Ciber ataques

¿Está Brasil preparado?

Major Luis Eduardo Pombo Celles Cordeiro, Fuerza Aérea de Brasil

Introducción

Oficialmente, la importancia del sector cibernético fue considerada por primera vez como un asunto de alta política por el gobierno brasileño en 2008, (lo que significa que son asuntos relacionados con la supervivencia del estado mismo) cuando se publicó una versión de la *Estrategia Nacional de Defensa (END)*, que define el ciberespacio como una de las tres áreas estratégicas principales (junto con la nuclear y la espacial) para la seguridad nacional.[1]

Se puede decir con seguridad que el gobierno federal hace responsable de la ciberdefensa a tres instituciones principales:

- El Gabinete de Seguridad Institucional (GSI, por sus siglas en portugués),
  - La *Agencia Brasileña de Inteligencia* y
  - El *Departamento de Seguridad de Informaciones y Comunicaciones* (DSIC).
- El Ministerio de Defensa (MD, por sus siglas en portugués) y
  - El Centro de Defensa Cibernética (CDCiber)
- El Ministerio de Justicia (MJ, por sus siglas en portugués).[2]
  - El Servicio de Represión de Delitos Cibernéticos (SRCC)

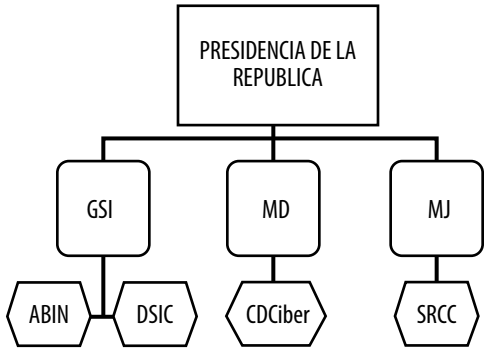

Figura 1: Cuadro de ciberdefensa brasileña en el poder Ejecutivo
Fuente: el autor, 2016.

En los cuatro últimos años, Brasil organizó seis eventos principales

- Cumbre Río + 20 en 2012,
- Copa Confederaciones en 2013,
- Día Mundial de la Juventud en 2013,
- Copa del Mundo de Fútbol en 2014,
- Juegos Olímpicos y Paralímpicos de Verano de 2016)

Sin ningún incidente cibernético principal informado, lo que podría considerarse como prueba de que, al menos, a nivel técnico, la preparación de las personas involucradas en la ciberdefensa de la red protegida resultó efectiva.

Por lo tanto, este artículo examinará el nivel de gestión aplicado al sector cibernético dentro del gobierno federal brasileño, respondiendo a la pregunta siguiente: una vez que se haya definido la política de seguridad del estado para el sector cibernético, ¿es viable aplicarlo de forma que todos los involucrados (GSI, MJ, MD) puedan actuar de forma descentralizada bajo una sola supervisión?

Para responder a esto, este artículo analiza primero la importancia del sector cibernético como asunto de alta política, y sus relaciones con la defensa nacional de Brasil. Después se presentarán las organizaciones estatales y sus responsabilidades, analizando la necesidad de una gestión centralizada y la ejecución descentralizada de las tareas. Por último, se presentará una solución de gestión, seguida por las conclusiones finales.

Al final, este artículo trata de mejorar la capacidad de la Defensa del Estado de Brasil usando una herramienta de gestión estratégica en un área específica que es indispensable para la sociedad contemporánea brasileña: el sector cibernético.

