CIBERDEFENSA Y CIBERSEGURIDAD: NUEVAS AMENAZAS A LA SEGURIDAD NACIONAL, ESTRUCTURAS NACIONALES DE CIBERDEFENSA, ESTRATEGIAS DE CIBERSEGURIDAD Y COOPERACIÓN INTERAGENCIAS EN ESTE ÁMBITO.

Teniente Coronel PABLO CAMPS

RESUMEN

Las nuevas tecnologías de la información y de las comunicaciones dieron origen al ciberespacio. El mismo constituye el quinto dominio de interacción humana, y cada día se hace más extenso albergando más información y brindando más y más servicios. Como resultado, este nuevo espacio ha dado lugar a la aparición de nuevas amenazas creadas por individuos, organizaciones o estados que buscan aprovecharse esta nueva forma virtual de interactuar. Las actividades ilícitas en este medio pueden causar efectos muy importantes a la víctima y reportar importantes beneficios al perpetrador, quien además muchas veces no puede ser identificado.

Los estados, como garantes de la seguridad y tranquilidad de sus habitantes han debido adaptar sus estructuras y marcos normativos para prevenir y enfrentar este nuevo escenario donde las fronteras no son claras, y los actores pueden no identificarse claramente.

El presente trabajo se enfoca en la situación de la República Oriental del Uruguay en lo referente a su grado de seguridad y capacidad de defensa en el ciberespacio. Para ello, se presentan inicialmente las nuevas amenazas identificadas por la legislación nacional, para pasar luego al detalle de las estructuras más importantes encargadas de prevenir o repeler un eventual ataque. Finalmente se discute la situación actual del País en cuanto a una estrategia de ciberseguridad.

Palabras clave: Ciberespacio. Ciberseguridad. Ciberdefensa. Uruguay. Nuevas tecnologías.

CYBERDEFENSE AND CYBERSECURITY: NEW THREATS TO THE NATIONAL SECURITY, NATIONAL CYBERDEFENSE STRUCTURES, CIBERSECURITY STRATEGIES AND INTER AGENCIES COOPERATION ON THIS AREA.

ABSTRACT

The new information technologies and communications gave rise to cyberspace. It is the fifth domain of human interaction, and each day becomes more extensive hosting and providing more and more services. As a result, this new space has led to the emergence of new threats posed by individuals, organizations or states seeking to exploit this new virtual way to interact. Illicit activities in this environment can cause major effects on the victim and report important benefits to the perpetrator, who also often cannot be identified.

States, as guarantors of security and tranquility of its inhabitants have had to adapt their structures and regulatory frameworks to prevent and address this new scenario where the boundaries are not clear, and the actors can not be clearly identified.

This paper focuses on the situation of the Oriental Republic of Uruguay regarding the degree of security and defense capability in cyberspace. To do this, initially the new threats identified by national legislation are presented, then move to the detail of the most important structures responsible for preventing or repel a possible attack. Finally, the current situation of the country regarding a strategy for cybersecurity is discussed.

Keywords: Cyberspace. Cybersecurity. Cyber defense. Uruguay. New technologies.

INTRODUCCIÓN

Para referirnos a la ciberseguridad y la ciberdefensa debemos comenzar por definir ambos términos para evitar ambigüedades. De acuerdo con el Consejo Argentino de Relaciones Internacionales[1] la ciberdefensa es un "conjunto de acciones de defensa activas, pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición". Por su parte la ciberseguridad es definida como el "conjunto de acciones de carácter preventivo que tienen por objeto el asegurar el uso de las redes propias y negarlo a terceros". Si bien las definiciones tienen parte común, podemos diferenciar un término del otro considerando que la ciberseguridad se refiere más a lo preventivo para evitar que se tenga lugar un ataque, mientras que la ciberdefensa se identifica más con lo reactivo frente a un ataque.

Otro elemento que puede llegar a crear interrogantes es que tipo de estructuras deben articularse por parte de los estados para tener una adecuada seguridad en el ciberespacio. Sobre este punto, considerando que una cadena es tan frágil como su eslabón más débil, las soluciones más efectivas serán las que se establezcan estructuras robustas partiendo desde individuos que operan equipos en el ciberespacio formados y concientizados sobre la importancia de la seguridad, pasando por equipos con adecuados niveles de seguridad, software seguro y correctamente configurado y equipos de monitoreo y respuesta capaces de detectar amenazas y prevenir ataques antes de que ocurran o de que causen mayores daños en caso de concretarse.

