

# SISTEMAS



## Criptoactivos

Implicaciones tecnológicas,  
económicas y sociales



ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

Calle 93 No. 13 - 32 of. 102  
Bogotá, D.C.  
[www.acis.org.co](http://www.acis.org.co)



# ISACA®

Bogotá Chapter



**Certified Information Security Manager.**  
An ISACA® Certification



**Certified in the Governance of Enterprise IT.**  
An ISACA® Certification



**Certified in Emerging Technology.**  
An ISACA® Certification

**CSX** CYBERSECURITY  
FUNDAMENTALS CERTIFICATE

**CQBIT** 2019

**Mayor Información**  
[www.isaca.org/credentialing](http://www.isaca.org/credentialing)

Los miembros de ISACA pueden beneficiarse del acceso, ahorros y conocimiento para impulsar su éxito en auditoría, control, seguridad, ciberseguridad y gobernanza de SI / TI en una multitud de industrias. Member Advantage abarca el conjunto de beneficios que los miembros de ISACA reciben para avanzar profesionalmente y ser recompensados personalmente a lo largo de toda su carrera.

¡Sé parte de **ISACA Bogotá!**



# En esta edición

## Editorial

4

**Criptoactivos: retando las fronteras del sistema financiero internacional**

**DOI: 10.29236/sistemas.n163a1**

En un contexto frágil, ansioso, no lineal e incomprensible (FANI) lo normal es enfrentar tensiones e inestabilidades en cualquier momento; en este sentido, los criptoactivos se configuran como el nuevo referente de valor en el contexto digital que establece nuevas oportunidades y retos para las inversiones y movimientos económicos internacionales, más allá de las fronteras tradicionales del sistema financiero actual.

## Columnista Invitado

10

**Criptoactivos y su esencia**

**DOI: 10.29236/sistemas.n163a2**

La innovación financiera impulsada por su desarrollo.

## Entrevista

18

**Experto en criptoactivos**

**DOI: 10.29236/sistemas.n163a3**

Pablo Sanz Bayón señala a Colombia entre las diez economías del mundo más grandes en criptomonedas.

## Investigación

26

**XXII Encuesta Nacional de Seguridad Informática**

**DOI: 10.29236/sistemas.n163a4**

Aprendiendo del futuro de la ciberseguridad.

## Cara y Sello

81

**Criptoactivos**

**DOI: 10.29236/sistemas.n163a5**

Implicaciones tecnológicas, económicas y sociales.

## Uno

94

**Criptoactivos**

**DOI: 10.29236/sistemas.n163a6**

Deconstruyendo los bienes, los valores y los medios de pago en un contexto digital.

## Dos

107

**Monedas digitales**

**DOI: 10.29236/sistemas.n163a7**

Protocolos de consenso y consumo de energía: Impacto y retos medioambientales de las criptodivisas.

Publicación de la Asociación Colombiana de  
Ingenieros de Sistemas (ACIS)  
Resolución No. 003983 del  
Ministerio de Gobierno  
Tarifa Postal Reducida Servicios Postales  
Nacional S.A. No. 2015-186 4-72  
ISSN 0120-5919  
Apartado Aéreo No. 94334  
Bogotá D.C., Colombia

**Dirección General**

Jeimy J. Cano M.

**Consejo de Redacción**

Francisco Rueda F.  
Gabriela Sánchez A.  
Manuel Dávila S.  
Andrés Ricardo Almanza J.  
Emir Hernando Pernet C.  
Fabio Augusto González O.  
Jorge Eliécer Camargo M.  
María Mercedes Corral S.

**Editores Técnicos**

Jeimy J. Cano M.  
Andrés Ricardo Almanza J.

**Editora**

Sara Gallardo M.

**Junta Directiva ACIS**

2022-2024

**Presidente**

Luis Javier Parra B.

**Vicepresidente**

Jorge Fernando Bejarano L.

**Secretario**

Rodrigo Rebolledo M.

**Tesorero**

Jaime García C.