El sector cibernético y la defensa nacional

Según Choucri, hay presente un elemento sin precedentes en las relaciones de poder actuales: la importancia del sector privado como agente de poder catalizador. Si hasta ahora se considera que el estado es el único representante legítimo de los intereses de la nación en el escenario político de relaciones internacionales, tal vez sea necesario reflexionar sobre esta correlación teniendo en cuenta la relevancia del sector privado, y esto es más cierto cuando el tema es cibernético.[3]

También es importante resaltar que una de las características principales de este cambio es el individualismo de la persona que, mediante sus propios dispositivos personales, puede comunicarse con una gran cantidad de personas en un período corto, aumentando su poder de influir

y ser influenciado. Probablemente nunca se ha visto en la historia de las relaciones humanas que el individuo haya ganado tanto poder.[4]

Para Brasil, la importancia del sector cibernético es explícita en la Estrategia Nacional de Defensa (END, por sus siglas en portugués), cuando considera que el sector cibernético es una de las tres áreas estratégicas de defensa y, en particular, para la *Fuerza Aérea de Brasil* (FAB, por sus siglas en portugués), cuando define como objetivo que la FAB debe poder operar en un área no solamente internamente, sino también con otras Fuerzas Armadas en operaciones conjuntas dentro de las guías estratégicas de la FAB establecidas por la END.[5] Esto nos lleva a un nuevo entendimiento de los asuntos cibernéticos con un cambio de estado de baja política (ordinaria para el funcionamiento del estado) a alta política (vital para la supervivencia del estado) como vimos en END.

No obstante, un problema que se debe observar es que desde un punto de vista tecnológico hoy esto es imposible, que el estado asuma todas las responsabilidades del sector cibernético porque el sector privado o los ciudadanos cederán su reparto de poder (poder cibernético) y lo deleguen al estado. Hay dos ejemplos recientes que apoyan este argumento.

Recientemente algunos jueces brasileños, en más de una ocasión, han prohibido la aplicación Whatsapp afirmando que el programador de software no estaba pasando las conversaciones solicitadas por orden del tribunal. En todos los casos, la primera reacción de los brasileños fue migrar a aplicaciones similares como Viber y Telegram, la segunda fue atacar no solamente al juez sino a todo el sistema judicial brasileño acusándole de megalomanía, falta de empatía, incapacidad funcional, etc. Ninguna prohibición duró más de 48 horas antes de ser revocada en una instancia más alta.[6]

En 2016, durante una *comisión de consulta de delitos cibernéticos* parlamentarios, el jefe de SRCC, el agente Elmer Vicente Coelho, fue enfático para declarar que muchas compañías que operan en el mercado de software, como Whatsapp, no tienen una subsidiaria o un representante en Brasil, y deciden simplemente hacer caso omiso de la ley brasileña. Esto significa que el estado brasileño no tiene poder sobre lo que hace la compañía, aun cuando es uno de los programas de software de comunicación más populares del país.[7]

En este caso, el estado debe actuar con precaución para no exceder su poder sobre las corporaciones privadas y los ciudadanos sin inclinarse hacia el totalitarismo. Por lo tanto, nuestro razonamiento es que una solución debe concentrarse en la organización sistémica del sector en vez del lado operacional (o táctico, en la terminología de la administración civil) del concepto de la "última tecnología", ya que estos conocimientos expertos (operacionales y tácticos) radican en el sector privado.

Según Ferreira Neto, EE.UU. tiene seis agencias concentradas en su defensa de redes nacional e internacionalmente, y el Consejo de Seguridad Nacional es el que define la política del estado para este sector y la ocupación de cada agente (por ejemplo: defender la infraestructura y las medidas extraterritoriales de las redes militares es responsabilidad del Cibercomando de EE.UU. y la infraestructura civil federal es responsabilidad del Departamento de Seguridad Nacional).[8]

El mismo autor cita ejemplos de países que siguieron el modelo de EE.UU. y empezaron a organizarse para defender sus intereses en el entorno virtual:

- El Reino Unido creando la Oficina de Ciberseguridad (OCS, por sus siglas en inglés),
- Canadá con la compañía de Estrategia de Seguridad Cibernética,
- Alemania a través de la Estrategia de *Ciberseguridad para Alemania* y
- Francia a través de la *Defensa y Seguridad de Sistemas de Información: Estrategia de Francia*;
- Incluso habla de la creación de unidades específicas para este sector en China y Corea del Norte.[9]

De esa manera, podemos entender que la última tecnología en el sector cibernético está presente en los países que no solamente se dieron cuenta de la importancia del sector cibernético para su defensa, sino que también, fueron capaces de definir ramas de sus fuerzas de seguridad sobre el asunto. Brasil ha seguido esta línea de razonamiento.