El ciberespacio llegó para quedarse, y cada vez se extiende más en el actual mundo globalizado. Este nuevo ámbito de interacción humana está abierto a los diferentes actores que pueden ser tanto atacantes como víctimas. En este medio, los ataques 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 la norma en este espacio 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.

NUEVAS AMENAZAS

Generalidades

Desde la llegada de las nuevas tecnologías de la información, se ha buscado a través de ellas facilitar tareas a sus usuarios, brindarle nuevos servicios y posibilidades muy variadas. Así fue posible progresivamente el procesamiento automático de la información, y posteriormente la comunicación entre computadores utilizando redes que se extendieron más y más hasta cubrir todo nuestro planeta. La creación de Internet, marca sin lugar a dudas un hito trascendente en la evolución de las nuevas tecnologías, pero el crecimiento exponencial en lo que a procesamiento y comunicaciones digitales se refiere ha alcanzado niveles no imaginados hace tan solo un par de décadas. En nuestros días es cada vez más común hablar de dispositivos inteligentes, utilizando un concepto tradicionalmente asociado exclusivamente con el ser humano.

---

[1] CONSEJO ARGENTINO DE RELACIONES INTERNACIONALES (2013).

De esta forma además de los teléfonos inteligentes que son de accesibilidad casi universal en el mundo desarrollado, agregamos los televisores inteligentes, las señales de tránsito inteligentes, vehículos inteligentes, y muchos dispositivos o aparatos que incluyen ese adjetivo en su descripción, y que basan las prestaciones que brindan en las tecnologías de la información y de las comunicaciones.

El amplio y vertiginoso crecimiento en torno a las tecnologías de la información paulatinamente abrió un nuevo espacio para el desarrollo de las actividades humanas: el ciberespacio. Éste se constituyó de acuerdo con la revista The Economist[2] en el quinto dominio de interacción humana luego del terrestre, marítimo, aéreo y espacial. Pero es conveniente especificar a qué nos referimos cuando hablamos de ciberespacio. Existen al respecto múltiples definiciones pero en general coinciden en que abarcan los medios que basados en las tecnologías de la información y las comunicaciones son utilizados para brindar algún servicio. Acorde a lo anterior, y en función de lo que se planteará más adelante es conveniente puntualizar que Internet no es el ciberespacio, aunque constituye una parte muy importante de él.

Este nuevo ámbito virtual de interacción humana, que inicialmente fue abierto y buscó hacer disponible información y nuevas posibilidades, resultó campo fértil para que actividades mal intencionadas o ilícitas comenzaran a desarrollarse al igual que anteriormente lo hacían en el mundo real. En tal sentido las tradicionales amenazas mutaron su forma y ámbito de actuación, pasando ahora a accionar en el ciberespacio. Términos como ciberdelito, cibercrimen, ciberactivismo, ciberterrorismo, ciberespionaje, ciberataque, ciberseguridad entre otros surgen como analogía a los anteriores y pasan a constituirse en nuevas amenazas en el ámbito cibernético.

Como consecuencia de la aparición de estas nuevas amenazas, los estados han debido encarar primeramente una transformación de sus estructuras y crear nuevas organizaciones para enfrentarlas. De igual forma, los marcos normativos han debido ser actualizados para perseguir y dar captura a quienes utilizan este nuevo ámbito para cometer actividades ilícitas. La República Oriental del Uruguay, al igual que las demás naciones, se encuentra en este proceso, y ha realizado importantes avances en la materia.

Normativa Nacional

La Ley 18.650[3] fue aprobada en el año 2010 y constituye luego de la Constitución de la República el Marco para la Defensa Nacional del País. La misma define en su artículo 1º la Defensa Nacional como sigue:

> 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.

Destaca en la definición realizada por la norma el carácter civil y militar de la defensa, lo que involucra y compete a todos los ciudadanos de la República. Además especifica finalmente su objetivo que es contribuir a generar las condiciones para el bienestar de la población. Se entiende naturalmente que cualquier actividad o acto que atente contra ese bienestar será objeto de la Defensa Nacional.