**Vocales**

Hilda Cristina Chaparro L.  
Soledad Mercedes Gutiérrez R.  
Ernesto José Garnica B.

**Directora Ejecutiva**

Beatriz E. Caicedo R.

**Diseño y diagramación**

Bruce Garavito

Los artículos que aparecen en esta edición no  
reflejan necesariamente el pensamiento de la  
Asociación. Se publican bajo la responsabilidad  
de los autores.

**Abril - Junio 2022**

Calle 93 No.13-32 Of. 102  
Teléfonos 616 1407 - 616 1409  
A.A. 94334  
Bogotá D.C.  
www.acis.org.co

# NASCO

NACIONAL DE COMPUTADORES S.A.

APOYA ESTA PUBLICACIÓN

TEL: 6 06 06 06- CR 15 No 72-73



**Confía en 4-72,**  
el servicio de envíos  
de Colombia

Línea de atención al cliente:  
**(57 - 1) 472 2000 en Bogotá**  
**01 8000 111 210 a nivel Nacional**

.....  
**www.4-72.com.co**



**YOU  
DESERVE  
THE  
BEST  
SECURITY**

<https://www.checkpoint.com/es/>

# Criptoactivos: retando las fronteras del sistema financiero internacional

DOI: 10.29236/sistemas.n163a1



*En un contexto frágil, ansioso, no lineal e incomprensible (FANI) lo normal es enfrentar tensiones e inestabilidades en cualquier momento; en este sentido, los criptoactivos se configuran como el nuevo referente de valor en el contexto digital que establece nuevas oportunidades y retos para las inversiones y movimientos económicos internacionales, más allá de las fronteras tradicionales del sistema financiero actual.*

Jeimy J. Cano M.

La aceptación y el crecimiento exponencial de los criptoactivos son el resultado de un doble fenómeno: en primer lugar, un mayor interés por las transacciones financieras que operan fuera de los límites de los controles financieros tradicionales para proporcionar privacidad y seudonimato; y, en segundo lugar,

unas tasas de inflación elevadas que hacen que estos nuevos activos sean inversiones financieras potencialmente más estables que las monedas tradicionales (Gore & Camp, 2022).

En este contexto, los criptoactivos como nueva representación del va-

lor en el contexto digital juegan un papel fundamental como habilitadores de posibilidades, servicios o productos que terminan capitalizando nuevas oportunidades para los individuos y cambiando la forma tradicional de las operaciones financieras. Por tanto, como afirma el Banco de España, “la evidencia empírica muestra que, en general, en el pasado, las innovaciones en el sector financiero han elevado el crecimiento potencial de la economía, (...) también han llevado aparejados procesos de fragilidad financiera, elevando los riesgos para la estabilidad del sistema, especialmente durante su fase de adopción, que, en algunos casos, han llegado a producir crisis bancarias” (Banco de España, 2022, p.150).

Así las cosas, ya no es suficiente con mantenerse informado y consciente de las volatilidades económicas y geopolíticas globales, sino que es necesario una vista informada de la evolución de los criptoactivos sabiendo que estos activos basados en tecnologías criptográficas están fundados en las siguientes características:

- está registrado en alguna forma de libro mayor digital distribuido y asegurado con criptografía,
- no está emitido ni garantizado por un banco central o una autoridad pública, y
- puede utilizarse como medio de intercambio y/o con fines de inversión y/o para acceder a un

bien o servicio (Houben & Snyers, 2020).

