UNIVERSIDAD DE LA DEFENSA
FACULTAD MILITAR CONJUNTA
INSTITUTO DE CIBERDEFENSA DE LAS FUERZAS ARMADAS
DIPLOMATURA UNIVERSITARIA EN GERENCIAMIENTO DE LA CIBERDEFENSA

TRABAJO FINAL INTEGRADOR

Sesgos cognitivos y la legislación Argentina como limitantes en el quinto dominio

CT (EA) Juan M. Luna; SS (ARA) Juan I. Solis; Técnica Lourdes Fernández;

Director: CR Santiago Picon

TC (R) Carlos F. Amaya

21 de noviembre de 2023

Tabla de contenido

Resumen

La legislación local coarta la libertad de acción para las operaciones cibernéticas. La ciberseguridad y ciberdefensa, por separado, deben afrontar las amenazas según sean internas o externas. Por lo tanto, es necesario adaptarlas a la dinámica del quinto dominio con el fin de tomar medidas unificadas de respuesta.

La importancia de contar con el gestor de ciberdefensa, una figura con características híbridas (humanista y técnico), coadyuva a la integración de equipos para asesorar y asistir eficazmente al decisor.

La forma de interpretación de la legislación está marcada por los sesgos individuales y organizativos; el reconocimiento y el trabajo para morigerar el impacto en los recursos humanos colaborará en una efectiva labor en el quinto dominio.

Aportes

De acuerdo con lo mencionado en el presente trabajo, consideramos que es de vital importancia unificar la legislación para mejorar una respuesta ante una operación cibernética a nivel nacional en los ámbitos de Seguridad y Defensa. La unificación de la legislación garantizará una respuesta coherente y coordinada ante incidentes cibernéticos en todo el país.

Por el lado de los equipos de trabajo, la creación de equipos interdisciplinarios coadyuvará a lograr respuestas óptimas; como así también, generar informes de calidad que sirvan para la futura toma de decisiones. La diversidad de habilidades en estos equipos facilitará una comprensión más completa de las amenazas y una respuesta más efectiva. La colaboración entre expertos de diferentes disciplinas garantizará informes más completos y precisos. La estandarización de los informes facilitará la comparación y el intercambio de información entre diferentes entidades.

Y en cuanto al eslabón más vulnerable, los recursos humanos, crear e implementar capacitaciones para lograr un perfeccionamiento específico acorde a las exigencias que presentan las operaciones en el quinto dominio. Las actualizaciones periódicas de la formación son esenciales, dada la naturaleza dinámica del ciberespacio. La concientización pública sobre las amenazas cibernéticas y las mejores prácticas de seguridad es esencial. Una población informada contribuirá a la seguridad general y a la detección temprana de amenazas.

Planteamiento del problema

El denominado quinto dominio -ciberespacio-, se ve influenciado, y limitado, por los denominados sesgos, los mismos pueden ser aleatorios o sistémicos, cognitivos o perceptuales; también son llamados barreras. Éstos son una fuente generalizada, y pocas veces apreciada, de errores a la hora de redactar e interpretar la legislación vigente. De igual manera, la gestión de las operaciones cibernéticas indefectiblemente se verá influenciada por los sesgos, desde el diseño de algoritmos hasta la toma de decisiones y la implementación de políticas, ya que es inmanente al ser humano; como así también, según la tesis de doctorado de MARÍN MARTÍNEZ (2021) plantea que los sesgos intervienen en los algoritmos basados en el aprendizaje.

Ejemplo de los sesgos se pueden nombrar a la interpretación, relacionando con la capa social, del Manual de Tallin (no vinculante); en nuestro país es dicotómico responder a una operación cibernética, si la misma es llevada por actores internos o externos.

A lo mencionado se puede agregar la legislación local, que goza de una falta de actualización a la vorágine que se maneja en el quinto dominio. La Ley 25.326 -Protección de los datos personales- es un viva imagen de ello.

Por último, el recurso humano que posiblemente trabaja aislado, como así también un equipo de trabajo altamente cohesionado (que generalmente tiende a no tener críticas de sus miembros), tiene una alta probabilidad de extremar la influencia de los sesgos en la labor que llevan a cabo.

Solución propuesta

La creación de endogrupos interdepartamentales, que se encuentren regulados dentro de las normativas vigentes, para una mejor labor del operador, y así poder identificar y optimizar los distintos sesgos, dará como resultado una mejor calidad en los productos de ciberdefensa que coadyuvará a la toma de decisiones de manera eficaz. Además, una labor interagencial, logrará una respuesta eficiente a las amenazas de los distintos actores.