---

[2] THE ECONOMIST (2010).
[3] PODER LEGISLATIVO (2010)

La norma[4] a continuación establece en su artículo 2º las características de esa Defensa Nacional:

> La Defensa Nacional constituye un derecho y un deber del conjunto de la ciudadanía, en la forma y en los términos que se establecen en la Constitución de la República y en las leyes. Es un bien público, una función esencial, permanente, indelegable e integral del Estado. En su instrumentación confluyen coordinadamente las energías y los recursos del conjunto de la sociedad.

En este caso, se establece que la Defensa constituye un derecho y deber para toda la ciudadanía, y determina que el estado es el único que puede cumplir esa función. Con estas definiciones realizadas en su primer capítulo, la ley encuadra los conceptos fundamentales sobre su asunto.

El País aprobó además por decreto presidencial en el año 2014 su Política de Defensa Nacional[5]. Este documento comienza definiendo el escenario estratégico actual y el escenario futuro, pasando luego a establecer los intereses nacionales que inspiran al País como preámbulo de la determinación de los objetivos permanentes y estratégicos de la Defensa Nacional.

Una vez establecidos los objetivos mencionados, se identifican los posibles obstáculos a enfrentar, dentro de los cuales se menciona el Crimen Organizado. Dentro de este se incluye[6]: "[…] delitos como el narcotráfico, tráfico ilegal de armas, el lavado de activos, la trata de personas, la corrupción y el crimen cibernético, entre otros".

De igual forma se establece más adelante en el citado documento que otro posible obstáculo para lograr los objetivos de la Defensa Nacional es la Materialización del espionaje y los ataques cibernéticos[7]. A este respecto se establece que:

> En la actualidad se da en forma reiterada el espionaje por parte de Empresas, Organismos o Estados extra-regionales a los gobiernos de la región, las empresas públicas, así como a empresas privadas u organismos de la sociedad civil con el fin de captar ilícitamente información para obtener ventajas económicas y el control político, militar o social, en el plano estratégico de los países.

La Política de Defensa Nacional, finalmente establece sus lineamientos estratégicos, diferenciando los aspectos nacionales de los internacionales. Entre los primeros incluye: "Proteger al Uruguay de ataques cibernéticos y preservar la reserva de datos producto de la gestión estatal y privada, tanto a nivel nacional como regional, en cuanto esta última corresponda". El lineamiento especificado encauza las actividades de ciberdefensa o ciberseguridad que pueda realizar el País.

Como corolario de las normas presentadas, el Uruguay es encuentra próximo a aprobar su Política Militar de Defensa. La misma se encuentra en etapa de borrador actualmente, pero incluirá sin lugar a dudas lineamientos para el empleo de los recursos militares en el ámbito cibernético, alineados con el marco legal ya aprobado.

---

4 Ibíd.
5 PODER EJECUTIVO (2014).
6 Ibíd. Pág. 22.
7 Ibíd. Pág. 23.

ESTRUCTURAS NACIONALES Y COOPERACIÓN

Situación General del País

De acuerdo con los datos publicados por el Banco Mundial[8], 61,5 de cada 100 habitantes del país son usuarios de Internet. Este guarismo, que resulta bastante alto en la región, se debe a la promoción por parte del estado de diferentes políticas que favorecen el acceso a través de medios tanto alámbricos como inalámbricos. En este sentido, además se han aprobado diferentes normas que han procurado desarrollar el gobierno electrónico, a la vez que garantizar un adecuado nivel de seguridad.

En lo relativo a garantizar el mencionado nivel de seguridad, algunas de las medidas adoptadas incluyen el desarrollo de una legislación que acompañe el desarrollo de las nuevas tecnologías, la capacitación de quienes las utilizan[9], la creación de políticas de seguridad cibernética[10] en todos los organismos estatales, y la capacidad de detección y respuesta a incidentes cuando ocurran.

A continuación se detallarán las principales agencias del país actualmente responsables de la ciberseguridad y ciberdefensa, encargadas de prevenir un ataque y eventualmente llevar adelante una defensa si se materializa el mismo. Si bien como se detallará más adelante, no existe a la fecha una estrategia nacional definida para la materia, la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC) dependiente de la Presidencia de la República, a través del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) constituye el primer escalón encargado de la seguridad y defensa cibernética del país.

A nivel de los ministerios de Defensa Nacional y del Interior, existen también organizaciones encargadas de brindar la seguridad y defensa cibernética. En el caso del primer ministerio mencionado, se explican sus características más adelante. En el caso del Ministerio del Interior, la Unidad de Delitos Cibernéticos de la Policía Nacional es el organismo que tiene a su cargo la investigación de los delitos cibernéticos.

