Escenarios Actuales, año 28, mayo, Nº 1 (2023), pp. 175-191
Centro de Estudios e Investigaciones Militares
Santiago de Chile
ISSN 0717-6805

Ciberseguridad: un desafío para los Juegos Panamericanos y Parapanamericanos de Chile 2023, la experiencia de Brasil

Teniente Coronel Nicolás Kaiser Onetto[1]

Resumen

Los Juegos Panamericanos y Parapanamericanos de 2023 representan un importante desafío para el Estado de Chile, no solo porque es el mayor evento realizado posterior al Mundial del 62 o porque hay una gran cantidad de recursos comprometidos, sino porque las actuales condiciones del entorno de seguridad podrían afectar el normal desarrollo, el bienestar de competidores y público en general que asiste. La seguridad de los juegos no solo se puede abordar desde una perspectiva tradicional, también se debe considerar el ciberespacio como un dominio a ser afectado. Brasil, entre los años 2007 y 2016, tuvo la responsabilidad de organizar varios eventos de las características de Santiago 2023, acumulando una vasta experiencia desde la perspectiva de este dominio. La ciberseguridad de los Juegos requiere de una planificación y coordinación que permita la adecuada articulación de los modos y medios en función del fin, que es el buen desarrollo. Considerando la poca experiencia de Chile en estos tipos de eventos, se busca extraer lecciones de las acciones ejecutadas por Brasil para enfrentar las amenazas al ciberespacio.

Abstract

The 2023 Pan American and Para Panamerican Games represent an important challenge for the State of Chile, not only because it is the largest event held after the '62 World Cup or because there is a large amount of resources committed, but also because the current conditions of the security environment could affect the normal development, the welfare of competitors and

Palabras clave
Ciberseguridad
Ciberdefensa
Panamericanos
Parapanamericanos
Evento mayor

Keywords
Cyber security
Cyber defense
Panamerican games
Para Panamerican games
Major event

1 Oficial de Ejército, licenciado en Ciencias Militares, especialista de Estado Mayor, magíster en Ciberseguridad en la Universidad Adolfo Ibáñez y magíster en Ciencias Militares. Actualmente se desempeña como asesor de Estado Mayor en la Conferencia de Ejércitos Americanos en el Estudio Especializado de Inteligencia en Brasil. Email. nicolas.kaiser@ejercito.cl .

general public attending. Games security cannot only be approached from a traditional perspective, cyberspace must also be considered as a domain to be affected. Brazil between 2007 and 2016 had the responsibility of organizing several events of the characteristics of Santiago 2023, accumulating a vast experience from the perspective of this domain. Cybersecurity of the Games requires planning and coordination that allows the proper articulation of ways and means in terms of the end, which is the good development. Considering the little experience of Chile in these types of events, through the description of the experiences of Brazil, we seek to extract experiences in terms of the considerations that should be taken into account with respect to an eventual participation of the Armed Forces in the cybersecurity of the games.

Introducción

Tradicionalmente,el empleo de las Fuerzas Armadas ha estado ligado a los dominios terrestre, aéreo y marítimo. Sin embargo, con la irrupción de nuevas tecnologías y con los avances de la humanidad, se han incorporado el espacio y el ciberespacio. En los tres primeros dominios, la historia ha demostrado que una potencia puede lograr la superioridad y con ello obtener una ventaja relativa ante un oponente. En el caso de los dos últimos y en particular el ciberespacio, todavía no hay antecedentes o hechos que demuestren la superioridad por parte de un actor.

El ciberespacio ha sido reconocido por varias fuerzas armadas como un nuevo dominio del ambiente operacional, lo cual cada vez es más volátil, incierto, complejo y ambiguo (VUCA).[2] En este ambiente se identifican las capa física geográfica, infraestructura física y lógica-digital (figura Nº 1), las cuales se traslapan, lo que hace aún más complejo su protección:

Sus características hacen que sea transversal a los otros, por lo que requiere de una acción conjunta para la protección de la infraestructura crítica de la información[3] ligada a ella. Ejemplo de lo anterior es la seguridad de una red de fibra óptica submarina, la que requeriría de capacidad de la Armada y Ejército para su protección en caso de ser amenazada.

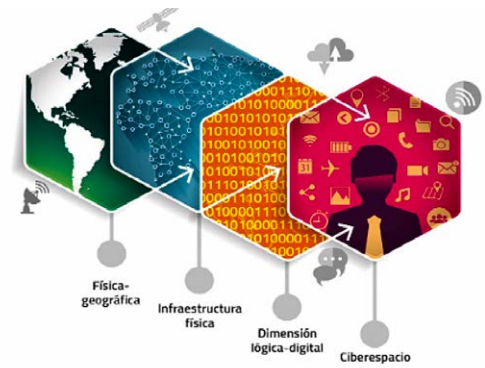


Figura Nº 1: Capas del ciberespacio.

Fuente: Aportes Teóricos a la Geopolítica Regional del Ciberespacio (Ocón, 2021).

Conforme a lo que establece la Constitución Política de la República de Chile, las Fuerzas Armadas *"existen para la defensa de la patria y son esenciales para la seguridad nacional"*.[4] Explícitamente, la misión hace referencia al empleo de las capacidades para hacer frente a una amenaza externa, sin embargo y dadas las actuales características del entorno, las

2 El término VUCA (volatility, uncertainty, complexity and ambiguity) fue acuñado en el Army War College (US Army, 2021) para describir las características del ambiente en que los líderes estratégicos se verían enfrentados.

3 Corresponde a aquellas instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación de servicio, interceptación, interrupción o destrucción puede tener una repercusión importante en la seguridad nacional, en la provisión de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que este debe proveer o garantizar (Gobierno de Chile, 2022).

4 Artículo 101 de la Constitución Política de la República (Ministerio Secretaría General de la Presidencia, 2005).

Fuerzas Armadas se han visto obligadas al desarrollo de capacidades polivalentes para actuar en otras misiones, distintas a la defensa, ya sea bajo normalidad constitucional o en excepción constitucional. En este sentido, el Libro de la Defensa Nacional de Chile 2017 definió que las Fuerzas Armadas puede ejercer funciones en sus 5 áreas de misión (AM)[5] (figura Nº 2) y con ello aportar con diversas capacidades a la acción del Estado, contribuyendo a la seguridad externa e interna.

Figura Nº 2: Áreas de Misión de la Defensa.

Fuente: Política de Defensa Nacional, 2020.

