ANÁLISIS DE LA CIBERDEFENSA Y CIBERSEGURIDAD EN LA SEGURIDAD CIUDADANA EN BOGOTÁ

AUTOR

JORGE ELIECER RODRIGUEZ GARZON

DOCENTE ASESOR

RUTH MERY QUITIAN BUSTOS

UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD

ADMINISTRACIÓN DE LA SEGURIDAD Y SALUD OCUPACIONAL

BOGOTÁ, COLOMBIA - 2022

Resumen

Dentro del ensayo se establece como objetivo la descripción de las características y situación de ciberseguridad de la información de las personas en el contexto de la ciudad de Bogotá, para ello se tomaron elementos de diagnóstico, situación actual, cifras, estrategias y acciones que permitan no solo identificar las condiciones en materia de ciberseguridad alrededor de la información personal, sino también el poder establecer estrategias, recomendaciones y acciones concretas para prevenir la ocurrencia y vulneración, minimizando así su afectación.

Se logra abordar las temáticas a través de un instrumento de revisión bibliográfica partiendo del método deductivo, en la comprensión de los conceptos de ciberseguridad y las prácticas comunes que facilitan la transgresión de la seguridad de las personas. Luego se muestra la radiografía de la situación actual en materia de ciberseguridad en la ciudad de Bogotá, con el fin de indicar con claridad cuáles pueden ser las estrategias o recomendaciones para hacer frente a dicha situación, todo esto desde una perspectiva no sólo en materia de acciones personales, también institucionales, a través de organismos tanto públicos como privados. Como conclusión se destaca que, aunque existen vulnerabilidades en el entorno de la ciberseguridad, el trabajo conjunto entre el sector público y el privado se ha orientado de forma significativa para combatir el fenómeno descrito y se han reforzado las estrategias para minimizar dichas problemáticas. A su vez las perspectivas futuras muestran un fortalecimiento de la ciberseguridad no solo en Bogotá, también lo es a nivel nacional.

Palabras Claves: *Ciberseguridad, Datos, Información, Vulneración, Protección.*

Introducción

A medida que los ataques cibernéticos continúan creciendo en tamaño, frecuencia y complejidad, la defensa cibernética es uno de los elementos más importantes y desafiantes de la estrategia de seguridad de cualquier organización. La ciberdefensa es un acto coordinado de resistencia que protege la información, los sistemas y las redes de los ataques cibernéticos mediante la implementación de procedimientos de protección como firewalls, detección y respuesta de red (NDR), detección y respuesta de punto final (EDR) para identificar, analizar y reportar que ocurre dentro de una red (Carlos et al., 2020). Aun así, los equipos de defensa cibernética enfrentan la tarea casi imposible de proteger todas las vulnerabilidades de una organización, y gran parte de esto significa poder comprender con precisión las tácticas, habilidades y motivaciones de los atacantes (Castillo & Bejarano, 2020).

Los inicios de los ciberataques se remontan a principios de la década de 1970, cuando se publicó en ARPANET el primer gusano informático, CREEPER, le siguió rápidamente REAPER, el primer software antivirus que allanó el camino para las defensas cibernéticas mucho más sofisticadas que conocemos hoy. A medida que Internet se ha convertido en una parte omnipresente de nuestra vida cotidiana, las defensas cibernéticas han tenido que evolucionar a una velocidad vertiginosa solo para mantenerse al día, pero con cada nueva defensa, el enemigo creaba un nuevo camino a su alrededor (Del Campo et al., 2021).

Después de CREEPER, los piratas informáticos fueron más allá de los simples gusanos y se apoyaron en malwares más avanzado y siniestro, como virus polimórficos, esquemas de phishing, ransomware y ataques de día cero. Con cada uno de ellos se generaron defensas

cibernéticas más efectivas, como software antivirus comercial, tecnología de firewall y recientemente, detección de punto final y respuesta de red (Cujabante Villamil et al., 2020b). Es por estos antecedentes que se debe adoptar un enfoque proactivo y unificado para las soluciones de ciberdefensa.