La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC)

De acuerdo a lo establecido en su propia web, AGESIC “fue creada en diciembre de 2005 con la denominación "Agencia para el Desarrollo de Gobierno Electrónico" (Artículo 72 - Ley Nº17.930) y su funcionamiento fue reglamentado en junio de 2006 (Decreto 205/006)”[11]. Su misión es:

> Liderar la estrategia de implementación del Gobierno Electrónico del país, como base de un Estado eficiente y centrado en el ciudadano, e impulsar la Sociedad de la Información y del Conocimiento como una nueva forma de ciudadanía, promoviendo la inclusión y la apropiación a través del buen uso de las tecnologías de la información y de las comunicaciones.

---

8 BANCO MUNDIAL (2016)

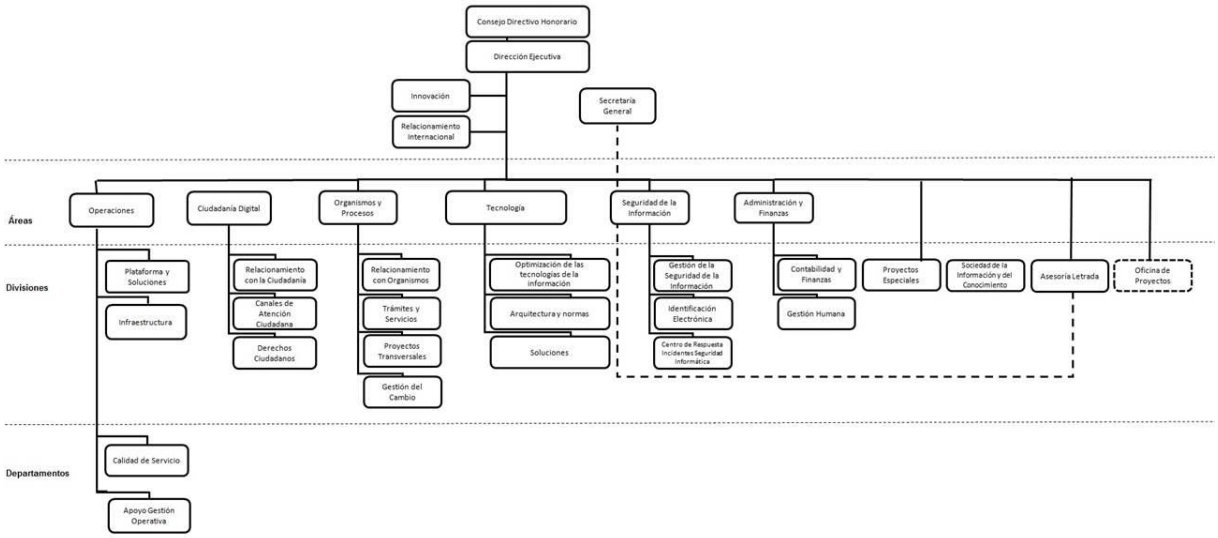
9 En todos los niveles educativos y etarios.

10 El Decreto del Poder Ejecutivo 452/2009, estableció que todos los organismos estatales deben desarrollar su política de seguridad cibernética.

11 AGESIC (2016). Disponible en <http://agesic.gub.uy/innovaportal/v/83/1/agesic/normativa-asociada.html?padre=33&idPadre=33>.

La agencia está organizada en base a seis áreas dependientes de una Dirección Ejecutiva, y veintiuna divisiones que dependen de una de las áreas, o directamente de la dirección. Una de las áreas es la de Seguridad de la Información como puede observarse en la Figura 1.

Figura 1 – Organigrama de AGESIC



Fuente: Página web de AGESIC[12]

Del área de Seguridad de la Información dependen las divisiones de Gestión de Seguridad de la Información, Identificación Electrónica y el Centro de Respuesta a Incidentes de Seguridad Informática. Cada una de estas divisiones tiene cometidos específicos que en su conjunto coadyuvan a obtener un nivel de seguridad adecuado, y es AGESIC quien establece las directivas asociadas y promueve su cumplimiento por parte de todas las dependencias gubernamentales.