ÁREA DE MISIÓN	DEFINICIÓN
Defensa de la soberanía e integridad territorial	Agrupa las misiones destinadas a prevenir y disuadir del uso de la fuerza militar en contra de nuestro país o a rechazar agresiones y actos hostiles contra la población, la soberanía, la integridad territorial, su independencia política, los recursos y bienes nacionales, y los intereses nacionales, incluyendo ciberataques como forma de agresión.
Cooperación internacional y apoyo a la política exterior	Agrupa las misiones a ejecutar en el ámbito internacional, conforme al interés nacional o en virtud de compromisos de seguridad asumidos por Chile, de acuerdo con nuestra política exterior.
Seguridad nacional e intereses territoriales	Agrupa misiones de las FF.AA. que contribuyen al control y soberanía nacional en todo su territorio, incluyendo zonas fronterizas y aisladas, la Antártica, áreas oceánicas, territorios insulares y los espacios aéreos, así como la contribución a la preservación del medioambiente y recursos naturales.
Contribución al desarrollo nacional y a la acción del Estado	Agrupa misiones que se realizan como contribución a la gestión del riesgo de desastres que realiza el Estado para enfrentar emergencias derivadas de catástrofes naturales o antrópicas, incluyendo pandemias y epidemias.
Emergencia nacional y protección civil	Agrupa diversas misiones de apoyo a la comunidad y a otros organismos del Estado, al desarrollo del país en el ámbito científico y tecnológico, de su industria nacional, preservación del medioambiente, integración física mediante conectividad de zonas fronterizas e insulares, elaboración de elementos cartográficos y construcción de obras viales e infraestructura, preservación de tradiciones patrias, y otros requerimientos de las autoridades competentes.

Tabla Nº 1: Áreas de Misión

Fuente: Política de Defensa Nacional, 2020, Chile.

5 Grupo de misiones interrelacionadas establecidas por el nivel político y que se basan en normas constitucionales y legales vigentes. Proporcionan una visión general del quehacer de la Defensa Nacional y entregan un marco de referencia común para la planificación y desarrollo de capacidades y la definición de cometidos o tareas que, en todos los niveles de conducción, la Defensa debe considerar para su cumplimiento (Ministerio de Defensa Nacional, 2017, p. 114).

Para lograr los objetivos de la política de defensa nacional respecto a las áreas de misión, el Ejército considera la ejecución de tres tipos de operaciones militares: de guerra, distintas a la guerra y comunes (figura Nº 3).

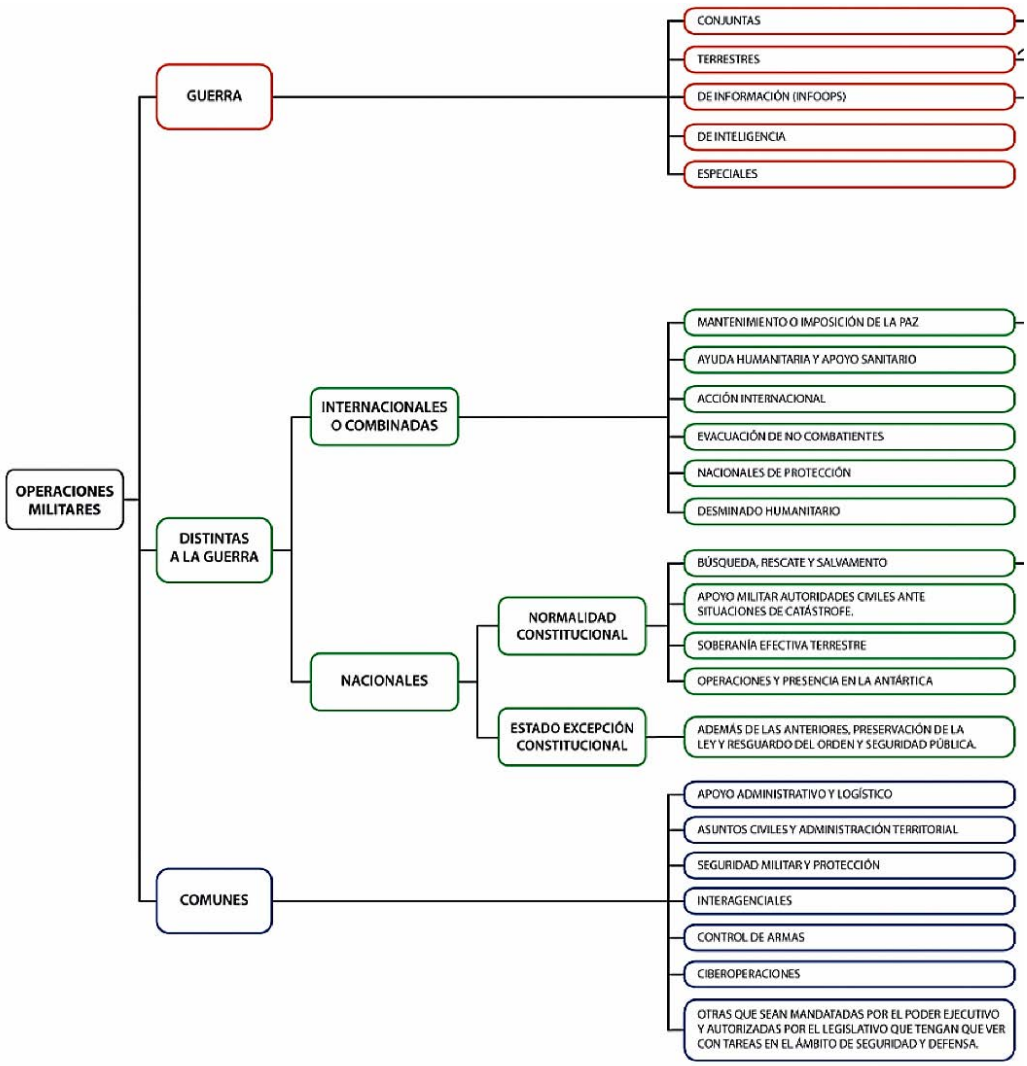


Figura Nº 3: Operaciones militares.

Fuente: DD-10001 "La Fuerza Terrestre" (Ejército de Chile, 2019).

En el caso de las ciberoperaciones, foco del presente trabajo, se consideran como operaciones comunes, ya que pueden aportar con efectos tanto en las operaciones de guerra como de no guerra, como también preservar la seguridad de los sistemas del Ejército y de esta forma contribuir con las áreas de misión distintas a las de la Defensa (tabla 2).

ÁREA DE MISIÓN	CONTRIBUCIÓN
Cooperación internacional	• Intercambio de conocimientos y experiencias • Intercambio de inteligencia de amenaza • Fortalecimiento de medidas de confianza mutua • Intercambio académico
Emergencia nacional y protección civil	• Gestión y protección de activos • Disponibilidad de sistemas de comunicaciones y mando y control para las autoridades civiles • Identificación de información falsa que circule a través del ciberespacio
Contribución al desarrollo nacional y a la acción del Estado	• Apoyo con sistemas de comunicaciones para apoyar la integración de zonas fronterizas • Apoyar la investigación y desarrollo en materias de ciberdefensa
Seguridad e intereses territoriales	• Obtención de información respecto a riesgos y amenazas

Tabla Nº 2: Relación entre ciberdefensa y áreas de misión.