Actores principales sobre defensa de ciberseguridad

Un estudio realizado por Mandarino Junior mostró que había dieciséis órganos diseminados entre ministerios y secretarías, autoridades federales responsables de ayudar y proteger el poder ejecutivo en lo que se refiere a amenazas de ciberseguridad en 2010. Eso hace que sea necesario resaltar unas cuantas consideraciones sobre el tema.[10]

1. La primera es que ninguno de estos órganos tenía ninguna jerarquía o jurisdicción administrativa sobre los otros, ya que cada uno de ellos opera en un campo específico de administración pública. A pesar de que el GSI determina, por ejemplo, las políticas de tecnología de información para todas las agencias federales, no puede determinar si el campo operacional de CDCiber empieza y termina el SRCC-PF de la Policía Federal, ya que cada uno está subordinado a una secretaría diferente. En realidad, cada uno de estos agentes trata de satisfacer sus propias necesidades, lo que es de entender, y por lo tanto no es un "jefe" o "zar" exclusivo que gestione los esfuerzos con un punto de vista estratégico.[11]
2. La segunda consideración es que, cuando hablamos sobre tecnología, no es posible excluir el sector privado del debate. Esto se debe al hecho de que el ciberespacio, accesible a nivel individual en dispositivos móviles, por ejemplo, es solamente posible gracias a la existencia de entornos artificiales que fueron creados y mantenidos por seres humanos, como la internet. Hoy en día, este poder en manos de industrias privadas, desde la fabricación de los componentes que constituyen los dispositivos de conexión a la infraestructura necesaria para que existan las redes.[12]
3. En tercer lugar, el sector privado no domina estas tecnologías, sino que también depende de las mismas tecnologías. Los bancos, las compañías energéticas, mineras y alimentarias, como las demás actividades industriales actuales dependen de esos progresos para poder existir en el mercado actual. Así, quien tenga el poder sobre estos conocimientos también tiene la influencia en los agentes económicos más importantes del estado y, en consecuencia, en el estado mismo.[13]
4. Como cuarta y última consideración personal se resalta que esta influencia sigue siendo más fuerte en la célula madre de una nación: los individuos, que ahora se ven a sí mismos como incapaces de ceder, por ejemplo, la comunicación a través de sus teléfonos celulares o administrar sus vidas usando su computadora personal y sus programas operacionales existentes.

De esta forma podemos ver que, junto con las cuatro organizaciones estatales mencionadas antes (ABIN, DSIC, CDCiber y SRCC), también tenemos el sector privado y al ciudadano, todos ellos involucrados en el ciberespacio, cada uno con sus propias necesidades específicas. Por otra parte, como se identificó la importancia del ciberespacio para la seguridad de la sociedad, el estado tiene la función de protegerla.

Así pues, ahora que hemos podido definir las organizaciones en el sector de seguridad cibernética y podemos concluir especialmente que sus objetivos están diversificados y que el estado tiene la responsabilidad de garantizar la seguridad en el ciberespacio, podemos afirmar que la función del gobierno brasileño debe ser la de coordinador, realizando una gestión centralizada que permita una implementación descentralizada a través de los involucrados.

La publicación del *Libro verde de defensa cibernética* en 2010 puede considerarse una iniciativa para agrupar los esfuerzos en este tema, ya que el GSI trata, por primera vez, de establecer ciertas guías estratégicas potenciales para el sector. No obstante, la complejidad de gestionar tantos intereses puede ser una de las razones por las que, hasta hoy, no hay un *Libro blanco de defensa cibernética,* en el que se defina la política nacional para el sector, consecuencia de un amplio debate entre el gobierno y la sociedad.[14]

En lo que se refiere a este artículo, asumamos que se ha publicado este libro blanco, por lo que Brasil tiene una política nacional de defensa cibernética. Empezando por este escenario, se establece la premisa de que no sería apropiado dejar que justo uno de esas organizaciones sea responsable de la gestión de toda la política, ya que se fijará en el problema según su visión, en busca de lo que esa organización en particular se imagina que son las prioridades y tratará de satisfacer, a su entender, las necesidades.