Poco después de su creación, en el año 2007 AGESIC recibió la función de "impulsar el avance de la Sociedad de la Información y del Conocimiento, promoviendo que las personas, las empresas y el Gobierno realicen el mejor uso de las tecnologías de la información y las comunicaciones"[13]. Este cometido lo ha cumplido a través del desarrollo de una Agenda Digital que periódicamente[14] se desarrolla basada en un consenso entre diferentes actores, y que constituye en los hechos la política digital del país para el período considerado.

[12] AGESIC (2016). Disponible en <http://agesic.gub.uy/innovaportal/v/92/1/agesic/organigrama.html?padre=57&idPadre=57>

[13] PODER LEGISLATIVO (2007) Art. 118.

[14] En general asociada a los períodos de gobierno.

El Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy)

Como se expuso anteriormente, este centro depende de AGESIC. El mismo fue creado en el año 2008 por la Ley 18.362, la cual establece que su cometido será "difundir las mejores prácticas en el tema, centralizar, coordinar la respuesta a incidentes informáticos y realizar las tareas preventivas que correspondan"[15]. Más adelante, en el año 2009 al procederse a la reglamentación de la mencionada norma, a través del Decreto No. 451[16] se establece que el CERTuy "protegerá los sistemas informáticos que soporten activos de información críticos del Estado, así como los sistemas circundantes a éstos".

El decreto mencionado profundiza además los cometidos derivados del definido originalmente en la ley. Los mismos son[17]:

> a) Asistir en la respuesta a incidentes de seguridad informática a los organismos estatales afectados. b) Coordinar con los responsables de la seguridad de la información de los organismos estatales para la prevención, detección, manejo y recopilación de información sobre incidentes de seguridad informática. c) Colaborar y proponer normas destinadas a incrementar los esfuerzos con la finalidad de aumentar los niveles de seguridad en los recursos y sistemas relacionados con las Tecnologías de la Información y la Comunicación (TIC) en el Estado. d) Asesorar y difundir información para incrementar los niveles de seguridad de las TIC, desarrollar herramientas, técnicas de protección y defensa de los organismos. e) Alertar ante amenazas y vulnerabilidades de seguridad en sistemas informáticos de los organismos. f) Realizar las tareas preventivas que correspondan. g) Coordinar planes de recuperación de desastres y realizar un análisis forense del incidente de seguridad informática reportado. h) Centralizar los reportes y llevar un registro de toda la información sobre incidentes de seguridad informática ocurridos en sistemas informáticos del Estado y reportados al CERTuy. i) Fomentar el desarrollo de capacidades y buenas prácticas así como la creación de equipos de respuesta ante incidentes de seguridad informática (CSIRT) para mejorar el trabajo colaborativo. j) Interactuar como único interlocutor nacional en las comunicaciones con organismos nacionales e internacionales de similar naturaleza.

Basado en sus cometidos, el CERTuy en caso de incidentes de seguridad informática en el país coordina con el CSIRT-ANTEL[18], con otros CSIRT regionales y organizaciones internacionales. El Centro es quien lleva la estadística sobre ataques cibernéticos y es el encargado de emitir alertas sobre riesgos emergentes. La Figura 2 presenta la gráfica correspondiente a los ataques cibernéticos registrados en el País en 2015.