Fuente: Elaboración propia a partir de "La ciberdefensa desde la perspectiva de la polivalencia" (Espina, 2020).

Chile, durante el 2023 realizará los Juegos Panamericanos y los Parapanamericanos,, considerado un evento deportivo mayor,[6] que congregará a miles de deportistas de distintos países del continente, como también un público diverso que apoyará a sus compatriotas.

Pero no solo habrá concurrencia de deportistas y público en general, sino que también es una instancia que despierta el interés para que grupos u organizaciones asistémicas busquen interrumpir o afectar el normal desarrollo de los Juegos. Una forma de hacerlo y que involucre una baja cantidad de recursos y tengan un alto impacto, son las acciones a través del ciberespacio ejecutadas por grupos "hacktivistas".

El presente artículo tiene como finalidad describir las experiencias de Brasil desde la perspectiva de ciberdefensa para este tipo de eventos mayores y a partir de ello reflexionar sobre cómo evolucionaron las capacidades de ciberdefensa de Brasil y como se integraron se integraron a la planificación de seguridad de los distintos eventos.

Brasil: evolución de un referente regional

La República Federativa de Brasil organizó, entre los años 2007 y 2016, ocho eventos, cuyas características les permiten ser clasificados como eventos importantes o de mayor envergadura. Dentro de los más relevantes están: Juegos Panamericanos de 2007, Conferencia de Río +20 de 2013, Jornada Mundial de la Juventud en 2013, Copa del Mundo de 2014 y Juegos Olímpicos y Paralímpicos de 2016. Los eventos clasificados como deportivos son los que demandaron nuevas estructuras y modelos de organización a nivel ministerial entre las Fuerzas Armadas y los organismos de seguridad pública.

Las Fuerzas Armadas de Brasil y en particular su Ejército tuvieron participación en prácticamente

6 Se puede considerar un "Gran Evento Deportivo Mayor, aquel evento que está marcado por tres aspectos: la repercusión internacional; el hecho de que incluya actividades cuya dimensión y complejidad requieran una planificación amplia y detallada; y la implicación, en su organización, de varias esferas de actividad, tanto gubernamentales como no gubernamentales". Exército Brasileiro. (2018). A Participação do Exército na Segurança dos Grandes Eventos–O Legado. Brasilia: Comando de Operações Terrestres.

todos los eventos, aportando capacidades para un mejor desarrollo de estos. A partir de cada evento se generaron experiencias que permitieron enfrentar de mejor forma la Copa del Mundo y los Juegos Olímpicos, los cuales fueron los eventos de mayor envergadura realizados. En cuanto a ciberdefensa, se evidencia un incremento en el nivel de madurez de su organización y en el desarrollo de capacidades. Es así que en la Estrategia de Defensa Nacional se le asigna al Ejército la responsabilidad del desarrollo estratégico de la ciberdefensa.

Ejército de Brasil: dificultades y experiencias

El Ejército de Brasil, el 2018, publicó "*A Participação do Exército na Segurança dos Grandes Eventos – O Legado*", cuya finalidad fue presentar las acciones desarrolladas, tanto en la planificación como ejecución de las diversas misiones y tareas asignadas para la seguridad de los grandes eventos, además de que sirviera de fuente de consulta respecto a las experiencias para las futuras generaciones que puedan tener la responsabilidad de planificar y ejecutar acciones de seguridad en eventos mayores.

A grandes rasgos, el informe aborda la descripción de los grandes eventos, el nivel de planificación, las estructuras operativas, las amenazas y acciones realizadas en diversas funciones como defensa antiaérea, ciberdefensa, NBQ[7], etc., en los distintos eventos.

Desde la perspectiva de ciberdefensa, las experiencias acumuladas, dada la complejidad e importancia de las tareas realizadas, terminó con la creación el 2014 de un Comando Conjunto de Ciberdefensa, siendo la base el Centro de Ciberdefensa del Ejército. A continuación, se detallan las más importantes experiencias de los principales eventos[8]

a. Conferencia Río +20 (13–22 junio 2012)

1) Misión: colaborar con las acciones de seguridad durante la Conferencia de las Naciones Unidas sobre el Desarrollo Sostenible (Río+20), coordinar e integrar las acciones de defensa contra las acciones cibernéticas hostiles.
2) Dificultades:
   - Poco tiempo para el reclutamiento y entrenamiento del personal;
   - Falta de un estudio previo y detallado de las necesidades de tecnología de la información (TI) para el Centro de Ciberdefensa.
   - Dificultad para establecer una matriz de comunicación fiable con los socios.
3) Buenas prácticas y lecciones aprendidas:
   - La identificación previa de escenarios hipotéticos permitió preparar a los medios de comunicación para responder a las posibles preguntas técnicas de la prensa, facilitando la organización del Centro de Ciberdefensa para la gestión de posibles crisis;
   - La necesidad de anticipar la disponibilidad de los sistemas de información críticos, para permitir el análisis de riesgos y la consiguiente implantación de los controles necesarios;
   - La necesidad de realizar ejercicios preliminares en escenarios que incluyan las amenazas probables.

7 Nuclear, bactereológica y química.
8 *Ibídem*, pp. 111 – 119.

b. Copa Confederaciones (15-30 de junio de 2013)

1) **Misión:** colaborar con las acciones de seguridad durante la Copa Confederaciones FIFA/2013; coordinar e integrar las acciones de seguridad y defensa cibernética.
2) **Dificultades:**
   - Una vulnerabilidad en la aplicación GRC[9] permitía la inserción de un código indebido, que podía comprometer el uso de este sistema durante la operación;
   - Falta de personal especialista en el Centro de Ciberdefensa, lo que dificultó los despliegues, por lo que se tuvo que convocar a militares de otras ramas.
3) **Buenas prácticas y lecciones aprendidas:**

- El análisis de incidentes maduró considerablemente durante la operación y los resultados obtenidos fueron relevantes;
- La plantilla del Informe de la Operación, preparada por el Centro de Ciberdefensa, fue esencial para mapear el conocimiento generado en los destacamentos remotos (Dst. Rmto.) durante la operación.

c. Jornada Mundial de la Juventud (23-28 de julio de 2013)