La seguridad y la defensa cibernéticas a menudo se usan indistintamente, aunque están relacionadas, existen diferencias claras e importantes. La ciberseguridad es un conjunto de soluciones o estrategias que emplea una organización para evitar peligros y amenazas en el ciberespacio, es de destacar que la prevención de amenazas cibernéticas es una parte importante de cualquier estrategia de seguridad deben incluir brechas, cumplimiento, acciones, etc. (Villacís, 2022).

Las preocupaciones sobre la seguridad han crecido constantemente para los gobiernos y los actores públicos en las últimas décadas y es que a medida que la tecnología mejora, también lo hace la necesidad de protección y seguridad. Los problemas surgen en varios dominios de aplicación, como la identidad, la protección de datos o la defensa donde los gobiernos y otros actores de ciberdefensa tienen grandes expectativas en cuanto a seguridad, experiencia en certificación y niveles tecnológicos, incluida la capacidad de confiar plenamente en cualquier sistema extranjero que pueda integrarse en su ecosistema (Marín et al., 2019).

Esta situación no es distinta para Colombia y en especial para la ciudad de Bogotá al ser la capital del país y su región más dinámica e importante tanto en número de habitantes, así como en el desarrollo económico y social del país. A partir de ello, el objetivo del ensayo es establecer las características, situación y acciones de mejora de la ciberseguridad de la información

personal en el contexto de la ciudad de Bogotá, así como los elementos de ciberdefensa aplicables. Teniendo en cuenta lo anterior, en primera instancia se debe describir un marco teórico general sobre la ciberseguridad y ciberdefensa, las distintas tipologías de ataques y acciones que se realizan para vulnerar la seguridad. De igual forma, mostrar las condiciones actuales de ciberseguridad, seguido de las acciones en ciberdefensa que puedan ser aplicables para minimizar las vulnerabilidades encontradas. Finalmente es indispensable analizar las estrategias y acciones para mejorar la ciberseguridad con respecto a la información personal de los ciudadanos de la Capital de Colombia.

Análisis estadístico de la ciberseguridad y ciberdefensa

En 2012 hubo 41 mil millones de intentos de ciberataques en todo el mundo y 7 mil millones en Colombia. El cibercrimen está generando cada vez más rentabilidad para los atacantes, y con eso en mente, la trayectoria de los ciberataques para empresas y agencias gubernamentales seguirá creciendo si no hay herramientas para contrarrestarlos y protegerse. Según el último informe de la fiscalía general de la Nación, en 2020 el número de ciberataques en Colombia aumentó un 38% con respecto al año anterior (Gómez et al., 2021).

Si bien las empresas y agencias gubernamentales han estado trabajando arduamente en estrategias para fortalecer las medidas de ciberseguridad, estas no han sido suficientes, casos como la eliminación de información o la atribución de datos a través de ransomware o ataques de día cero, así como fugas de datos, continúan ocurriendo y las organizaciones tienen grandes pérdidas económicas a raíz de los de los altos pagos a los ciberdelincuentes dentro de la tipología delictiva por inseguridad en el ciberespacio (Torres Rojas, 2021).

En los últimos meses se han conocido numerosos casos de ciberataques a organismos oficiales a nivel mundial y nacional, el año 2021 ha puesto de relieve la capacidad de defensa de la ciberseguridad de las empresas y organismos públicos, sin embargo, la eficacia de sus sistemas de seguridad se ha visto comprometida y así se ha podido demostrar en algunos de los ciberataques más sonados de 2021 y todo lo ocurrido en 2022 (Cano-Martínez, 2022). Se podría pensar que el aumento de estos ataques se debe a la sofisticación de las técnicas utilizadas en relación con la escalada de los mismos, la cantidad de rescate exigida por los atacantes a las víctimas que ha aumentado considerablemente, especialmente debido a la apreciación del valor de la moneda virtual Bitcoin (Bueno Munar, 2022). Debido a esto, las grandes corporaciones han pagado decenas de millones de dólares en rescates a los atacantes.