Objetivos

De manera general, será el de identificar y relacionar los sesgos que intervienen en el ámbito de la ciberdefensa; para crear un plan de trabajo que logre optimizarlos.

Los objetivos específicos serán:

- Conceptualizar y caracterizar a los sesgos en el ámbito de la ciberdefensa.
- Identificar las herramientas afines para dicha optimización.
- Proponer cambios en la legislación vigente para lograr un esfuerzo sinergia en el quinto dominio.

Marco teórico preliminar

Los limitantes a la hora de operar en el quinto dominio son, entre otros, los sesgos y la legislación local.

El diccionario de Cambridge define a los sesgos como “La forma en que una persona en particular entiende los eventos, los hechos y otras personas, que se basa en su propio conjunto particular de creencias y experiencias y puede no ser razonable o precisa”.

Dividiendo a la producción de información en dos momentos, la obtención y la producción propiamente dicha; encontramos la presencia de sesgos en ambas etapas. La empresa CISCO en su curso “conceptos básicos del análisis de datos” (*Data Analytics Essentials*), trata a los sesgos cognitivos en el ámbito de la obtención de datos; y enfocándonos en el análisis para la producción de información, encontramos a Kriszan (1999), Heuer (1999) y Payá Santos (2017). Los mencionados sostienen que los sesgos hacen referencia a atajos mentales que se traducen en barreras que conducen a errores mentales surgidos de la aplicación de técnicas para la simplificación del procesamiento de la información.

En el ámbito de la obtención los sesgos son de **confirmación** que se refiere a los tipos de datos seleccionados para el análisis; además se encuentran los de **selección**, aquí el elemento de obtención puede caer en elección de un conjunto de datos incompletos o no representativos para el análisis.

Otro tipo de sesgo en la obtención son los de **interpretación**, externa e interna, los mismos pueden surgir de la mala interpretación del requerimiento de obtención (cómo fue formulada la pregunta) o bien, de la interpretación de lo que muestran los datos; los de **información** se refieren al cúmulo de datos que sirvieron para producir la información que será analizada; por último, se encuentran los **predictivos**, estos hacen referencia a la recopilación de datos históricos que son empleados para realizar análisis y las condiciones históricas, varían de la actual.

En cuanto a producción, identificamos a la **evaluación de la evidencia** que se refiere a que, ante vacíos de información, el analista los completa con su experiencia; con respecto a los de **percepción de la causa - efecto**, hace referencia a estimación personal, con base en la evidencia y la experiencia, a cómo se evalúa el impacto de una acción. Otro sesgo es relacionado a la **estimación de probabilidades**, la restricción de información disponible en tiempo y forma hará que las probabilidades sean evaluadas con una baja probabilidad, mientras que un exceso, generaría una exagerada probabilidad de una apreciación; por último, la **retrospección en la evaluación de informes**, este es de vital importancia para el asesoramiento oportuno para acciones concretas y para legislar. Las diferentes perspectivas del analista, consumidor y supervisor, tienen sus propios sesgos por el nivel de contacto con la realidad del área, como así también, aquí se acentúan los sesgos organizativos.

Con respecto a la legislación local nos encontramos con que la ley de Defensa Nacional y la de Seguridad Interior, difieren en las competencias a las Fuerzas Armadas y a las Fuerzas de Seguridad y Policiales, respectivamente (Ley N° 23.554/1988, 1988) (Ley Nº 24.059/1992, 1992).

Por el lado del sector Defensa, la Directiva de Política de Defensa Nacional (DPDN) correspondiente al año 2021 (Presidencia, 2021); sostiene que *“la ciberdefensa debe minimizar el riesgo de la exposición y contrarrestar eventos que afecten la libre disponibilidad del ciberespacio en las operaciones militares que realice el INSTRUMENTO MILITAR, en*

cumplimiento de la normativa vigente en materia de Defensa Nacional", siendo *"abordado a partir de niveles de disuasión razonables, en cumplimiento de la misión primaria y esencial del INSTRUMENTO MILITAR"*.

Además sostiene que *"La priorización, desde la perspectiva de la Defensa, del control efectivo de los espacios … aeroespaciales y ciberespaciales de jurisdicción nacional…".*

Complementando la DPDN, el Ministerio de Defensa, mediante la resolución Nro. 105/2023, creó el **Comité de infraestructuras Críticas de la Información de la Defensa** y el **Centro de Supervisión y Control de Gestión de Ciberdefensa**, para coadyuvar a los esfuerzos del Sistema de Defensa Nacional para asegurar el funcionamiento de las Infraestructuras Críticas, centralizar y gestionar la información para la prevención de incidentes cibernéticos (Ministerio de Defensa, República Argentina, 2023).