Figura 2 – Estadística de Incidentes 2015

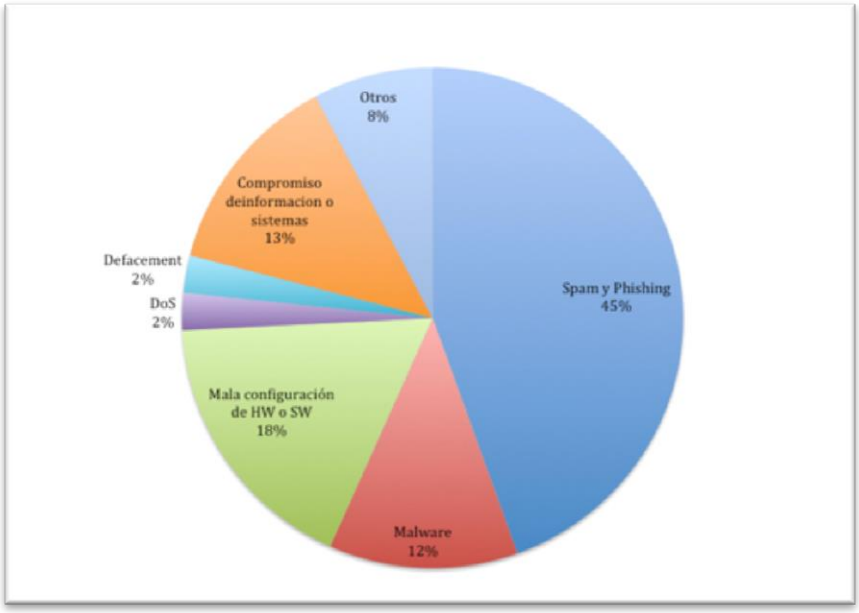
---

15 PODER LEGISLATIVO (2008) Art. 73.

16 PODER EJECUTIVO (2009) Capítulo I - Disposiciones Generales Artículo 1º.- Ámbito Objetivo.

17 Ibíd. Capítulo I - Disposiciones Generales Artículo 4º.- Cometidos.

18 Administración Nacional de Telecomunicaciones. Empresa estatal, es la principal empresa de telecomunicaciones nacional que brinda servicios de telefonía fija, móvil, de banda ancha y de datos. La misma cuenta con la mayor porción del mercado en las áreas mencionadas.



Fuente: Página web de CERTuy[19]

La gráfica presentada se elaboró en base a los 577 ataques registrados[20] durante el año. Ese número corresponde a un 20 % más de los ataques registrados por el Centro durante el año anterior.

Centro de Respuesta a Incidentes de Seguridad Cibernéticos de Defensa (DCSIRT)

En abril del año 2015 se creó en el ámbito del Ministerio de Defensa Nacional en Centro de Respuesta a Incidentes de Seguridad Cibernéticos de Defensa (DCSIRT). Su creación representa la primera organización en el ámbito específico de la Defensa Nacional encargada de atender los asuntos de ciberdefensa. La comunidad objetivo a la que dirige su acción son las organizaciones dependientes del propio 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.

Además de las eventuales acciones correctivas una vez que se materialice un ataque, el Centro se fija como objetivo medidas preventivas para minimizar su impacto. Entre ellas se puede mencionar la concientización en Gestión de Seguridad de la Información y la implementación de la Política de Gestión en Seguridad de la Información en el propio Ministerio entre otras. En este sentido, desde el año 2014 en el ámbito del Centro de Estudios Nacionales (C.AL.E.N.)[21], se realizan cursos sobre ciberseguridad dirigidos a profesionales provenientes del propio Ministerio, de otros organismos del estado e incluso del ámbito privado vinculados o simplemente interesados en la materia.

---

19 CERTUY (2016)

20 Es importante destacar que muchos de los incidentes que ocurren no se registran ya que no son reportados, ya sea porque la persona o entidad atacada le resta importancia a hacerlo, o por razones de reserva prefiere no hacerlo.

21 El Centro de Altos Estudios Nacionales constituye el Colegio de Defensa del Uruguay. El mismo depende del Ministerio de Defensa nacional.

El DCSIRT a partir de su creación pasa a formar parte de la estructura nacional de respuesta a incidentes, y trabaja a nivel nacional en estrecha coordinación con el ya mencionado CERTuy. El Ministerio integra además el Consejo Asesor Honorario de Seguridad de la Información (CAHSI) junto a otras instituciones nacionales[22].

Fuera de fronteras el DCSIRT para cumplir con su cometido integra igualmente con múltiples redes y equipos de respuesta como ser "el Comité Interamericano Contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA) y la de Ministerios de Defensa en el marco de la Unión de Naciones Suramericanas (UNASUR)"[23].

ESTRATEGIA DE CIBERSEGURIDAD

Como se ha expresado anteriormente, el País se encuentra en fase de desarrollo de su estrategia nacional de ciberseguridad, no contando actualmente con la misma. Sin embargo, los marcos legales aprobados, junto con las estructuras de alerta y de respuesta ya creadas han demostrado que se avanza en la dirección correcta para ese desarrollo.

El pasado mes de marzo, fue publicado un informe sobre ciberseguridad en América Latina y el Caribe[24] realizado por la Organización de Estados Americanos y el Banco Interamericano de Desarrollo. El extenso estudio realizado por múltiples expertos desarrolló un Modelo de Madurez de Capacidad de Seguridad Cibernética para evaluar cada uno de los países. Este modelo mide cuarenta y nueve indicadores agrupados en las siguientes cinco áreas: 1) Política y estrategia nacional de seguridad cibernética; 2) Cultura cibernética y sociedad; 3) Educación, formación y competencias en seguridad cibernética; 4) Marco jurídico y reglamentario; y 5) Normas, organizaciones y tecnologías.