El robo de información se ha convertido en un negocio rentable y ha sido testigo incluso de las organizaciones más grandes del mundo; a medida que las empresas paguen a los ciberdelincuentes, este sistema criminal seguirá creciendo. Muchas de estas situaciones ocurren en Colombia, de hecho, instituciones como el Senado, la Presidencia y las Fuerzas Armadas han sido atacadas. Casos recientes incluyen el Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima), Aeronáutica Civil y el Departamento Administrativo Nacional de Estadística de Colombia (DANE) reportando ransomware, daños a servidores internos y ataques informáticos a información sensible y confidencial (Cadena Alvarado, 2022).

El grado de criticidad y las características de los ataques pueden variar, sin embargo, las modalidades más comunes están asociadas a la infección de malware de diferentes escalas, pero la motivación es la obtención ilícita de ganancias, ya sea a través del robo de credenciales, secuestro de información (ransomware), exfiltración de información y fuga de características de

seguridad para la divulgación en línea y la venta de datos en DarkNet (aunque cada vez más, la venta de datos en línea es superficial). (Del Campo et al., 2021).

En el primer trimestre de 2022 se registraron 9.226 denuncias por delitos cibernéticos en Bogotá; casi 3.000 casos menos que el año pasado, mientras que en el mismo primer trimestre del 2021 ya se reportaron 12.012 casos de violaciones a la integridad, confidencialidad y disponibilidad de datos y sistemas de información. Robo de computadoras con 3.574 casos en 2022 versus 3.981 casos reportados en el primer trimestre de 2021 (Bueno Munar, 2022). Además de ello, se conoce de casos recurrentes de robo de identidad bancaria, para luego transferir activos de cuentas afectadas. En cuanto a las violaciones de datos personales registraron una disminución del 39% a 1947 casos considerando la diferencia con 2021 cuando se informaron 3.204 casos. El robo de identidad en sitios web generalmente se asocia con casos de phishing, que registraron 914 casos en el primer trimestre de 2022 en comparación con 1.545 casos en el primer trimestre de 2021 (Cadena Alvarado, 2022).

Otra de las tendencias identificadas en el año 2022 fueron los ciberataques especializados dirigidos a proveedores de servicios o actores de la cadena de suministro de tecnología. Los actores malintencionados saben que, al dirigirse a vendedores y proveedores, podrían comprometer a sus clientes a través de activos tecnológicos compartidos. Muchas empresas trabajan con docenas de proveedores para todo, desde el suministro de materiales de producción hasta la subcontratación de mano de obra y tecnología (Cano-Martínez, 2022). Por este motivo, es muy importante proteger la cadena de suministro y asegurarse de que las empresas que suministran la tecnología estén debidamente aseguradas.

Las personas tanto jurídicas como naturales que han vivido la pandemia han aprendido mucho sobre ciberseguridad y las acciones de cómo integrar a sus procesos, debido a que en la región ha aumentado la cantidad de transacciones inusuales sospechosas de fraude en un 139 % en lo que va del año 2022, lo que requiere un esfuerzo gigantesco para detectarlas y contenerlas. Ante ello las organizaciones con políticas de autenticación basada en riesgos (RBA) o aquellas con esquemas de validación razonables tuvieron un buen desempeño; pero para las otras que solo acaban de definir su modelo de protección, su vulnerabilidad es una preocupación obvia (Villacís, 2022).

Un análisis más detallado de las modalidades más comúnmente reportadas; pone en primer lugar la vulneración de la protección de datos personales consagrada en el Código Penal colombiano como se evidencia en el artículo 269F, que presentó un incremento del 123% con más de 5.734 denuncias interpuestas frente a las 2.757 de 2020. En muchos casos, el contenido de los mensajes incluye enlaces que facilitan la navegación que redirige a sitios web con formularios donde recopilan información personal para generar suplantación de identidad o robo de la misma. (Cadena Alvarado, 2022). Es de especial análisis el hecho de que se siga suplantando a las agencias gubernamentales, cuyo objetivo es generar confianza a las posibles víctimas y explotar el engaño para acceder a su información.