Mientras que, la Estrategia Nacional de Ciberseguridad de la República Argentina (Ministerio de Defensa, República Argentina, 2023), sostiene a la responsabilidad compartida como principio rector.

En el año 2021, como organismo dependiente de la Dirección Nacional de Ciberseguridad de la República Argentina, se crea el Centro Nacional de Respuesta a Incidentes Informáticos (CERT.AR.) que tiene como objetivo *"...coordinar la gestión de incidentes de seguridad a nivel nacional y prestar asistencia en aquellos que afecten a las entidades y jurisdicciones del sector público nacional definidas en el inciso a) del artículo 8° de la ley nº 24.156 y sus modificatorios y a las infraestructuras críticas de información, declaradas como tales"* (Dirección Nacional de Ciberseguridad, 2021).

Metodologías y técnicas utilizadas para contrastar la Hipótesis

El trabajo lo desarrollamos aplicando la exploración de la web para hallar información relacionada con los temas antes mencionados, para luego contrastarlo con herramientas on-demand. A su vez, con toda la información obtenida utilizamos el método Scamper para organizar los pensamientos.

El método Scamper fue utilizado para constatar la viabilidad de los objetivos planteados. De tal modo pudimos reducir la cantidad de los mismos y optimizar las posibles soluciones.

Para apreciar cómo estamos posicionados utilizamos el Índice global de ciberseguridad (2020), donde la ITU confeccionó el perfíl del país (International Telecommunication Union, 2021). Ver Anexo 1: perfil del país ITU.

El mencionado índice a su vez refleja que a nivel mundial el país ocupa el puesto 91 sobre 182; y a nivel regional 13 de 35 países. Siendo de consideración las ponderaciones en cuanto a Capacity Development (desarrollo de la capacidad) y Cooperative Measures (medidas cooperativas), lo que nos categoriza como un país en desarrollo en cuanto al área ciber.

A nivel local la búsqueda de los informes del Centro Nacional de Respuesta a Incidentes Informáticos, arrojó las siguientes cifras hubo un incremento de ataques en 2021, respecto a 2020 (Dirección Nacional de Ciberseguridad, 2022):

- Año 2020: Doscientos veintiséis (226) ataques.
- Año 2021: Quinientos noventa y un (591) ataques.

El informe publicado en el año 2023 indica que hubo una disminución de ataques en 2022, respecto a 2021 (Dirección Nacional de Ciberseguridad, 2023):

- Año 2021: Quinientos noventa y un (591) ataques.
- Año 2022: Trescientos treinta y cinco (335) ataques.

El informe refleja que el aumento interanual fue de 261,50% entre 2020 a 2021, si bien la expresión en porcentaje parece importante al observar la variable numérica discreta nos encontramos con que podría no marcar los valores reales de las amenazas, además que el

porcentaje no sería real.. *"...según el impacto que cause el incidente, se consideraron cuatro niveles de severidad, que son denominados como bajo, medio, alto y crítico. Durante el período analizado, es decir el año 2021, 467 de los incidentes reportados (79,02%) fueron de severidad alta, seguidos de 69 de severidad media (11,68%), 39 de severidad baja (6,60%) y 16 de severidad crítica (2,71%)..."*. En el informe de 2021 a 2022 los incidentes reportados bajaron un 43,3% los ataques, "*...si bien se redujo la cantidad de incidentes reportados, hubo un incremento en los incidentes considerados críticos, como por ejemplo los dirigidos a los Ministerios, que al ser entidades públicas, tuvieron gran visibilidad. De los datos relevados en el sector privado nos encontramos con una situación similar al verse disminuidos los incidentes reportados por phishing, pero aumentaron los incidentes por ransomware dirigidos. Esto presupone los vectores de ataques e intereses económicos y/o dañinos de los ciberatacantes…"*.

Por ejemplo el informe de la INTERPOL de 2020 indica que, solo, en el sector privado *"... entre enero y el 24 de abril de 2020 se detectaron 907 000 correos basura, 737 incidentes de tipo malware, y 48 000 URL maliciosas, todos ellos relacionados con la COVID-19"* (Interpol, 2020). De aquí podemos apreciar la falta de información del sector público y los meses faltantes, por lo tanto, podrían existir sesgos de información y/o interpretación en el informe del Centro Nacional de Respuesta a Incidentes Informáticos.

Con respecto a las denuncias voluntarias de los incidentes, ver Anexo 2: informe de denuncia de incidente ciber., el informe presenta cierto tecnicismo que puede ser tomado como una barrera para las organizaciones que no tengan un área específica de gestión de la información y deben realizar la denuncia.