Al tratar de adoptar una visión integrada sobre el asunto como forma de obtener conocimientos estratégicos sobre el tema, se define una hipótesis: la adopción de una herramienta de gestión estratégica aumentará la capacidad nacional de lograr los objetivos nacionales cuando defina, de forma integradora, la responsabilidad de implementar la política nacional de defensa cibernética permitiendo a esta "oficina cibernética" integrar la visión segmentada real existente en el sector cibernético.

Para corroborar o rebatir esto, usaremos los conceptos ya citados, buscando mostrar una respuesta viable, ya que la importancia de la defensa nacional queda resaltada cuando se comprueba la ausencia de una visión estratégica sobre el tema que dificulta el debate sobre un tema completo e interdisciplinario, porque cada agente observará solamente su propia perspectiva personal sobre el asunto.

Los individuos se preocuparán más de sus necesidades, los agentes privados de sus objetivos y el estado, actuando como órgano representativo de los intereses de las personas, concentrándose en la defensa nacional de Brasil mediante acciones de sus agentes (ABIN, DSIC, CDCiber y SRCC).

No obstante, si la responsabilidad estratégica sobre el tema no está completamente definida, se observa su importancia. Existe pues un factor realmente valioso para la sociedad y, por lo tanto, para la seguridad, proporcionada por el estado y una vulnerabilidad en la capacidad de defensa del estado debido a la ausencia de una visión general del asunto.

De esa forma, podemos observar un escenario en el que los agentes se comportan de forma aislada, motivados por diferentes intereses tanto dentro como fuera de la esfera del gobierno federal. ¿Cómo sería posible coordinar todas esas operaciones de una sola forma sin que interfiera en los intereses individuales?

Como solución a este dilema, la investigación adoptará la gestión estratégica basada en las opiniones de Kaplan y Norton sobre el asunto, aproximando la solución de la creación de una *Unidad de Gestión Estratégica* (UGE, por sus siglas en portugués) como propuesta para ser implementada por el estado brasileño, como solución para tener en cuenta los intereses de todos los agentes involucrados y aumentar la capacidad para lograr los objetivos previstos.[15]

La opción estaba basada en el hecho de que, según lo describe Kaplan y Norton, la UGE es como "[…] *el ingeniero de un reloj refinado que mantiene todos los mecanismos sincronizados a pesar de girar a diferentes velocidades".* Esto significa que un UGE sería capaz de mantener el individualismo de los agentes, supervisar como actúa cada uno de ellos según una política nacional definida por el sector sin interferencia directa en sus individualismos.[16]

No obstante, el uso de la UGE como herramienta fiable para implementar la política nacional de defensa cibernética presenta, al menos, tres preguntas que podrían rebatir la hipótesis de que la adopción de una herramienta de gestión estratégica aumentará la capacidad nacional de alcanzar los objetivos nacionales:

- El número de personas requeridas para implementar y gestionar
- El proceso haría que el proceso fuera imposible, la UGE no se aplica a agencias estatales (dirigidas a la efectividad) porque fue desarrollada por corporaciones civiles (que tratan de generar beneficios), y
- Que los intereses se dispersan entre agentes dentro y fuera del gobierno, haciendo impráctico que se desarrollen soluciones que se adapten a todos los intereses involucrados.