La segunda modalidad con mayor incremento; está directamente relacionada con la tendencia anterior y se refleja en el aumento del 33% en las denuncias de usurpación de identidad presentadas por sitios web para recabar datos personales consagrados en el Código Penal en el artículo 269G; Esta modalidad, que bien podría adoptar la forma de phishing, smishing o pharming, registró un cambio absoluto de 608 casos, con 2.473 denunciados a la Fiscalía General

de la República, frente a los 1.865 de 2020. Los enlaces maliciosos siguen siendo el principal vector de infección utilizado por los ciberdelincuentes además de códigos maliciosos que explotan vulnerabilidades en aplicaciones y sistemas operativos obsoletos o con errores (Cano-Martínez, 2022).

Ante estos datos expuestos se puede ver como se ha dado un incremento significativo alrededor de las amenazas y ataques cibernéticos tanto en Colombia como en la ciudad de Bogotá, esto en relación con el aumento de la usabilidad de los medios electrónicos para diversas acciones de compras, trabajos, estudios y demás aspectos que se vieron impulsados por la presencia de la pandemia del coronavirus que se apoyó de forma constante en la virtualización de muchas actividades lo que hace que el nivel de exposición a este tipo de ataques sea mucho mayor dado que las personas se encuentran más tiempo en la red.

Conceptos claves de seguridad informática

Antes de poder establecer las estrategias y recomendaciones para la mejora de la seguridad informática adoptadas por las organizaciones, se hace necesario indicar algunos conceptos claves que se relacionan con la ciberdefensa y ciberseguridad los cuales se exponen a continuación:

1.Malware

Software que realiza una tarea maliciosa en un dispositivo o red de destino, corrompe datos o toma el control de un sistema.

2. Suplantación de identidad

En un ataque por correo electrónico, se engaña al destinatario del correo electrónico para que revele información confidencial o descargue malware haciendo clic en un hipervínculo en el mensaje.

3. Suplantación de identidad subacuática

Esta es una forma más sofisticada de phishing en la que el atacante detecta a la víctima y finge ser alguien que conoce y en quien confía.

4. Ataque "Man in the Middle" (MitM)

Cuando un atacante establece una posición entre el emisor y el receptor de mensajes electrónicos y los intercepta, posiblemente modificándose durante la transmisión. El emisor y el receptor creen que se están comunicando directamente entre sí. Un ataque MitM podría usarse en el ejército para confundir a un enemigo.

5. Troyanos

Llamado así por el caballo de Troya en la historia griega antigua, el caballo de Troya es un tipo de malware que se infiltra en un sistema de destino que se parece a algo, p. Software listo para usar, pero luego filtra el código malicioso una vez dentro del sistema host.

6. Ransomware

Un ataque que encripta datos en el sistema de destino y exige un rescate para que el usuario recupere el acceso a los datos. Estos ataques van desde molestias menores hasta incidentes importantes, como el apagón de datos de la ciudad de Atlanta en 2018.

7. Ataque de denegación de servicio o ataque de denegación de servicio distribuido (DDoS)

Cuando un atacante toma el control de muchos (quizás miles) de dispositivos y los usa para invocar funciones de un sistema de destino, p. un sitio web que hace que se bloquee debido a una sobrecarga.

8. Ataque a dispositivos IoT

Los dispositivos IoT, como los sensores industriales, son vulnerables a varios tipos de ciberamenazas. Esto incluye que los piratas informáticos se apoderen del dispositivo para convertirlo en parte de un ataque DDoS y el acceso no autorizado a los datos recopilados del dispositivo. Debido a su número, distribución geográfica y, a menudo, sistemas operativos obsoletos, los dispositivos IoT son un objetivo principal para los actores malintencionados.

