BOLETÍN N° 05
BOGOTÁ D.C. MAYO—JULIO DE 2022

ISSN: 2981-3506

ESICI
Escuela de Inteligencia y Contrainteligencia
Brigadier General Ricardo Charry Solano

BOLETÍN ESTRATÉGICO MULTIDISCIPLINAR

EL RIESGO DE LOS CIBERATAQUES PARA COLOMBIA

Escrito por: Valentina Castro
Orientado por: Pamela Pirateque y Sergio Ramírez

Resumen: En el presente boletín se analiza el efecto de los *ataques cibernéticos*[1] en Colombia y las posibles amenazas que dichos ataques puedan ocasionar al país en cuanto a la *seguridad ciudadana*[2] y la *seguridad del Estado*[3], en especial, en el marco de las elecciones presidenciales del 2022, teniendo en cuenta el juego geopolítico en la región llevado a cabo por Rusia y China con implicaciones en la *ciberseguridad*[4] y *ciberdefensa*[5] nacional Encontrándose que Colombia, a pesar de contar con una *Estrategia Nacional Integral de Ciberseguridad*[6] *y Ciberdefensa*, actualmente es vulnerable a los ciberataques, en particular las entidades estatales como la Registraduría Nacional.

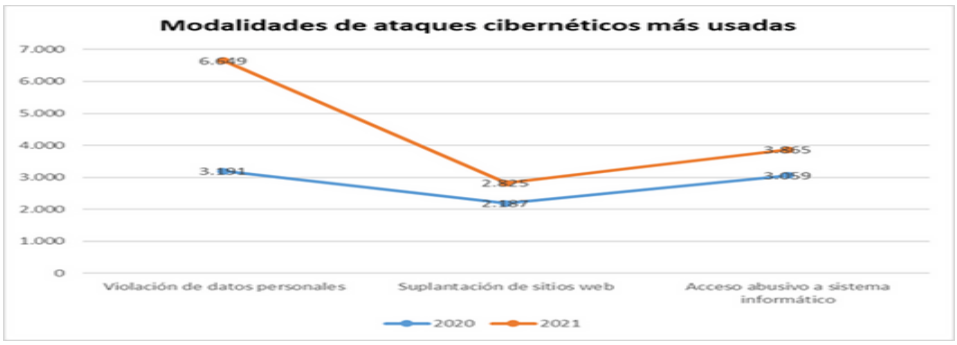
ANTECEDENTES

- En **2018**, días antes de la jornada electoral presidencial "en Colombia se registraron 28.000 ataques de robots a páginas de la Registraduría Nacional para dañar la operabilidad de las páginas electorales" (DW, 2018), acciones que pusieron en riesgo la seguridad del Estado.
- De acuerdo con Fortinet[7], en **2019** "se registraron 48 billones de intentos de ciberataques en Colombia y el sistema bancario fue el mayor blanco" (El Espectador, 2021), sucesos que pusieron en juego la seguridad ciudadana.
- De igual forma, en el año **2021**, en "Colombia hubo más de 11.200 millones de intentos de ciberataques, según datos de Fortinet. En promedio, esto equivale a 31 millones de intentos de ciberataques por día" (Semana, 2022), nuevamente impactando la seguridad ciudadanadel país.

Extraído de: El Espectador (2020)

CONTEXTO ACTUAL

- En el marco de las próximas elecciones presidenciales el 29 de mayo del 2022, los ataques cibernéticos han tomado un rol importante al momento de referirse a la ciberdefensa del Estado colombiano, puesto que los hechos han demostrado que cuando el país entra en contiendas electorales los ciberataques arremeten contra entidades Estatales, en especial la Registraduría Nacional.
- En marzo del 2022 el registrador Alexander Vega Rocha manifestó públicamente cómo la página web de la Registraduría Nacional recibió 400.000 ataques en tan solo una semana en el marco de las elecciones legislativas (El Tiempo, 2022).
- Según la información de las centrales de inteligencia de la Policía Nacional, "estos ataques provendrían de países como Rusia, China, Venezuela y Nicaragua" (El Tiempo, 2022).
- Por otro lado, en cuanto a la seguridad ciudadana, el concepto de*ciberseguridad* va tomando cada vez más fuerza, esto debido a lavulnerabilidad frente a la ciberdelincuencia derivada con la aparicióndel coronavirus (COVID-19), como consecuencia del aumento en lavirtualización de la vida y el trabajo: clases remotas en colegios y universidades, incremento en el uso de aplicaciones de mensajería,aumento de transacciones bancarias online, comunicación deinformación por correo, expedición de documentos online, entre otros. Los delincuentes aprovechando el aumento en el uso de mediosvirtuales y la imposibilidad de desplazamiento, han incrementado eluso de páginas falsas, textos desinformativos, mensajes con virusadjuntos y llamadas engañosas para apropiarse tanto de datospersonales como de datos bancarios. (Ospina y Sanabria, 2020, p.208),esto se refleja en la siguiente grafica:

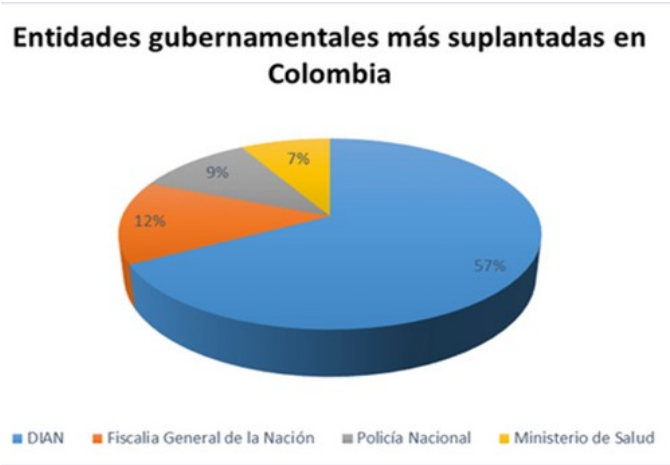


Elaboración propia con datos de asuntos legales (2021)

1. Un ciberataque tiene como finalidad última producir mayor incertidumbre en el modelo de seguridad y control de una organización o nación, es decir, revelar los puntos ciegos y ocultos en las implementaciones de seguridad que las empresas y las naciones tienen (Cano, J., 2020, p. 69).
2. La Seguridad Ciudadana "se entiende como la protección universal a los ciudadanos en especial contra el delito violento y el temor a la inseguridad, garantizando su vida, integridad, libertad y patrimonio económico" (DNP, 2022).
3. La seguridad del Estado "es un concepto que tiene como actor central al Estado en el sistema internacional y que pretende justamente proteger al Estado, concebido como población, territorio y soberanía, contra cualquier ataque externo o interno" (Fuentes, 2005).
4. Capacidad del Estado para "minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética" (Documento Conpes 3701, 2011).
5. capacidad del Estado para "prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional" (Documento Conpes 3701, 2011).
6. Lineamientos de política para ciberseguridad y ciberdefensa (Documento Conpes 3701, 2011).
7. Fortinet es una empresa orientada a la seguridad en redes y la seguridad informática, fundada por Ken Xie, en Sunnyvale, California, Estados Unidos, en el año 2000.

IMPLICACIONES

- El efecto que se puede generar en la Seguridad del Estado por medio de los ataques cibernéticos a las plataformas gubernamentales, las cuales son altamente susceptibles[8] a los ciberataques, es la sustracción o alteración de información estratégica de entidades de la administración pública, a nivel central o subnacional. Esto tal y como se evidencia en la siguiente gráfica.



Elaboración propia con datos de asuntos legales (2021)

- Lo anterior conlleva auna desestabilizaciónpolítica y social del país ante la posible intervención de Rusia mediante la persuasión sobre segmentos de lapoblación para interferir en el relacionamiento y elmarco de legitimidadsostenido ante lasinstituciones, loanterior mediante eluso de fake news onoticias tergiversadasen medio de estallidossociales, lo cual generaría una fractura entre la ciudadanía y las instituciones.

- Con respecto a la Seguridad Ciudadana, los ciberataques en Colombia impactan negativamente el sector económico (entre muchos otros). Cerca del 43% de las empresas colombianas no estánpreparadas para enfrentar ciberataques, pues sólo en 2015 Colombia registró pérdidas porcerca de 1 billón de dólares por ciberataques (Semana, 2016).