1) **Misión:** colaborar con las acciones de seguridad durante la Jornada Mundial de la Juventud (JMJ), coordinar e integrar las acciones de seguridad y defensa cibernética.
2) **Dificultades:** falta de tiempo para el estudio del perímetro de las redes de interés.
3) **Buenas prácticas y lecciones aprendidas:**
   - El despliegue de militares del Centro de Ciberdefensa para el reconocimiento, antes del inicio de la operación, contribuyó a una mejor comprensión de la misión, reforzó la interacción con otros organismos implicados, permitió formular alertas y recomendaciones previas de ciberseguridad y ciberdefensa al Centro de Coordinación y Defensa del Área (CCDA), permitió el asesoramiento a los responsables informáticos de los organismos implicados en la operación;
   - Entre los servicios ofrecidos por el Centro de Ciberdefensa, se hizo hincapié en el análisis de las vulnerabilidades de los activos de Comando Militar del Este (CML)[10] y del sistema Pacificador[11] del Ministerio de Defensa. Del análisis, se generó un informe de riesgos y recomendaciones de mejores prácticas y procedimientos de seguridad a los administradores del Pacificador;
   - Elaboración de un inventario de los activos[12] que componen la infraestructura informática del CML, junto con un análisis de vulnerabilidades, lo que tuvo como resultado un informe que trataba las vulnerabilidades de los activos y otro con recomendaciones de seguridad, con el fin de apoyar el

9 *Governance, Risk & Compliance.*
10 *Comando Militar Leste.*
11 Sistema de Mando y Control (C2) destinado a apoyar las operaciones de Garantía de Ley y Orden y de defensa/seguridad de grandes eventos, contribuyendo a la comprensión situacional, la sincronización de las acciones entre los elementos implicados, así como el tratamiento de los incidentes que se produzcan.
12 Un inventario de activos se define como una lista de todos aquellos recursos (físicos, software, documentos, servicios, personas, instalaciones, etc.) que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos (INCIBE, 2016).

proceso de endurecimiento *(hardening)*[13] de los activos de CML. El producto fue un informe técnico con sugerencias para la implementación de mejoras.

- Durante la operación se produjo un nuevo y fructífero intercambio de conocimientos entre los militares de las tres ramas de la defensa. Se enfatizó que este procedimiento debía mantenerse, incluso porque el Ejército brasileño no tenía la capacidad de desplegar medios en todos los puestos de ciberdefensa necesarios para el Mundial, por lo que el apoyo logístico proporcionado por las demás fuerzas fue fundamental para el éxito de la misión.

d. Copa del Mundo (12 junio -13 julio de 2014)

1) **Misión:** coordinar e integrar en un ambiente conjunto las acciones de seguridad y defensa cibernética, para contribuir al establecimiento y mantenimiento de la seguridad en la Copa del Mundo 2014.
2) **Dificultades**:
   - Dificultades de comunicación entre los equipos de tratamiento del Centro de Ciberdefensa y otros organismos, debido a que la herramienta Risk Manager no utilizaba el cifrado PGP;[14]
   - Limitaciones de la herramienta Risk Manager en el proceso de gestión del tratamiento de incidentes en la red;
   - Falta de uso de la clave pública PGP para todos los miembros;
   - Falta de sincronización de las visitas técnicas de la unidad de Ciberdefensa a la sede, con las visitas técnicas del Ministerio de Defensa, lo que generó un desajuste en la preparación y configuración de la Red Operativa de la Defensa (ROD) para cumplir con los requisitos del Centro de Ciberdefensa;
   - El análisis de riesgos y vulnerabilidades, en algunas sedes se efectuó muy cerca del inicio del evento, lo que no permitió al CCDA/CICCR[15] asimilar el Informe de Riesgos Operativos (IRO) en su totalidad (esta actividad no pudo realizarse con antelación porque varios CCDA/Centro Regional Integrado de Mando y Control (CICCR) no estaban operando);
   - Falta de una herramienta de mensajería instantánea (*chat*) que facilite la interacción entre los miembros del Destacamento Remoto y los analistas del Centro de Ciberdefensa.
3) **Buenas prácticas y lecciones aprendidas:**
   - La implementación de plantillas (matrices) de notificación resultó eficaz y facilitó la categorización de los eventos;
   - La importancia de sincronizar la disponibilidad operativa de la infraestructura informática remota, necesaria para la coordinación de una operación desde el Centro de Monitoreo de Ciberdefensa (*C Mon Ciber*), con las estructuras homólogas del Ministerio de Defensa, ya que las capacidades de los sistemas de la unidad de ciberdefensa deben ser presentadas

13 Proceso destinado a eliminar un medio de ataque parcheando vulnerabilidades y desactivando servicios no esenciales (NIST, 2015).

14 PGP (Pretty Good Privacy) utiliza una combinación de clave pública y cifrado convencional, para proporcionar servicios de seguridad para los mensajes de correo y archivos de datos. Estos servicios incluyen confidencialidad y firma digital (PONS, 2021).

15 Centro de Coordinación de Defensa Aérea/Centro Integrado de Mando y Control Regional.

primero a ese ministerio, que realizará las configuraciones/adaptaciones necesarias en el ámbito de su propia planificación;
- El análisis de riesgos y vulnerabilidades debe realizarse en una fecha que permita al responsable de la infraestructura de red tener tiempo para asimilar plenamente el Informe de Riesgos Operativos (IRO);
- El montaje de la infraestructura informática del CCDA bajo la responsabilidad de Fuerzas Especiales podría ser supervisado más estrechamente por el Sistema Telemático del Ejército (*SisTEx*), con el fin de incorporar, desde el principio, las mejores prácticas informáticas que permitan que los sistemas entren en funcionamiento con vulnerabilidades reducidas;
- Las visitas preliminares de los equipos del Centro de Ciberdefensa a los lugares donde se instalarían los destacamentos remotos contribuyeron en gran medida a reforzar la interacción entre la unidad y las agencias/instituciones apoyadas;
- La decisión de realizar el análisis de riesgos y vulnerabilidades en los CCDA resultó ser extremadamente productiva, generando un entorno de seguridad preventivo y un mejor conocimiento de las redes de los CCDA;
- La preparación modular (Manejo de Incidentes y Procesos Internos) del Destacamento Remoto demostró ser exitosa, abordando las habilidades necesarias para el cumplimiento de la misión, además de haber desarrollado el espíritu de equipo, nivelado los conocimientos y sistematizado los procedimientos;
- El protocolo de comunicaciones establecido para una operación debe permitir la interacción constante y consistente entre todos los técnicos involucrados.

e. Juegos Olímpicos y Paralímpicos (agosto-septiembre de 2016)

1) **Misión**: coordinar e integrar[16] en un entorno conjunto las acciones de seguridad y defensa cibernética para contribuir al establecimiento y mantenimiento de la seguridad en los Juegos Olímpicos y Paralímpicos 2016; análisis de riesgo de activos críticos para el evento; gestión de incidentes de red; ciberinteligencia; y seguridad y defensa de su propia red, insertada en el entorno cibernético del evento.
2) **Dificultades:**
   - El software de gestión de eventos de seguridad funcionó con restricciones;
   - La ABIN[17] no autoriza la instalación de *softwares* que no estén certificados por la propia agencia;
   - La ABIN no dispone de una célula que se ocupe exclusivamente de la cibernética, lo que dificulta el intercambio de información relativa al sector cibernético;
   - Parte de las estructuras a las que se envió un oficial de enlace no estaban acreditadas y no recibieron estaciones de trabajo;
   - Las herramientas de protección y conocimiento de la situación se pusieron en

16 La misión de la coordinación es combinar armoniosamente los esfuerzos para lograr la seguridad y defensa cibernética de los Juegos Olímpicos y Paralímpicos 2016, optimizando los resultados y aumentando la eficacia de la acción conjunta de todas las entidades gubernamentales de ciberseguridad y defensa involucradas en el evento. La misión de integrar es contribuir a los procesos de seguridad y defensa cibernética de los Juegos Olímpicos y Paralímpicos de 2016, a través de las acciones de coordinación de socios.