9. Violaciones de datos

Una violación de datos es el robo de datos por parte de un actor malicioso. Las razones de las filtraciones de datos incluyen delitos (p. ej., robo de identidad), querer avergonzar a una institución (p. ej., Edward Snowden o el hackeo del DNC) y espionaje.

10. Malware en aplicaciones móviles

Los dispositivos móviles, como otro hardware informático, son vulnerables a los ataques de malware. Los atacantes pueden incrustar malware en descargas de aplicaciones, sitios web móviles o correos electrónicos y mensajes de texto de phishing. Una vez comprometido, un

dispositivo móvil puede brindarle al actor malintencionado acceso a información personal, datos de ubicación, cuentas financieras y más.

Acciones y estrategias para la mejora de la seguridad informática

La seguridad cibernética requiere cada vez más la colaboración entre organizaciones debido a la aparición de amenazas cibernéticas nuevas, diversas y transnacionales, estas amenazas pueden ser de diversos tipos. Por ejemplo, el ciberterrorismo se puede utilizar para incitar el miedo a la violencia con fines políticos y obtener apoyo para grupos violentos, mientras que los ciberataques respaldados por el estado se pueden lanzar para sabotear o espiar a otras entidades (Pinto Rico et al., 2018).

Por otro lado, los delincuentes maliciosos y los militantes pueden piratear los sistemas informáticos corporativos y gubernamentales para interrumpir las operaciones o robar activos valiosos. Finalmente, existe el peligro de una amenaza interna que emana de empleados descontentos que sabotean o protestan contra su propia organización, por lo que aspectos como la ignorancia o el descuido del personal pueden exacerbar aún más estas amenazas (Agüero & Vallejo, 2019).

Ante estas amenazas se requiere ciberinteligencia sobre las capacidades y planes de los actores maliciosos para anticiparse y protegerse contra las ciberamenazas (Jasper, 2017; Mattern et al., 2014; Velasco, 2016). Siguiendo a Gill y Phythian (2006, p. 19), definimos inteligencia como un proceso de recopilación y análisis de información con el objetivo de proporcionar alertas y desarrollar políticas para proteger o mejorar una ventaja relativa (Gómez et al., 2021). En el contexto de la seguridad cibernética, esto significa que las capacidades, intenciones y

actividades de los adversarios y competidores potenciales, a medida que evolucionan, en el dominio cibernético deben entenderse y analizarse (Torres Rojas, 2021). Con la ayuda de la ciberinteligencia, las organizaciones públicas y privadas pueden fortalecer su ciberseguridad y proteger la privacidad digital, la propiedad y la infraestructura crítica.

La complejidad y la velocidad de las ciberamenazas actuales hacen que sea casi imposible que las organizaciones las gestionen de forma independiente, por lo que al actuar de forma aislada no podrá contrarrestar las amenazas cibernéticas que evolucionan rápidamente, existe una necesidad urgente de construir una inteligencia compartida para la cual la colaboración y la apertura con otras organizaciones son esenciales (Villacís, 2022).

Dicha colaboración es más efectiva cuando se extiende más allá de las fronteras, involucrando no solo a los proveedores tradicionales de seguridad pública sino también a los actores privados (Ortiz Osorio, 2020). Si bien la necesidad de un papel activo para las partes públicas y privadas en las redes de ciberseguridad es indiscutible, en la práctica, la colaboración cibernética a menudo resulta compleja. Pero, si bien hay mucha investigación sobre asociaciones internacionales y nacionales entre agencias de inteligencia pública, se sabe poco sobre la colaboración con y entre partes privadas en redes de inteligencia cibernética (o seguridad cibernética) (Diaz Padilla, 2021).

Frente a las nuevas y crecientes amenazas a la ciberseguridad (Rudner, 2013), se reconoce ampliamente que ningún actor de inteligencia puede tener éxito actuando solo (Cujabante Villamil et al., 2020a). En cambio, la gestión eficaz de la ciberseguridad requiere el esfuerzo concertado de diferentes actores a nivel internacional como es el caso de organizaciones públicas

de ciberseguridad, agencias independientes, empresas prestadoras de servicios de internet entre otros. Así mismo los servicios de inteligencia de diferentes países han formado sociedades y coaliciones para intercambiar información analizada de manera rápida y eficiente (Huaman Baltazar, 2021).