- Por otra parte, desde el inicio de la pandemia, es evidente que el cibercrimen ya no es realizado espontáneamente por individuos aislados, sino que es cometido de manera estructurada por organizaciones delincuenciales muy especializadas, con carácter transnacional, que hacen segmentación y ubicación de las posibles víctimas y que despliegan gran variedad de técnicas de seguimiento (Ospina y Sanabria, 2020, p. 208).

- La injerencia de actores externos a Colombia en las decisionespolíticas del país atenta contra la seguridad del Estado. Según uninforme publicado por Global Americans[9], existe un esfuerzo permanente de gobierno como Rusia y China para inmiscuir sus tendencias políticas en la región. Se encontró, por ejemplo, que "a través de medios como Russia Today (RT), Telesur y Xinhua Español, estos países refuerzan ideas sobre las fallas de la democracia, avivando así el descontento social en la ciudadanía local" (Salazar, D, 2021).

- Según dicho informe, Rusiainterviene en la política de Colombia difundiendomensajes contra el Gobierno, especialmente en manifestaciones. Mientrasque China busca permear al gobierno colombiano a entrar en una política comercial enfocada a la “sociedad benéfica entre los Estados” (Salazar, D, 2021).

Extraído de: FortiGuard Labs, organizacion de investigacion e inteligencia de amenazas de Fortinet (2020)

- El anterior contexto obedecería al ámbito de la ciberdefensa como el ámbito de la ciberseguridad, en tanto que con diferentes enfoques "informativos", actores como Rusia y China pretendan establecer una visión propia sobre la dimensión de seguridad ciudadana de Colombia, tergiversando noticias para beneficio político- económico de dichos actores en la región, generando inestabilidad en el país, y desde luego atentando en contra de la seguridad del Estado.

8. La problemática central se fundamenta en que la capacidad actual del Estado para enfrentar las amenazas cibernéticas presenta debilidades y no existe una estrategia nacional al respecto. A partir de ello se establecen las causas y efectos que permitirán desarrollar políticas de prevención y control, ante el incremento de amenazas informáticas. (Documento Conpes 3701, 2011).

9. Global Americans es un centro de investigación enfocado en los derechos humanos, la democracia y la inclusión social en Latinoamérica (Global Americans, 2022). Informe sobre el impacto de la desinformación en las propagandas políticas sobre los resultados de las elecciones.

ESICI
Escuela de Inteligencia y Contrainteligencia
Brigadier General Ricardo Charry Solano