17 ABIN: Agencia Brasileira de Inteligencia.

funcionamiento y se configuraron en una fecha muy próxima al inicio de la fase de empleo;
- Los administradores informáticos del CGDA,[18] del CDA[19] y del CDS[20] tenían una actuación limitada en la supervisión y cumplimiento de las políticas de Seguridad de la Información y de las Comunicaciones (SIC);
- Los miembros del estado mayor del Centro de Operaciones (COp) tenían poco conocimiento doctrinal sobre el uso de las cibercapacidades;
- Las alertas generadas por las Fuerzas no se compartían directamente con los demás CSIRT de Defensa;
- La alta demanda de personal para componer los destacamentos conjuntos de ciberdefensa dificultaba la provisión de equipos técnicos en reserva para su rápido empleo en caso de necesidad.

3) **Buenas prácticas y lecciones aprendidas:**
   - Establecer confianza y una buena relación con los miembros del Comité Río 2016 y las empresas participantes fue fundamental para el acceso a la información a la hora de aclarar dudas durante los eventos;
   - La existencia de elementos de enlace en las diferentes agencias hizo posible enviar y recibir mensajes con mayor agilidad (además permitió que las demandas entre las agencias pudieran sufrir pequeños ajustes durante la operación, principalmente en lo que respecta a la relevancia y pertinencia del contenido);
   - Los oficiales de enlace en el Comité Río 2016 y en el Centro de Inteligencia de los Juegos (CIJ) fue importante para compartir datos técnicos y no técnicos;
   - Las visitas de orientación técnica (VOT) realizadas a las estructuras estratégicas, así como a los centros de operaciones de la CGDA, CDA y CDS, contribuyeron de manera significativa a aumentar la seguridad y defensa cibernética;
   - El entrenamiento de los miembros del Destacamento Conjunto de Ciberdefensa fue esencial, ya que se centró en la formación y preparación del personal que no era miembro del Centro de Ciberdefensa;
   - Reuniones de coordinación con representantes de distintos organismos y agencias federales contribuyeron al establecimiento de la confianza mutua entre las entidades;
   - El uso de nuevas herramientas de ciber protección y conocimiento de la situación, con el consiguiente aumento de la capacidad de la unidad de Ciberdefensa para identificar los eventos de seguridad de la red, debido al monitoreo en tiempo real;
   - Concurrencia de un apoyo constante de los Centros de Telemática e Informática en las policías;
   - El empleo de personal militar y civil de las 3 (tres) Fuerzas, con alto nivel técnico, incluyendo experiencia en grandes eventos;
   - Trabajo de colaboración con el CSIRT de las Fuerzas y el Equipo de Tratamiento de Redes (ETIR) de las organizaciones asociadas, incluyendo el establecimiento de protocolos de comunicación;
   - Activación del Comando Conjunto de Ciberdefensa con suficiente antelación a la

18 Centro de Coordinación General de Defensa Aérea.
19 Centro de Defensa Área.
20 Centro de Desarrollo de Sistemas.

fecha de inicio de los Juegos Olímpicos de Río 2016; oportunidad para que el estado mayor emplee la capacidad cibernética en actividades relacionadas con operaciones de inteligencia y operaciones de información;

- Presencia de enlace militar en las estructuras de interés (Corte Internacional de Justicia-CIJ, CICCR, Centro Integrado de Comando y Control Nacional-CICCN, MD, Comité Organizador de Río 2016 y Centro de Operaciones de Río de Janeiro) para el seguimiento y la rápida coordinación de las acciones destinadas a la protección del ciberespacio.

Cada participación tuvo una organización de la tarea distinta, que involucró la coordinación e integración de diversos organismos conforme al evento a realizarse, sin embargo, desde la perspectiva de la seguridad y defensa cibernética, las experiencias obtenidas en los eventos pudieron ser implementadas en lo sucesivo. La participación de las Fuerzas Armadas de Brasil, lideradas por el Ejército, permitió el desarrollo de una capacidad conjunta en ciberdefensa, terminando con la formación del Comando Conjunto de Ciberdefensa, estructura del nivel operacional referente en la región.

Por otra parte, se evidencia que a partir de las dificultades y las buenas prácticas adoptadas en cada evento, le permitieron tener una mejor preparación y respuesta. La preparación y coordinación previa al inicio de los eventos resultó clave para identificar debilidades, como también explotar las oportunidades en la ejecución.

Núcleo de Fuentes Abiertas en los Juegos Olímpicos

Brasil el 2011 estableció la Secretaría Extraordinaria para Grandes Eventos (SESGE), con la finalidad de coordinar el esfuerzo conjunto de seguridad necesaria para los eventos que realizaría entre los años 2013 y 2016.[21] Como se detalló previamente, Brasil acumuló vasta experiencia en materias de seguridad en grandes eventos, en parte por la acción integrada a partir de los Juegos Panamericanos de 2007 entre los Ministerios de Justica, de Defensa y Agencia Brasileña de Inteligencia, gobiernos locales y organismos internacionales.[22]

Para la seguridad de los Juegos Olímpicos y Paralímpicos de Río en 2016 se desarrolló el Plan Estratégico de Seguridad Integral (PESI), que estaba compuesto por tres ejes: seguridad pública, defensa e inteligencia. La misión fue *"garantizar la seguridad de los Juegos, de forma discreta y amigable bajo la coordinación del Gobierno Federal, de forma integrada con los gobiernos estatales y municipales del Comité Organizador".*[23]

Los organismos responsables en los distintos ejes fueron el Ministerio de Justicia (responsable de la seguridad pública), el Ministerio de Defensa y la Agencia Brasileña de Inteligencia (ABIN). Para efectos de los Juegos, cada organismo creó una organización que asumiera la responsabilidad de la planificación y posterior ejecución de la seguridad (figura Nº 4).

21 Ministerio de Justicia. Publicado el 13 de Mayo del 2016. Consultado el 21 de Noviembre de 2022 de Secretaría Extraordinária de Segurança para Grandes Eventos Disponible en: https://web.archive.org/web/20160513065853/http://justica.gov.br/sua-seguranca/grandes-eventos/

22 Secretaría de Comunicación Social. (2016). Seguridad en los Juegos Olímpicos y Paralímpicos Rio 2016, p. 6. Presidencia de la República Federativa de Brasil. Consultado el 23 de noviembre de 2022. Disponible en: http://www.rededoesporte.gov.br/es/presskit/archivos/fact-sheet-seguridad

23 *Ibídem*, p. 5 .