A nivel nacional, las agencias de inteligencia pública tienen el mandato de trabajar juntas, mientras que se alienta cada vez más a las partes privadas a tomar el camino de compartir inteligencia cibernética y medidas colectivas de seguridad cibernética (Villacís, 2022). Cuando tales esfuerzos fallan, "existe el riesgo de que la inteligencia no llegue a manos de quienes la necesitan, cuando la necesitan" (Cujabante Villamil et al., 2020a, pag 5). Debido a esto, las operaciones de inteligencia cibernética requieren proactividad, una comprensión precisa y actualizada del entorno de amenazas y una toma de decisiones basada en datos (Del Campo et al., 2021). Frente a contratiempos y posibles riesgos de inactividad, un número cada vez mayor de actores se dedican a la ciberinteligencia, lo que ha permitido el surgimiento de redes de ciberinteligencia por lo que no es sorprendente que estas redes enfrenten algunos problemas y desafíos de colaboración.

Ante estos escenarios se esperaría una cooperación de inteligencia más estrecha a nivel nacional, ya que existe apoyo político para compartir información cibernética entre agencias gubernamentales, así como organizaciones privadas, sin embargo, este optimismo a menudo resulta ser infundado o poco desarrollado. Esto dado que en la realidad la recopilación y el análisis de información parecen estar muy fragmentados en muchos países, ya que las autoridades operan en relativo aislamiento, creando barreras significativas que dificultan la colaboración exitosa, como lo han demostrado varios estudios de caso (Montoya et al., 2020).

Esta fragmentación conduce al uso de procesos de recopilación de información incongruentes y procedimientos burocráticos desalineados (Robles Puentes, 2020). Ante esto, como muestra un análisis de los servicios de inteligencia belgas, esta fragmentación puede reducir la motivación de cooperación entre los diferentes actores o incluso impedir que vean los beneficios (Marin et al., 2019). Aún más problemático es que muchas agencias de inteligencia tienen mandatos similares o superpuestos y pueden participar en guerras territoriales (Rozo Díaz, 2021). De hecho, las guerras territoriales son un problema común, ya que las autoridades públicas tienen sus propios intereses y ven a otros actores (dentro del gobierno) como una amenaza para sus intereses (Padilla et al., 2021).

La polarización resultante puede evitar sinergias operativas al crear silos, silencio y redundancia (Castillo & Bejarano, 2020). De hecho, "las guerras territoriales burocráticas a menudo actúan como una barrera para la necesaria integración geográfica y funcional" (Sloan, 2006, p. 203). Si bien estas acciones pueden parecer insignificantes, la polarización parece obstinada y, por lo tanto, no se reemplaza fácilmente en la práctica por la colaboración (Realpe & Cano, 2020). Estas experiencias de colaboración del sector público en ciberinteligencia apuntan a la necesidad de expectativas cautelosas de colaboración público-privada en ciberseguridad.

Recientemente, la participación del sector privado en la colaboración de inteligencia cibernética ha atraído una atención considerable. Se ha recomendado ampliamente la participación del sector privado en los esfuerzos de colaboración para mejorar la gestión de amenazas cibernéticas (Mosquera, 2021). Frente a esto varios autores norteamericanos incluso han argumentado que la ciberseguridad requiere, en última instancia, de la colaboración entre los

actores del sector público y privado (Ospina Díaz & Sanabria Rangel, 2020). Por lo tanto, no sorprende que varios gobiernos hayan intentado establecer alianzas y redes público-privadas (o intersectoriales) para compartir ciberinteligencia (Robles Puentes, 2020). Por ejemplo, en Canadá, se han establecido redes público-privadas para mejorar el intercambio de información cibernética recopilada y analizada (Pinto Rico et al., 2018). De manera similar, el Centro de Coordinación de Seguridad de Infraestructura Nacional del Reino Unido reúne a diferentes partes para proteger la infraestructura crítica de las amenazas cibernéticas.