Referencias

Cambridge Dictionary. (S/I). *COGNITIVE BIAS | English meaning - Cambridge Dictionary*. Cambridge Dictionary. Recuperada Noviembre 13, 2023, desde https://dictionary.cambridge.org/dictionary/english/cognitive-bias

Dirección Nacional de Ciberseguridad. (2021, Febrero 19). *Disposición 1/2021*. Argentina.gob.ar. Recuperada Noviembre 15, 2023, desde https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-1-2021-347311

Dirección Nacional de Ciberseguridad. (2022, Febrero 2). *Informe 2 CERT 2021 F*. Argentina.gob.ar. Recuperada Noviembre 17, 2023, desde https://www.argentina.gob.ar/sites/default/files/2022/02/informe_2_cert_2021_f__0.pdf

Dirección Nacional de Ciberseguridad. (2023, Febrero 2). *Informe CERT 2022.docx*. Argentina.gob.ar. Recuperada Noviembre 17, 2023, desde https://www.argentina.gob.ar/sites/default/files/2023/02/informe_cert_2022.docx.pdf

Heuer, R. J. (1999). *Psychology of Intelligence Analysis - Center for the Study of Intelligence*. International Association of Law Enforcement Intelligence Analysts. Recuperada November 13, 2023, desde https://www.ialeia.org/docs/Psychology_of_Intelligence_Analysis.pdf

International Telecommunication Union. (2021). *Global Cybersecurity Index 2020*. ITU. Recuperada Noviembre 17, 2023, desde https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Interpol. (2020, Agosto 4). *Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19*. Interpol. Recuperada Noviembre 17, 2023, desde https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

Kriszan, L., & Colegio Conjunto de Inteligencia Militar - Estados Unidos de América. (1999). *Elementos esenciales de inteligencia para todos*. Google Books. Recuperada Noviembre 13, 2023, desde https://books.google.com.ar/books?id=qNVf0AunxA0C&ots=DnrjfdBQWj&dq=Krizan%2C%20Lisa%2C%20Intelligence%20Es%3Fsentials%20for%20Everyone%2C%20Occasional%20Paper%20Number%20Six%2C%20Center%20for%20Stra%3Ftegic%20Intelligence%20Research%20-%20Joint%20Military

Ley N° 23.554/1988. (1988, Octubre 2). *Ley de DEFENSA NACIONAL N° 23.554*. InfoLeg. Recuperada Noviembre 13, 2023, desde https://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20988/texact.htm

Ley Nº 24.059/1992. (1992, Enero 0). *Ley de SEGURIDAD INTERIOR Nº 24.059*. InfoLeg. Recuperada Noviembre 13, 2023, desde https://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/458/texact.htm

MARÍN MARTÍNEZ, A. P. (2021, Noviembre). *TESIS DOCTORAL: CIBERÉTICA, AGENTES MORALES ARTIFICIALES Y RESPONSABILIDAD JURÍDICA INTERNACIONAL*. BULERIA Principal. Recuperada Noviembre 4, 2023, desde https://buleria.unileon.es/bitstream/handle/10612/15457/Ciber%C3%A9tica_agentes_morales_artificiales.pdf?sequence=1&isAllowed=y

Ministerio de Defensa, República Argentina. (2023, Enero 30). *Actualización de la Política de Ciberdefensa y creación de dos áreas para la supervisión y control de amenazas en el ciberespacio*. Argentina.gob.ar. Recuperada Noviembre 16, 2023, desde https://www.argentina.gob.ar/noticias/actualizacion-de-la-politica-de-ciberdefensa-y-creacion-de-dos-areas-para-la-supervision-y

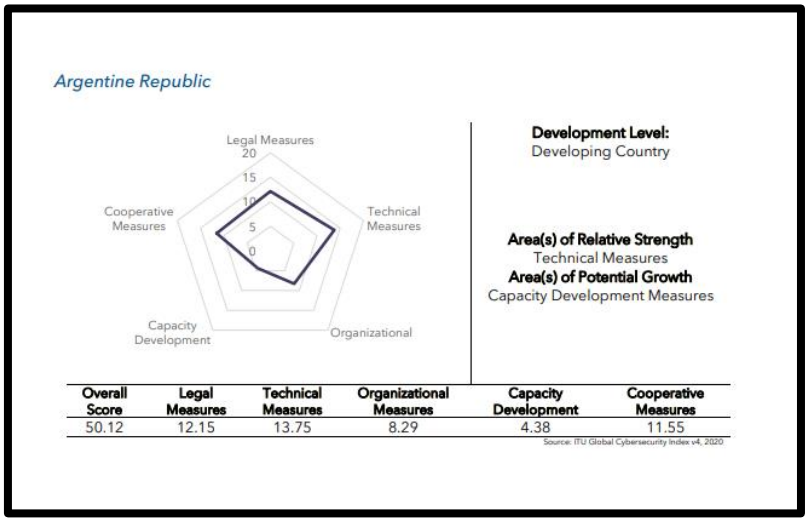
Payá Santos, C. (2017, Julio 25). *Aproximación transversal a los sesgos cognitivos del analista de inteligencia*. TDX (Tesis Doctorals en Xarxa). Recuperada Noviembre 13, 2023, desde https://www.tdx.cat/handle/10803/572076