Figura Nº 4: Organismos responsables de la seguridad.

Fuente: Memorial del Ejército 503. La seguridad en eventos deportivos mayores, experiencias para Santiago 2023 (Kaiser, 2019).

Previo a los Juegos de 2016, y dado el contexto mundial y local, existían preocupaciones por miedo a los actos terroristas, al aumento de protestas organizadas por redes sociales y a la turbulencia política que se vivía en el país.[24] Lo anterior, en parte, por el explosivo aumento de uso de Internet y la gran de cantidad de información que circulaba en ella.

Para el 2016, la población mundial era de 7.395 millones y de ellos el 51 % utilizaban teléfonos móviles y el 46 % eran usuarios de Internet. Por otra parte, el 31 % de la población estaba presente en redes sociales y el 27 % se conectaba a ellas a través de su dispositivo móvil.[25]

Para poder lidiar con ese aspecto, Brasil creó una estructura para hacerse cargo de la información atingente a los Juegos que circulaba en fuentes abiertas (Internet principalmente). Esa estructura fueron los Núcleos de Fuentes Abiertas (NuFA), los cuales dependían de la Dirección de Coordinación General de Inteligencia de la SESGE, y cuya finalidad fue utilizar la información disponible para producir conocimiento válido y oportuno para ser aplicado durante el desarrollo de los Juegos.[26]

Como todo proceso de inteligencia, el direccionamiento de la obtención de información se limitó a los hechos, noticias, datos e informaciones de interés para la Seguridad Pública, la Seguridad Nacional y la actividad de inteligencia relativa a Río 2016, producto de la dificultad de analizar todo el contenido disponible en la red.

24 BARRETO, Alesandro & WENDT, Emerson. Inteligência e Investigação Criminal em Fonte. 2020, 3ª edición, p. 60. Rio de Janeiro: Brasport Livros e Multiídia Ltda.

25 GUIBERT, Yasyana. Publicado el 19 de abril de 2016. El porcentaje de usuarios de Internet alcanza al 46 % de la población mundial según We Are Social (2016). Consultado el 23 de noviembre de 2022, de Marketing 4 Ecommerce. Disponible en: https://marketing4ecommerce.net/usuarios-de-internet-mundo-2016/

26 BARRETO & WENDT. *Op. cit.* pp. 65-66.

Conforme a lo señalado por Barreto & Wendt, fue clave para el desarrollo de las tareas y productos los aspectos indicados en la figura Nº 5, ya que permitieron la identificación cualitativa de contenido, como también la elaboración de productos útiles para los tomadores de decisión.

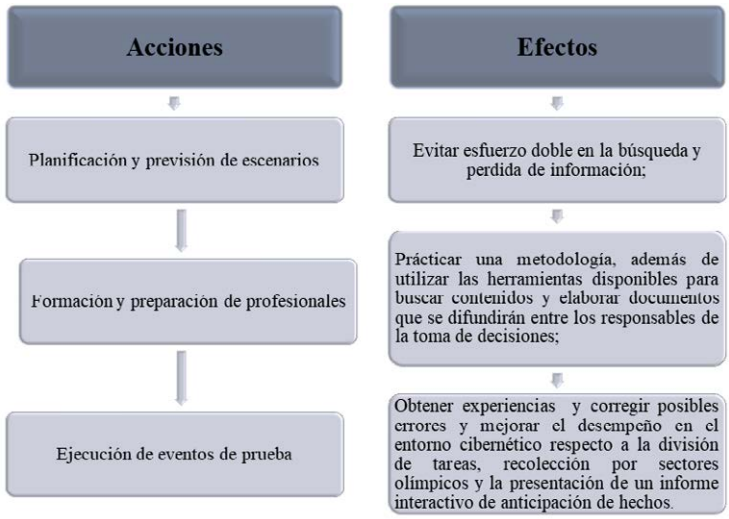


Figura Nº 5: Acciones preventivas desarrolladas.

Fuente: Elaboración propia.

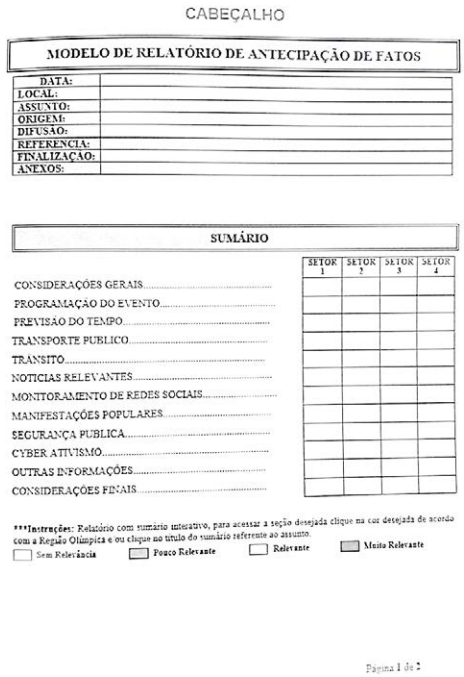
Los productos utilizados por los NuFA fueron el Informe de Anticipación de Hechos (figura Nº 6) y el Boletín de Noticias (figura Nº 7). El primero surgió de la necesidad de compilar la información de las regiones olímpicas que fuese relevante y tuviese un impacto en la seguridad del evento en un solo documento. A grandes rasgos, los tópicos se detallan en la tabla 3.

TÓPICO	DESCRIPCIÓN
Nivel de importancia	- Blanco: sin relevancia - Verde: poco relevante - Amarillo: relevante - Rojo: muy relevante
Programación de la jornada	Actos a celebrar por sectores el día siguiente (secciones, juegos, fiestas, eventos)
Clima y tiempo	Previsión meteorológica y contenidos relacionados. En algunos casos, se incorporaron los mapas meteorológicos por sectores en la ciudad de Río de Janeiro, con énfasis en los lugares de competición.
Transporte	Cambios y cierres de carreteras y otras circunstancias que afectan al flujo normal de vehículos en puntos de Río y, principalmente, en las localidades cercanas a los eventos.
Tráfico	Cambios y cierres de carreteras y otras circunstancias que afectan al flujo normal de vehículos en puntos de Río y, principalmente, en las localidades cercanas a los eventos.
Noticias relevantes	Noticias con relevancia nacional o alguna proyección en Río de Janeiro y/o evento. Los asuntos estaban restringidos a: evento olímpico, infraestructura, internacional, salud, seguridad pública, sistema penitenciario, terrorismo y otros asuntos de interés.