A nivel local y en especial para el caso de la ciudad de Bogotá se debe tambien replicar el trabajo conjunto entre instituciones publicas y privadas donde se involucren acciones no solo de mejoramiento de la infraestructura de ciberdefensa para organismos cruciales como la policía nacional, la fiscalía, las instituciones bancarias, las dependencias políticas entre otras. Si no tambien se deben adelantar acciones de pedagogía para los usuarios a nivel personal, corporativo y laboral frente a la exposición que existe alrededor de las amenazas cibernéticas y la forma en como pueden prevenirlas evitando la ingeniería social que es una de las grandes problemáticas existente alrededor de la vulnerabilidad en los sistemas informáticos.

Finalmente pero no menos importante, se deben seguir aumentando las acciones de ciberdefensa haciendo uso de infraestructura tecnológica que sea mucho mas robusta y con protocolos de red que puedan brindar un mayor blindaje frente a los ataques que son recibidos de formas constante por los hackers e intrusos de la red que cada día buscan mejorar sus acciones y que estas cumplan con sus objetivos de vulnerabilidad, de allí entonces la necesidad de que las empresas y las personas tambien se actualicen.

Conclusiones

La ciberseguridad ha tomado actualmente un rol importante dentro de los elementos de la protección de los datos y la información esencialmente en un mundo donde el internet se ha vuelto fundamental en el diario vivir de las personas y se relaciona con una diversidad de sectores que van desde lo social, económico, educación, entre otros, donde el volumen de datos que se tienen diariamente son sumamente álgidos, de allí entonces que la ciberseguridad sea tan importante en la actualidad.

Las personas, las empresas y los gobiernos deben invertir en seguridad cibernética para proteger sus datos y activos de los delincuentes. La importancia de la ciberseguridad en este mundo cada vez más centrado en Internet es primordial. La seguridad cibernética es importante para obtener una ventaja competitiva, ya que ayuda a proteger a las empresas y organizaciones de los ataques cibernéticos. Invertir en seguridad cibernética permite a las organizaciones mejorar su postura de seguridad y evitar que los piratas informáticos ingresen a sus sistemas.

A nivel local tanto en Colombia como en Bogotá, las acciones de ataques cibernéticos muestran una clara tendencia al aumento, por lo que se hace mas que necesario la adopción de estrategias y alternativas para lograr una mejor protección y reducir la vulnerabilidad a la que las empresas y personas se encuentran expuestas. Se debe entender que las acciones de vulneración de datos, robos y acceso a datos son una realidad que se desprenden de la misma naturaleza del uso del internet, por ello es un aspecto que no se debe descuidar en ningún momento si se quiere tener una usabilidad eficiente de la red.

Referencias

Agüero, W. F., & Vallejo, M. C. (2019). *Integrando estrategias de ciberdefensa mediante una propuesta de trabajo*. Universidad de la Defensa Nacional UNDEF.

Bueno Munar, L. D. (2022). *Ciberseguridad en Colombia, avances y retos*.

Cadena Alvarado, A. M. (2022). *Crecimiento del ciberfraude en Colombia durante la pandemia por Covid-19*.

Cano-Martínez, J. J. (2022). Prospectiva de ciberseguridad nacional para Colombia a 2030. *Revista Científica General José María Córdova*, *20*.

Carlos, C. G. C., Luciano, M. S., & Carlos, F. V. (2020). *Análisis y estrategia de implementación de un marco de trabajo de ciberseguridad para la unidad de Ciberdefensa del Ejército Nacional.*

Castillo, R. D. L., & Bejarano, M. H. (2020). Ciberseguridad y Ciberdefensa en Colombia. *Revista Avenir*, *4*(2), 25–36.