Cada uno de los indicadores, fue evaluado individualmente para todos los países de América Latina y el Caribe, estableciéndose cinco niveles de madurez. Los mismos se definieron como: Inicial, Formativo, Establecido, Estratégico y Dinámico, correspondiendo a cada uno un valor de uno a cinco respectivamente.

Como es posible observar en la Figura 3, el País recibe en cuatro de los seis indicadores del área de Política y estrategia una evaluación de estado Establecido o Estratégico, siendo los dos indicadores restantes evaluados como en estado Formativo.

---

[22] El Consejo Asesor Honorario de Seguridad de la Información (CAHSI) está integrado por representantes de la Pro Secretaría de la Presidencia de la República, del Ministerio de Defensa Nacional del Ministerio del Interior, de ANTEL y de la Universidad de la República.

[23] MINISTERIO DE DEFENSA NACIONAL (2016).

[24] ORGANIZACIÓN DE ESTADOS AMERICANOS, BANCO INTERAMERICANO DE DESARROLLO (2016).

Figura 3 – Valoración para Uruguay de Indicadores correspondientes al Área Política y Estrategia

Fuente: Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?[25]

El informe basa su evaluación en las siguientes consideraciones:

> La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) incluyó el tema de seguridad cibernética en su Agenda Digital quinquenal para 2011-2015, y enfatizará aún más la seguridad cibernética en el próximo plan a 5 años. Por otra parte, la Política de Defensa Nacional de Uruguay incorpora medidas de defensa cibernética. El mecanismo nacional de respuesta a incidentes de seguridad informática del país, el CERTuy establecido en 2008, coordina regularmente con otros CSIRT regionales y organizaciones internacionales. Además de respuesta a incidentes, el CERTuy suministra registros estadísticos sobre ataques cibernéticos y emite alertas sobre riesgos emergentes. Uruguay también se basa en el análisis y la respuesta de incidentes del CSIRT-ANTEL de la Administración Nacional de Telecomunicaciones, que fue fundada en 2005 para abordar cuestiones relacionadas con los datos y servicios de telefonía celular. Por otra parte, la Política de Defensa Nacional de Uruguay incorpora medidas de defensa cibernética.[26]

Sin lugar a dudas queda un largo camino por recorrer para llegar a tener una completa estrategia de ciberdefensa y ciberseguridad, así como las estructuras conjuntas e integradas para enfrentar un eventual ataque. Sin embargo es posible delinear algunas características que muy probablemente tendrán las mismas.

En cuanto a la creación de una estrategia de empleo de medios en el ciberespacio, sin dudas la misma se ajustará a los preceptos que establece nuestra legislación en lo referido al ejercicio del derecho de legítima defensa consagrado en la Carta de las Naciones Unidas y se reserva el uso de la fuerza para los casos de agresión militar[27]. En este sentido, un ataque cibernético por parte del estado se daría únicamente ante una agresión externa en ese ámbito.

La creación de estructuras de ciberdefensa militares, seguramente estarán encuadradas en el ámbito del Estado Mayor de la Defensa que depende del Ministerio de Defensa Nacional y le compete tanto la elaboración doctrinaria, como la planificación y el mando de las operaciones conjuntas de las fuerzas armadas.

---

[25] Ibíd. Pág. 109.
[26] Ibíd. Pág. 108.
[27] PODER LEGISLATIVO (2010) Art. 4º.

CONCLUSIONES

La disponibilidad creciente de las nuevas tecnologías de la información y de las comunicaciones ha dado lugar a la creación de un nuevo ámbito de interacción entre los seres humanos. En este lugar virtual se ofrecen y brindan múltiples servicios de gran utilidad, pero ha dado lugar a la realización de actividades ilícitas de diferentes características.

La realización de actividades que afecten la seguridad de los diferentes países por parte de otras naciones, organizaciones o individuos es posible, y puede causar efectos devastadores. Por esto, los estados deben adaptar su legislación y crear nuevas estructuras para combatir las nuevas amenazas que surgen. El Uruguay, al igual que los restantes países del orbe ha modernizado su marco legal y ha incluido a las amenazas provenientes del ciberespacio entre las que pueden afectar el bienestar de su población, pasando estas a ser objeto de la Defensa Nacional.