TÓPICO	DESCRIPCIÓN
Seguimiento de las redes sociales	Análisis cuantitativo y cualitativo de las menciones de los juegos y de los términos de interés publicados en las redes sociales, como *hashtags*, eventos, *engagement* y previsiones sobre determinados temas.
Manifestaciones previstas	Recopilación de datos para identificar las manifestaciones que tendrían lugar al día siguiente y que tendrían un impacto directo o indirecto en los juegos.
Seguridad pública. Hechos relacionados con deportistas	Familia olímpica; turistas; hechos policiales destacados; organizaciones criminales; y sistema penitenciario.
Ciberactivismo	Seguimiento de los ataques de *defacement* y denegación de servicio a las aplicaciones gubernamentales de Internet o relacionadas con los Juegos Olímpicos y Paralímpicos.
Otras observaciones	Información no prevista en los temas anteriores y que se considera útil para los intereses de los responsables de la toma de decisiones.
Consideraciones finales	Datos sobre las actividades desarrolladas por el equipo de analistas en la jornada.

Tabla Nº 3: Tópicos de Informe de Anticipación de Hechos.

Fuente: Inteligência e Investigação em Fontes Abertas (Barreto & Wendt, 2020, pp. 67-68).


CABEÇALHO

MODELO DE RELATÓRIO DE ANTECIPAÇÃO DE FATOS

DATA:	
LOCAL:	
ASSUNTO:	
ORIGEM:	
DIFUSÃO:	
REFERÊNCIA:	
FINALIZAÇÃO:	
ANEXOS:	

SUMÁRIO

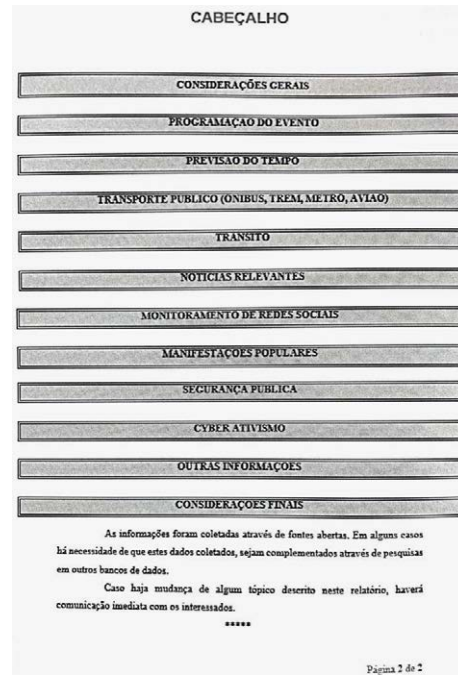
CONSIDERAÇÕES GERAIS.....
PROGRAMAÇÃO DO EVENTO.....
PREVISÃO DO TEMPO.....
TRANSPORTE PUBLICO.....
TRANSITO.....
NOTICIAS RELEVANTES.....
MONITORAMENTO DE REDES SOCIAIS.....
MANIFESTAÇÕES POPULARES.....
SEGURANÇA PUBLICA.....
CYBER ATIVISMO.....
OUTRAS INFORMAÇÕES.....
CONSIDERAÇÕES FINAIS.....

SETOR 1	SETOR 2	SETOR 3	SETOR 4

***Instruções: Relatório com sumário interativo, para acessar a seção desejada clique na cor desejada de acordo com a Região Olímpica e ou clique no título do sumário referente ao assunto.

Sem Relevância | Pouco Relevante | Relevante | Muito Relevante

Página 1 de 2


CABEÇALHO

CONSIDERAÇÕES GERAIS

PROGRAMAÇÃO DO EVENTO

PREVISÃO DO TEMPO

TRANSPORTE PUBLICO (ONIBUS, TREM, METRÔ, AVIÃO)

TRANSITO

NOTICIAS RELEVANTES

MONITORAMENTO DE REDES SOCIAIS

MANIFESTAÇÕES POPULARES

SEGURANÇA PUBLICA

CYBER ATIVISMO

OUTRAS INFORMAÇÕES

CONSIDERAÇÕES FINAIS

As informações foram coletadas através de fontes abertas. Em alguns casos há necessidade de que estes dados coletados, sejam complementados através de pesquisas em outros bancos de dados.

Caso haja mudança de algum tópico descrito neste relatório, haverá comunicação imediata com os interessados.

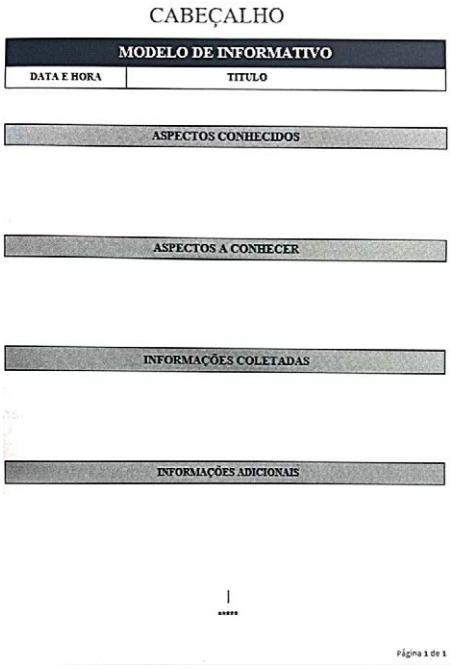
*****

Página 2 de 2

Figura Nº 6: Modelo de Informe de Anticipación de Hechos.

Fuente: Inteligência e Investigação em Fontes Abertas (Barreto & Wendt, 2020, pp. 67, 68).

El Boletín informativo se realizaba para recopilar datos disponibles en fuentes abiertas. A diferencia del informe anterior, la difusión de información obedecía al concepto *push-pull*, en el sentido que era reactiva respecto a una petición de alguna autoridad (*pull*) o bien, se entregaba proactivamente respecto a un hecho que requería seguir investigando (*push*). Para la elaboración del informe siempre se tuvo en cuenta el principio de oportunidad, distribuyendo la información a los tomadores de decisión.


CABEÇALHO

MODELO DE INFORMATIVO

DATA E HORA	TITULO

ASPECTOS CONHECIDOS

ASPECTOS A CONHECER

INFORMAÇÕES COLETADAS

INFORMAÇÕES ADICIONAIS

Página 1 de 1

Figura Nº 7: Modelo de Boletín Informativo.

Fuente: Inteligência e Investigação em Fontes Abertas (Barreto & Wendt, 2020, p. 69).

Reflexiones para Santiago 2023

Santiago albergará el 2023 los Juegos Panamericanos y Parapanamericanos, que, si bien no tienen la misma envergadura que un Mundial o Juegos Olímpicos, es probablemente para el Estado de Chile el mayor evento deportivo organizado después del Mundial del 62, considerando que la situación política, social, económica y avances tecnológicos de entonces dista mucho de la actual.

