad, Formación, Capacitación y Habilidades de Seguridad Cibernética y Estándares, Organizaciones y Tecnologías. Asimismo, el país alcanza la máxima puntuación en temas referidos a la organización y coordinación de respuesta a incidentes; el desarrollo de la temática en el gobierno y la confianza de las personas en el uso de servicios de gobierno, entre otros” (CERTuy, 2020).

En función del análisis realizado podemos concluir que Uruguay ha incluido dentro de su marco legal a las amenazas provenientes del ciberespacio. También se cuenta con un número importante de instituciones, tanto del ámbito civil como militar, con cometidos en ciberseguridad.

Que si bien el país no posee aún una estrategia de ciberseguridad a nivel nacional se ha realizado un marco de ciberseguridad basado en los estándares internacionales y se ha obtenido una evaluación positiva por parte de organismos internacionales.

REFERENCIAS BIBLIOGRAFÍCAS

Camps P., Ciberdefensa y Ciberseguridad: nuevas amenazas a la seguridad nacional, estructuras nacionales de ciberdefensa, estrategias de ciberseguridad y cooperación interagencias en este ámbito. Ciberdefensa y Nuevas amenazas a la seguridad nacional, Río de Janeiro, 2016.

Camps P., Curso de Ciberseguridad en Calen, 2022.

Centro de Operaciones de Ciberseguridad (SOC). Recuperado de: https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/institucional/estructura-del-organismo/division-centro-operaciones-ciberseguridad-soc

CERT/CC. Recuperado de: http://www.cert.org

CERTuy, Recuperado de: https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/publicaciones/que-es-el-certuy

Csirt Antel. Recuperado de: https://www.csirt-antel.com.uy

D-CSIRT. Recuperado de: https://www.gub.uy/ministerio-defensa-nacional/tramites-y-servicios/servicios/equipo-respuesta-incidentes-seguridad-informatica-defensa-d-csirt

Diario El País, Ministerio del Interior creó Unidad para combatir hackers. Recuperado de: https://www.elpais.com.uy/informacion/policiales/ministerio-interior-creo-unidad-combatir-hackers.html

Harari Y., "21 lecciones para el siglo XXI". Editorial Sudamericana, 2018.

Servicio Central de Informática de la UDELAR (SeCIU). Recuperado de: https://www.seciu.edu.uy/

Viega M. y Hernández M., Derecho Informático e Informática Jurídica II, Fundación de Cultura Universitaria, 2018.

Viega M., Ciberseguridad 2020: la situación de Uruguay en el informe de la OEA y el BID. Recuperado de: https://www.youtube.com/watch?v=ujdboeuyLD4&t=18s

Viega M., La Historia clínica electrónica nacional en Uruguay: su desarrollo e impacto jurídico". Libro "e-salud, autonomía y datos clínicos. Un nuevo paradigma". Editorial Dykinson, 2021. Gobierno de España - Ministerio de Ciencia e Innovación.

Viega M., La Historia clínica electrónica nacional como infraestructura crítica, Revista de CADE, 2021.