La gestión estratégica basada en la creación de una UGE fue utilizada con éxito por Chrysler Group hacia el 2000, donde se las arreglaron para poner a 13 personas a cargo de propagar y controlar el material relacionado con la tarjeta de puntuación de estrategia a más de 90.000 empleados (KAPLAN; NORTON, 2005). De hecho, una CGU tiene nueve divisiones que, dentro del concepto adoptado, podrían ser gestionadas en teoría por nueve personas.[17]

Si extrapolamos esto a la realidad brasileña, veremos que el personal activo total de las organizaciones mencionadas (ABIN, DSIC, CDCiber y SRCC) es de unas 350.000 personas. Así pues, si hacemos caso omiso de algunos factores endógenos, podemos estimar que una oficina que implemente y gestione la policía de ciberdefensa nacional necesitará a unas 50 personas. Y este equipo sería responsable de hablar con compañías privadas y representantes de la sociedad, desde asociaciones y organizaciones hasta individuos que deseen participar en el proceso.

Evidentemente, esta es una estimación empírica y por lo tanto no es de fiar sin un estudio hecho para confirmar dicha afirmación. No obstante, es correcto indicar que el objetivo de la CGU es verificar si las políticas propuestas se implementan mediante el análisis de indicadores, que su tamaño dependerá de la complejidad y profundidad del tipo de análisis que se vaya a verificar. Así pues, la contingencia de personal requerida será tan grande como la tarea que se vaya a realizar y, así, no habrá problema referente al número de personas involucradas en la implementación del proceso porque variarán según los encargados de tomar decisiones.

En la cuestión de la aplicabilidad en el sector gubernamental, se sabe que el proyecto de la Tarjeta de Puntuación Equilibrada del Ejército de EE.UU. de 2005 fue capaz de desarrollar su propia UGE. La versión militar de la oficina asumió el papel de un programa de comunicación de estrategia influyendo en 13 comandos principales y más de 300 comandos secundarios de todo el mundo, demostrando que, en este caso, los mismos principios se aplican tanto a organizaciones estatales como privadas, demostrando que es posible aplicar la gestión estratégica a través de la UGE a agencias estatales, de modo que puedan aumentar la efectividad de la implementación de políticas nacionales.[18]

Ambas UGE (de Chrysler y del Ejército de EE.UU.) estaban consideradas como una "herramienta de mando y control", diseñada para comprobar los resultados y eliminar la iniciativa. En la práctica ocurría exactamente lo opuesto: las ideas locales podrían pues "ponerse en las agendas de revisiones estratégicas trimestrales y anuales, y adoptar e integrar los mejores conceptos en estrategias empresariales y comerciales".[19]

De esa forma, la UGE no interfiere en las actividades intrínsecas de cada miembro del sistema y tiene la responsabilidad de integrar las actividades relacionadas, gestionando los procesos de gestión estratégica y operacional, y estructurando la inclusión de procesos de administración que podrían ser útiles al ejecutar las actividades relacionadas, y esto está relacionado con la pluralidad de los agentes involucrados.

La diversidad de los intereses no representará un problema para la implementación de la Política Nacional de Defensa Cibernética, ya que la UGE adoptará una visión integral de todo el proceso, tratando de lograr los objetivos estratégicos y, al mismo tiempo, permitiendo lograr los intereses individuales a nivel táctico.

Así pues, al final, la UGE no interfiere en las actividades intrínsecas de cada miembro del sistema y tiene la responsabilidad de integrar las actividades relacionadas, administrando los procesos de gestión estratégica y de operación y estructurando la inclusión de procesos de adminis-

tración que podrían ser útiles para ejecutar las actividades relacionadas. Las decisiones de arriba abajo no son solamente recibidas por los componentes, sino que los ajustes y las opiniones a cada nivel tienen un enlace o un foco que debe dirigirse y procesarse.[20]

Con una comunicación más transparente, toda la sociedad saldrá ganando: las personas encargadas de tomar decisiones a nivel estratégico que propagarán su política, los actores que serán participantes activos en la planificación estratégica y los agentes de la UGE que no podrán ser solamente capaces de implementar la Política Nacional de Defensa Cibernética, sino que también podrán mejorarla.