Como antecedente es conveniente recordad que Chile renunció a ser la sede de las ediciones VII (1975) y X (1987) de los Juegos Panamericanos por razones económicas.

Un gran evento es una instancia donde se verán incrementadas las actividades en el ciberespacio. Cada vez son más numerosas las actividades que tienen lugar en un evento de estas características y que dependen de procesos informatizados, por lo que el uso de las tecnologías de información y comunicación resultan claves. Por consiguiente, las plataformas tecnológicas del evento en el ciberespacio se presentan como objetivos gratificantes para los agentes perturbadores y otros elementos que desean poner en peligro el desarrollo del evento en cuestión

A partir de la experiencia de Brasil, resulta evidente que la protección de los activos tanto del gobierno como de los Juegos, requiere acción integrada y coordinada de los distintos organismos involucrados, demandando tiempo su planificación y preparación. Brasil logró una estructura robusta debido a la experiencia obtenida entre los años 2007 y 2016. El mapeo de redes, análisis de vulnerabilidades, levantamiento de escenarios, ejercicios de prueba, reuniones previas y otras, se presentan como buenas prácticas a considerar, siendo el tiempo un factor crítico para lograr una estructura sólida y que pueda responder frente a incidentes de manera eficiente.

En los últimos años las amenazas se han vuelto más persistentes y la presencia de la delincuencia organizada transnacional ha aumentado, complejizando la condición de seguridad y, por consiguiente, generando respuestas excepcionales como el empleo de las Fuerzas Armadas por parte de los Estados. Derivado de lo anterior, variados son los riesgos que podrían afectar el normal desarrollo de los Juegos. Mucha información circulará por fuentes abiertas, por lo que una estructura similar a los NuFA pareciera ser una alternativa de solución para Santiago 2023. No obstante lo señalado, sabemos que el tema de la seguridad pública les compete a las policías, vale decir a Carabineros de Chile y la Policía de Investigaciones.

Un evento adverso no solo afectará el normal desarrollo de los Juegos, sino que también impactará negativamente al país. Brasil, Canadá y Perú fueron los últimos países en organizar los Juegos Panamericanos y cada uno abordó la seguridad de distinta manera, considerando el contexto particular de riesgos y amenazas. Independiente de la solución, la participación de las Fuerzas Armadas en apoyo a los eventos fue un hecho que se ajustó a las realidades y requerimientos de cada país.

Cada Estado responsable de organizar estos eventos adopta diferentes estrategias en materias de seguridad, como también las Fuerzas Armadas que prestan apoyo de distintas maneras. En el caso de Chile y del Ejército en particular, el apoyo no será desde la perspectiva de la ciberdefensa, sino más bien del área de misión Contribución al Desarrollo Nacional y a la Acción del Estado, así como de la Vinculación con el Medio, colocando a disposición de la organización de los juegos infraestructura deportiva de la Escuela Militar, Escuela de Equitación y Polígono de Tiro "Lo Aguirre".[27]

Bibliografía

BARRETO, Alesandro & Wendt, Emerson. *Inteligência e Investigação Criminal em Fontes Abertas* (3ª edición ed.). Rio de Janerio: Brasport Livros e Multiídia Ltda. 2020

Ejército de Chile. DD-10001 "La Fuerza Terrestre". Santiago: División Doctrina. 2019

ESPINA, Augusto. "La ciberdefensa desde la perspectiva de la polivalencia". *Escenarios Actuales,* pp. 61-73. Edición septiembre de 2020.

Exército Brasileiro. *A Participação do Exército na Segurança dos Grandes Eventos*–O Legado. Brasilia: Comando de Operaçôes Terrestres. 2018

Gobierno de Chile. Proyecto Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información. Consultado el 16 de enero de 2023. Disponible en: https://www.diarioconstitucional.cl/wp-content/uploads/2022/09/14847-06-ciber.pdf. Publicado el 2 de marzo de 2022.

GUIBERT, Yasyana. El porcentaje de usuarios de Internet alcanza al 46 % de la población mundial según We Are Social (2016). Consultado el 23 de noviembre de 2022, de Marketing 4 Ecommerce. Disponible en: https://marketing4ecommerce.net/usuarios-de-internet-mundo-2016/. (19 de abril de 2016).

INCIBE. Inventarios de activos y gestión de la seguridad SCI. Consultado el 16 de enero de 2023, disponible en https://www.incibe-cert.es/blog/inventario-activos-y-gestion-seguridad-sci. Publicado el 29 de diciembre de 2016.

KAISER, Nicolás. "La seguridad en eventos deportivos mayores. Experiencias para Santiago 2023". *Memorial del Ejército* N° 503, pp. 85-101, edición julio 2019. Disponible en https://ejercito.cl/biblioteca/publicaciones-academicas/memorial-del-ejercito-de-chile

Ministerio de Defensa Nacional. Libro de la Defensa Nacional. Santiago. 2017.

Ministerio de Justicia. Consultado el 21 de noviembre de 2022, de Secretaría Extraordinaria de Segurança para Grandes Eventos. Disponible en: https://

27 El convenio fue firmado el 30 de enero del 2023 entre el Ejército y la Corporación Santiago 2023.

web.archive.org/web/20160513065853/http://justica.gov.br/sua-seguranca/grandes-eventos/. Publicado el 13 de mayo de 2016.

Ministerio Secretaría General de la Presidencia. Constitución Política de la República de Chile. Consultado el 28 de noviembre de 2022. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=242302. Publicado el 22 de septiembre de 2005.

National Institute of Standard and Technology (NIST). A Profile for U.S. Federal Cryptographic Key Management Systems. Consultado el 16 de enero de 2023, de NIST. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-152.pdf. Publicado en octubre de 2015.

OCÓN, Alfredo Leandro. "Aportes teóricos a la geopolítica regional del ciberespacio". Pensamiento Propio, pp. 241-250. Consultado el 25 de noviembre de 2022. Disponible en: file:///C:/Users/SEPCEA4.SEPCEA3/Downloads/011-Comentario_Ocon1.pdf. Publicado el septiembre de 2021.

PONS, Luis. ¿Qué es el cifrado PGP y cómo funciona? Consultado el 16 de enero de 2023, de ICM. Disponible en: https://www.icm.es/2021/01/23/pgp-cifrado/. Publicado el 23 de enero de 2021.

Secretaría de Comunicación Social. Seguridad en los Juegos Olímpicos y Paralímpicos Rio 2016. Presidencia de la República Federativa de Brasil. Consultado el 23 de noviembre de 2022. Disponible en: http://www.rededoesporte.gov.br/es/presskit/archivos/fact-sheet-seguridad. Publicado el 2016.

US Army. (21 de noviembre de 2021). US Army Hertiage & Education Center. Consultado el 03 de mayo de 2022, de Who first originated the term VUCA: Volatility, Uncertainty, Complexity and Ambiguity. Disponible en: https://usawc.libanswers.com/faq/84869.