En virtud de lo anterior, se han estructurado políticas y creado al más alto nivel organizaciones para enfrentar las nuevas amenazas. El País ha identificado como primordial fomentar el gobierno electrónico y a la vez estructurar a nivel nacional redes que permitan brindar seguridad cibernética y garantizar el libre uso de los recursos reales y virtuales. Estas redes tienen como base la concientización de la población en lo referente a seguridad de la información y su capacitación para utilizar de la mejor forma los servicios.

A pesar de que el País carece de una estrategia de ciberseguridad, ha sido evaluado positivamente en un reciente informe conjunto del Banco Interamericano de Desarrollo y la Organización de Estados Americanos.

De igual forma se carece actualmente de una organización conjunta a nivel Fuerzas Armadas que tenga como cometido específico repeler ataques cibernéticos que afecten la seguridad nacional o eventualmente realizarlos como respuesta a un ataque anterior.

BIBLIOGRAFÍA

AGESIC. *Página Web.* [en línea] 2016. Disponible en <http://agesic.gub.uy> Fecha de consulta 20 mar.2016.

BANCO MUNDIAL. *Internet users (per 100 people)*. [en línea] 2016. Disponible en: <http://data.worldbank.org/indicator/IT.NET.USER.P2> Fecha de consulta 15 mar.2016**.**

CERTUY. *Página Web*. [en línea] 2016. Disponible en <https://www.cert.uy/inicio/novedades/ amenazas_y_alertas/ estadistica_de_incidentes_certuy_2015> Fecha de consulta 20 mar.2016.

CONSEJO ARGENTINO DE RELACIONES INTERNACIONALES. *Ciberdefensa-Ciberseguridad Riesgos y Amenazas.* [en línea] 2013. Disponible en: <http://www.cari.org.ar/pdf/ciberdefensa_riesgos _amenazas.pdf.> Fecha de consulta 15 mar.2016.

MINISTERIO DE DEFENSA NACIONAL. *Página Web.* [en línea] 2016. Disponible en <http:// www.mdn.gub.uy/?q=node/3994> Fecha de consulta 25 mar.2016**.**

ORGANIZACIÓN DE ESTADOS AMERICANOS, BANCO INTERAMERICANO DE DESARROLLO. *Ciberseguridad ¿Estamos Preparados en America Latina y el Caribe?* [en línea] 2016. Disponible en < https://publications.iadb.org/bitstream/handle/11319/7449/Ciberseguridad-Estamos-preparados-en-America-Latina-y-el-Caribe.pdf?sequence=2> Fecha de consulta 25 mar.2016**.**

PODER EJECUTIVO. *Decreto 451/009* [en línea] 2009. Disponible en <https://www.cert.uy/ wps/wcm/connect/certuy/8f327272-c58e-4a63-8bb7-b6d37db4ec22/Decreto+451-009.pdf?MOD= AJPERES&CONVERT_TO=url&CACHEID=8f327272-c58e-4a63-8bb7-b6d37db4ec22> Fecha de consulta 20 ene.2016**.**

PODER EJECUTIVO. *Decreto 105/014* [en línea] 2009. Disponible en <http://www.calen.edu.uy/ noticias/2014/05_mayo/pdf/Politica-de-Defensa-Nacional-CODENA-Uruguay-2014.pdf> Fecha de consulta 10 ene.2016**.**

PODER LEGISLATIVO. *Ley Nº 18.172* [en línea] 2007. Disponible en < https://parlamento.gub.uy/ documentosyleyes/leyes/ley/18172?width=800&height=600&hl=en_US1&iframe=true&rel=nofollow> Fecha de consulta 10 ene.2016.

PODER LEGISLATIVO. *Ley Nº 18.362* [en línea] 2008. Disponible en < https://parlamento.gub.uy/ documentosyleyes/leyes/ley/18362?width=800&height=600&hl=en_US1&iframe=true&rel=nofollow> Fecha de consulta 10 ene.2016.

PODER LEGISLATIVO. *Ley Nº 18.650* [en línea] 2010 Disponible en <https://parlamento.gub.uy/ documentosyleyes/leyes/ley/18650?width=800&height=600&hl=en_US1&iframe=true&rel=nofollow> Fecha de consulta 10 ene.2016**.**

THE ECONOMIST. *Ciberwar.* 2010. Volúmen 396, número 8689, 3-9 Julio.