BOLETÍN ESTRATÉGICO MULTIDISCIPLINAR

REFERENCIAS

1. Asunto Legales. Editorial La República S.A.S. (2021, 8 julio). Los ataques cibernéticos aumentaron 30% durante el primer semestre de este año. https://www.asuntoslegales.com.co/actualidad/los-ataques-ciberneticos-aumentaron-30-durante-el- primer-semestre-de-este-ano-3198212
2. Asunto Legales. Editorial La República S.A.S. (2022, 3 marzo). Dane e Invima sostienen que hackeo a sus páginas web no afectó información privilegiada. https://www.asuntoslegales.com.co/actualidad/dane-e-invima-sostienen-que-hackeo-a-sus- paginas-web-no-afecto-informacion-privilegiada-3315738
3. Asunto Legales. Editorial La República S.A.S. (2022, febrero 16). Ciberdelitos subieron 37% durante el primer trimestre de 2020, en los peores meses de la crisis. https://www.asuntoslegales.com.co/actualidad/ciberdelitos-subieron-37-durante-el- primer-trimestre-de-2020-en-los-peores-meses-de-la-crisis-3126480
4. Cano, J. J. (2020). Ciberataques. Sistemas, (157), 67-74.
5. Departamento Administrativo de la Función Pública (DAFP). (2018). Resultados de la consulta FURAG para el año 2018 por sector. https:// www.funcionpublica.gov.co/web/mipg/resultados-2018
6. Deutsche Welle (www.dw.com). (2018). Detectan ataques cibernéticos a ente electoral de Colombia. DW.COM. https://www.dw.com/es/detectan-ataques-cibern%C3%A9ticos-a-entidad-electoral-de-colombia/a-42898310
7. DNP. (2022). Grupo de Convivencia y Seguridad Ciudadana. Departamento Nacional de Planeación. https://www.dnp.gov.co/programas/justicia-seguridad-y-gobierno/grupo-de-convivencia-y-seguridad- ciudadana#:~:text=La%20Seguridad% 20Ciudadana%20se%20entiende,integridad%2C%20libertad%20y%20patrimonio%20 econ%C3%B3mico.
8. Documento Conpes 3701. (2011). Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf
9. El Espectador. Colombia fue objeto de 7 billones de intentos de ciberataques en 2020. (2021, 1 mayo). https://www.elespectador.com/tecnologia/ colombia-fue-objeto-de-7-billones-de-intentos-de-ciberataques-en-2020-article/
10. El Espectador. En 2019 se registraron 48 billones de intentos de ciberataques en Colombia. (2021, 1 mayo).https://www.elespectador.com/tecnologia/ en-2019-se-registraron-48-billones-de-intentos-de-ciberataques-en-colombia- article-908787//
11. El Tiempo. La conexión de supuestos ciberataques rusos con las elecciones en Colombia. (2022, 9 marzo).https://www.eltiempo.com/justicia/ delitos/ciberataques-en-elecciones-que-tan-real-es-el-riesgo-657060
12. Fortinet. Acerca de nosotros. (2022). https://www.fortinet.com/lat/corporate/about-us/about-us
13. Fuentes, Claudia, Seguridad humana y seguridad nacional: relación conceptual y práctica, Santiago de Chile, ANEPE.
14. Global Americans. (2021, noviembre). MEDICIÓN DEL IMPACTO DE LA INFORMACIÓN FALSA, LA DESINFORMACIÓN Y LA PROPAGANDA EN AMÉRICA LATINA. https://theglobalamericans.org/wp- content/uploads/2021/11/2021.11.03-Global-Americans_Reporte-Desinformacion.pdf
15. Infobae. 2020 fue el año en que Colombia tuvo más ciberataques. (2021, 25 febrero). https://www.infobae.com/america/colombia/2021/02/25/2020-fue-el-ano-que-colombia-tuvo-mas-ciberataques/
16. Infobae. La Registraduría Nacional de Colombia sufrió más de 3.000 intentos de ataques cibernéticos durante las elecciones presidenciales. (2018, 27 mayo). https://www.infobae.com/america/colombia/2018/05/27/la-registraduria-nacional-de- colombia-sufrio-mas-de-3-000-intentos-de-ataques-ciberneticos-durante-las-elecciones-presidenciales/
17. International Telecommunication Union (ITU). (2010). Unión Internacional de Telecomunicaciones. http://www.itu.int/net/itunews/issues/2010/09/20 -es.aspx
18. Leiva, E. A. (2015). Estrategias nacionales de ciberseguridad: Estudio comparativo basado en enfoque top-down desde una visión global a una visión local. Revista Latinoamericana de Ingeniería de Software, 3(4), 161-176.
19. Molina, M. D. (2009). Efectos para Colombia de los debates en torno a la seguridad del Estado y a la seguridad humana. Scielo. http:// www.scielo.org.co/scielo.php?script=sci_arttext&pid=S2011-03242009000100006
20. Ospina Díaz, M. R., y Sanabria Rangel, P. E. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Revista Criminalidad, 62(2), 199-217.
21. Salazar, D. (2021, 19 noviembre). Rusia y China están interesados en elecciones de América Latina, según reciente informe. Asuntos Legales. https:// www.asuntoslegales.com.co/actualidad/rusia-y-china-estan-interesados-en-elecciones-de-america- latina-segun-reciente-informe-3264812
22. Santos, D. (2022, 6 febrero).Colombia, en los ojos de Rusia y China. El Tiempo. https:// www.eltiempo.com/opinion/columnistas/diego-santos/colombia-en-los-ojos-de-rusia-y-china-columna-de-diego- santos-649870

Editor: Departamento de Educación, Ciencia, Tecnología, Investigación y Doctrina-DECTID

Teléfono: 322-382-5884

Correo electrónico: semilleros.esici@cedoc.edu.co

Dirección: Carrera 8A No. 101-33, Bogotá D.C.