Presidencia. (2021, Julio 19). *DIRECTIVA DE POLÍTICA DE DEFENSA NACIONAL - Decreto 457/2021*. BOLETIN OFICIAL REPUBLICA ARGENTINA. Recuperada Noviembre 13, 2023, desde https://www.boletinoficial.gob.ar/detalleAviso/primera/246990/20210719

Secretaría de Innovación Pública. (2023, Septiembre 4). *JEFATURA DE GABINETE DE MINISTROS SECRETARÍA DE INNOVACIÓN PÚBLICA - Resolución 44/2023*. BOLETIN OFICIAL REPUBLICA ARGENTINA. Recuperada Noviembre 13, 2023, desde https://www.boletinoficial.gob.ar/detalleAviso/primera/293377/20230904

Anexos

Anexo 1: perfil del país ITU.



Fuente: International Telecommunication Union, 2021.

Anexo 2: informe de denuncia de incidente ciber.

Tipo de incidente *
Seleccione el tipo de incidente a informar.

- Sitio web
- Compromiso de un activo de información
- Compromiso de una red informática
- Phising
- Spam
- Ransomware
- Malware / Virus informático

Severidad

	Ninguno	Bajo	Medio	Alto	Crítico
Grado					

La descripción del incidente es la parte más importante de este informe. Considere una descripción clara y bien descriptiva que nos ayude a la gestión del incidente.

Título del incidente *

Descripción *

Debilidad

Impacto

Su correo electrónico

Enviar

Fuente: https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar/reportar-un-incidente (recuperada 20 de noviembre de 2023)

CV

DATOS PERSONALES:

JUAN IGNACIO SOLIS

CONTACTO: juanignaciosolis85@gmail.com

TELÉFONO: +549 011 1521573606

EDUCACIÓN SUPERIOR:

- LICENCIADO EN ADMINISTRACIÓN CON ORIENTACIÓN PRIVADA – UNIVERSIDAD NACIONAL ARTURO JAURETCHE - 2016/21.
- MAESTRANDO DE 2DO AÑO EN INTELIGENCIA ESTRATÉGICA NACIONAL SIGLO XXI - UNIVERSIDAD NACIONAL DE LA PLATA.

CURSOS VIRTUALES AUTOGESTIONADOS:

- CIBERSEGURIDAD PARA MICROEMPRESAS Y AUTÓNOMOS - INCIBE - ESPAÑA - 2023.
- DATA ANALYTICS ESSENTIALS – CISCO – 2023.
- INTRODUCTION TO CYBERSECURITY – CISCO – 2023.

EXPERIENCIA LABORAL:

Integrante de la Armada Argentina desde 2003 a la fecha.

CV

DATOS PERSONALES:

APELLIDO Y NOMBRE: Fernández Lourdes Ximena.

CONTACTO: lufernandez97@gmail.com

TELÉFONO: +5492291466874

CIUDAD: Miramar, Buenos Aires.

EDUCACIÓN SUPERIOR:

- Técnico en Instalación y Mantenimiento de Sistemas de Cómputos.- ISFT N° 194
- Tramo de formación pedagógica para profesionales y técnicos superiores- FASTA

EXPERIENCIA LABORAL:

- Junio 2019- Marzo 2022 | Secretaria, inmobiliaria Ballarre(Miramar).
- Desde octubre 2019- Actualmente | Docente, DGCyE.

CV

DATOS PERSONALES: JUAN MANUEL LUNA

CONTACTO: juanmanuellunaabadia@gmail.com

TELÉFONO: +54264 4757750

EDUCACIÓN SUPERIOR:

- LICENCIADO EN CONDUCCIÓN Y GESTIÓN OPERATIVA.
- TÉCNICO EN REPARACIÓN Y MANTENIMIENTO DE PC..

EXPERIENCIA LABORAL:

Integrante del Ejercito Argentino desde 2007 a la fecha.