Conclusión

La sociedad moderna entiende, según los autores citados en este artículo, que las capacidades proporcionadas por el sector cibernético se han convertido en un activo vital en la relación de poder entre el gobierno y los individuos en la sociedad actual y, debido a eso, se toman medidas para garantizar la protección de los intereses nacionales junto al sector cibernético, pero se ha demostrado que esta clase de acción es una tarea difícil, ya que los actores estatales ya no tienen un control total (en el sentido legal) sobre el sector privado cuando el tema es la cibernética.

Los gobiernos, incapaces de ejercer su poder por completo, se han visto forzados a tomar medidas en el campo cibernético concentradas principalmente en capacitar a sus agentes (ya que esos dependen solamente de las decisiones gubernamentales) en vez de en medidas que regulen el sector en el entorno nacional debido a la complejidad del asunto.

No obstante, observamos que las estructuras que se están armando con este objetivo en Brasil tienen sus políticas definidas basándose en sus propias necesidades, sin un solo actor individual a nivel estratégico conduciendo a una visión no integral del asunto. Si consideramos el estado brasileño como un sistema exclusivo, se observa que dicha decisión proporciona soluciones aisladas y diversificadas, dificultando la planificación estratégica, ya que podría crear una interrupción o superposición de áreas de responsabilidad y, en consecuencia, una degradación de la capacidad de defensa.

A partir del principio de que Brasil estableció una Política Nacional de Defensa Cibernética, se presentó la existencia de una diversidad de organizaciones con diferentes objetivos dentro y fuera del gobierno, y se explicó cómo podría ser un problema, ya que todos ellos deben permanecer bajo el mismo paraguas en relación a la ciberdefensa nacional. Como solución a este dilema, se propuso el concepto de Unidad de Gestión Estratégica (UGE) como solución válida.

De esa forma, entendemos que la adopción de la UGE permitirá la implementación y el desarrollo de una futura Política Nacional de Ciberdefensa, y debido a eso aumentaría la capacidad del gobierno brasileño para alcanzar los objetivos nacionales, una vez que implemente un control centralizado y la ejecución descentralizada de las actividades estatales para el sector cibernético mediante gestión estratégica, respondiendo a la pregunta hecha al principio de este trabajo y por lo tanto presentan una línea de acción sobre cómo el estado brasileño puede gestionar el sector cibernético para mejorarlo.

Ciertamente, dicho hecho no cierra los debates sobre el asunto, por el contrario, creemos que estimula nuevas preguntas sobre la importancia del tema cibernético dentro del concepto de Poder Nacional, así como el protagonismo del GSI como agente central de una futura política nacional de defensa cibernética, ya que tiene la responsabilidad de coordinar el sector cibernético dentro del gobierno federal, pero no tiene la autoridad de gestionar esos asuntos de forma efectiva. Estar preparado para responder a estas preguntas, entre otras, es un desafío para el Brasil actual. ❑

Notas

1. BRASIL 2008, 18 de diciembre. Estrategia Nacional de Defesa (Estrategia Nacional de Defensa). Brasilia, 2008. Disponible en: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm>. Accedida el 20 de octubre de 2016.

2. ALMEIDA, Nival Nunes de; SOUZA, Eduardo André Araújo de. Arcabouço Político-Administrativo do Espaço Cibernético Brasileiro (Estructura política y administrativa del ciberespacio brasileño). El artículo presentado en la IX Cumbre Nacional

de la Asociación Brasileña de Estudios de Defensa (6 a 8 de julio de 2016). Disponible en: <www.enabed2016.abedef.org/resources/anais/3/1466280464_ARQUIVO_IX_ENABED_ARCABOUCO_EDUARDO_NIVAL.pdf>. Accedida el 18 de octubre de 2016.

3. CHOUCRI, Nazli. Cyberpolitics in International Relations (Ciberpolítica en relaciones internacionales). (Cambridge: MIT Press, 2012), 227.