Cujabante Villamil, X. A., Bahamón Jara, M. L., Prieto Venegas, J. C., & Quiroga Aguilar, J. A. (2020a). Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova*, *18*(30), 357–377.

Cujabante Villamil, X. A., Bahamón Jara, M. L., Prieto Venegas, J. C., & Quiroga Aguilar, J. A. (2020b). Cybersecurity and cyber defense in Colombia: A possible model for civil-military

relations. *Revista Científica General Jose María Cordova*, *18*(30), 357–377.

Del Campo, E. A. P., Alvis, S. P., Acevedo, M. E. S., & Aguirre, C. M. (2021). Estado y soberanía en el ciberespacio. *Via Inveniendi Et Iudicandi*, *16*(1), 1–46.

Diaz Padilla, J. D. L. R. (2021). *Diseño documental para la creación del centro de respuesta a incidentes cibernéticos de la Empresa Cibersecurity de Colombia LTDA.*

Gómez, O. M. V., Pérez, M. M. E., & Ramírez, P. A. C. (2021). Los delitos informáticos virtuales en redes sociales y las medidas que ha tomado el Estado colombiano para garantizar la protección integral de los ciudadanos al año 2019. *Dirección Editorial*, 231.

Huaman Baltazar, J. L. (2021). *Análisis de las Capacidades en Ciberseguridad y Ciberdefensa del Centro de Ciberdefensa y Telematica del Ejército, Lima, 2020*.

Marin, J., Nieto, Y., Huertas, F., & Montenegro, C. (2019). Modelo ontológico de los ciberdelitos: Caso de estudio Colombia. *Revista Ibérica de Sistemas e Tecnologias de Informação*, *E17*, 244–257.

Montoya, Y. C., Verdezoto, V. H., & Ramírez, A. V. (2020). *Ciberdefensa, Ciberseguridad Y Sus Efectos En La Sociedad*.

Mosquera-Chere, S. O. (2021). Experiencias de seguridad cibernética en países europeos y latinoamericanos. Apuntes hacia la defensa nacional. *Polo Del Conocimiento*, *6*(3), 1251–1273.

Ortiz Osorio, M. (2020). *Importancia de las buenas prácticas en ciberseguridad en el trabajo*

remoto de entidades públicas de Colombia en época de pandemia.

Ospina Díaz, M. R., & 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.

Padilla, D. E. C., Carvajal, C. F. A., Ortiz, R. A. C., Bernal, S. P. E., Riola, J. M., & Fajardo-Toro, C. H. (2021). *Ciberseguridad y ciberdefensa marítima: análisis bibliométrico años 1990–2021*.

Pinto Rico, R. A., Hernández Medina, M. J., Pinzón Hernández, C. C., Díaz López, D. O., & Camilo García Ruíz, J. C. (2018). Inteligencia de fuentes abierta (OSINT) para operaciones de ciberseguridad." Aplicación de OSINT en un contexto colombiano y análisis de sentimientos". *Revista Vinculos*, *15*(2).

Realpe, M. E., & Cano, J. (2020). *Amenazas Cibernéticas a la Seguridad y Defensa Nacional. Reflexiones y perspectivas en Colombia*.

Robles Puentes, H. A. (2020). *Panorama actual de la seguridad informática o de la ciberseguridad, a nivel del país y las tendencias actuales y futuras a nivel global.*

Rozo Díaz, J. F. (2021). *La importancia del hacking en la ciberseguridad a nivel organizacional en entidades de orden público en Colombia*.

Torres Rojas, L. D. (2021). *El ciberespacio como escenario estratégico de Seguridad y Defensa en el desarrollo de políticas en Colombia*.

Valoyes Mosquera, A. (2019). *Ciberseguridad en Colombia*.

Villacís, R. P. C. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador. *Revista Tecnológica Ciencia y Educación Edwards Deming*, *6*(1).

https://scholar.google.es/citations?view_op=view_citation&hl=es&user=6F_tiDwAAAAJ&citation_for_view=6F_tiDwAAAAJ:Tyk-4Ss8FVUC