4. Ibid., 228-230.

5. BRASIL DE 2012. Estrategia Nacional de Defesa (Estrategia Nacional de Defensa). (Brasilia, 2008), 6. Disponible en: <http://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf>. Accedida el 28 de octubre de 2016.

6. VICENTE, Elmer Coelho. Testimony in the commission on cyber crimes (Testimonio sobre la comisión de delitos cibernéticos) (agosto de 2015). (Brasilia: Cámara de los Diputados, 28 de agosto de 2015). Disponible en: <http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar- de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/notas-taquigraficas>. Accedida: 5 de enero de 2016.

7. Ibid.

8. FERREIRA NETO, Walfredo Bento. Segurança e Defesa Cibernética: da fronteira física aos muros virtuais (Seguridad y defensa cibernética: de las fronteras físicas a los muros virtuales) (Recife: Editora UFPE, 2014), 81.

9. Ibid, 82.

10. MANDARINO JUNIOR, Raphael. Segurança e Defesa do Espaço Cibernético Brasileiro (Seguridad y defensa del espacio cibernético brasileño) (Recife: Cubzac, 2010), 119.

11. ALMEIDA, Nival Nunes de; SOUZA, Eduardo André Araújo de. Arcabouço Político-Administrativo do Espaço Cibernético Brasileiro (Estructura política y administrativa de ciberespacio brasileño). Artículo presentado en la IX Cumbre Nacional de la Asociación Brasileña de Estudios de Defensa (6 a 8 de julio de 2016). Disponible en: <www.enabed2016.abedef.org/resources/anais/3/1466280464_ARQUIVO_IX_ENABED_ARCABOUCO_EDUARDO_NIVAL.pdf>. Accedida el 18 de octubre de 2016.

12. CHOUCRI, Nazli. Cyberpolitics in International Relations (Ciberpolítica en relaciones internacionales). (Cambridge: MIT Press, 2012), 230-233.

13. Ibid.

14. GABINETE DE SEGURIDAD INSTITUCIONAL - GSI. Livro Verde de Segurança Nacional (Libro verde de seguridad nacional). (Brasilia, Presidencia de la República, 2010), 05-15.

15. KAPLAN, Robert S.; NORTON, David P. The Office of Strategy Management (La oficina de gestión estratégica). (Harvard Business Review), 05. Disponible en: <https://hbr.org/2005/10/the-office-of-strategy-management>. Accedida el 23 de octubre de 2014.

16. KAPLAN, Robert S.; NORTON, David P. The Office of Strategy Management: emerging roles and responsibilities (La Oficina de Gestión Estratégica: funciones y responsabilidades emergentes). (Informe de tarjeta de puntuación equilibrada, julio a agosto de 2008), 02. Tomo 10. Número 4.

17. KAPLAN, Robert S.; NORTON, David P. The Office of Strategy Management (La Oficina de Gestión Estratégica). (Harvard Business Review), 05. Disponible en: <https://hbr.org/2005/10/the-office-of-strategy-management>. Accedida el 23 de octubre de 2014.

18. Ibid.

19. Ibid.

20. Ibid.

Mayor Luis Eduardo Pombo Celles Cordeiro, Fuerza Aérea de Brasil. (Maestría, Gestión Pública; Universidad de la Fuerza Aérea, Río de Janeiro) es responsable de la disciplina del empleo de la fuerza militar en la Escuela para Oficiales de Escuadrón de la Fuerza Aérea Brasileña en Río de Janeiro. Además, prepara los planes de estudio para los cursos y enseña la doctrina básica de la Fuerza Aérea. Antes de ocupar su puesto actual, se desempeñó en calidad de oficial de administración de personal en el 5/8 Escuadrón, Base Aérea Santa María. Fue egresado distinguido de la Escuela para Oficiales de Escuadrón, Base Aérea Maxwell, Alabama. El Mayor Pombo Celles es un piloto con más de 3,500 horas de vuelo en el T-25, AT-26, AT-27, C-97, C-98, U-42, H-50 H-1H y H-60L.