Es por esto que los criptoactivos, como nuevo agente disruptivo de las finanzas internacionales, se consolidan como el nuevo horizonte y reto internacional, que exige a las naciones, empresas e individuos mantener una postura vigilante y proactiva frente a sus riesgos inherentes: (Banco de España, 2022, p.156-158)

- La dependencia de su valor actual de las expectativas de compradores y vendedores sobre su valor en transacciones futuras que generan riesgos significativos de mercado y de liquidez.
- La ausencia de regulación y la incertidumbre tecnológica que pueden generar riesgo de crédito y de fraude en las transacciones con estos instrumentos.
- La tecnología subyacente de registro descentralizado tiene ciertos riesgos operativos intrínsecos (olvido o robo de claves de acceso a estos registros, fallos en la programación, uso de la naturaleza descentralizada con propósitos de fraude, etc.). Además, es dependiente de la estructura general de telecomunicaciones, con la posibilidad de que los ciberataques dificulten o impidan las transacciones.
- La participación de agentes con intenciones ilícitas (en particular,

el lavado de dinero) puede generar riesgos legales a otros participantes en estos mercados.

- Los riesgos climáticos físicos y de transición debido al elevado consumo energético de ciertas operaciones particularmente en los procesos de verificación.

De ahí que esta edición de la revista *Sistemas*, de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–, apunta a revisar, explorar y analizar los retos y oportunidades de los criptoactivos, con el fin de traer al escenario actual diferentes posturas y comprensiones sobre el tema, como insumo para plantear alternativas y opciones en un entorno FANI. Con ese propósito fueron convocados profesionales especialistas, quienes desde su experiencia proponen reflexiones para seguirle la pista al desarrollo de las tendencias y prácticas vigentes, capitalizando lecciones aprendidas, repensando las dinámicas de los negocios y retos actuales, así como al futuro que se avizora en el horizonte.

El abogado Erick Rincón, columnista invitado, establece desde su práctica como presidente de la Asociación Colombia Fintech, un marco base para reflexionar sobre la evolución de los criptoactivos, para lo cual presenta diferentes estadísticas donde se ilustran los avances del mercado de las criptomonedas motivando entre otros aspectos a los gobiernos a un mayor desplie-

gue y regulación de las mismas, habida cuenta de las nuevas oportunidades y retos que genera para el ecosistema digital colombiano y sus actores.

En la entrevista el profesor Pablo Sanz Bayón, profesor de Derecho Mercantil en la Facultad de Derecho (ICADE) de la Universidad Pontificia Comillas de Madrid, nos comparte sus reflexiones sobre los fundamentos de los criptoactivos, su visión sobre la evolución de esta temática en el mercado colombiano, así como aspectos de seguridad y protección para los ciudadanos. Igualmente detalla algunas ideas sobre el futuro en el que las humanidades serán parte fundamental para darle forma a los retos y oportunidades de estos activos digitales.

Por su parte, el ingeniero Andrés Almanza Junco presenta el análisis de los resultados de la versión número veintidós de la encuesta nacional de seguridad de la información, realizada cada año por ACIS, estudio que revela las tendencias más representativas de las empresas colombianas en los temas de protección de la información y la evolución del líder digital de seguridad, así como sus respectivos contrastes con la realidad internacional, que ubican a la ciberseguridad como una capacidad empresarial necesaria para el desarrollo de negocios digitales, en medio de las tensiones geopolíticas y de cumplimiento actuales.



El foro de esta revista fue un espacio para compartir visiones desde diferentes ángulos sobre los criptoactivos. Los ingenieros Fabio Mauricio Pinzón, Julio López Medina y la economista Ana María Zuluaga Tafur desarrollaron un diálogo abierto y nutrido para contrastar y complementar sus posturas desde la banca central, los reguladores del sector financiero y la práctica de consultoría. Ellos advierten sobre la necesidad de educar a los ciudadanos sobre estas nuevas propuestas financieras emergentes para que aumente su sensibilidad y conocimiento sobre esta realidad que va a estar circulando a su alrededor y que, si bien no va a ser moneda de curso legal, va a estar presente como una tentación permanente.

Así mismo, nuestros lectores dispondrán de dos artículos para reflexionar sobre los criptoactivos en dos visiones conceptuales y prácticas que buscan analizar sus orígenes e impactos concretos sobre el uso de esta nueva forma de materializar el valor en el escenario digital. En un primer documento el profesor Alejandro Useche, profesor asociado de la Universidad del Rosario, se ocupa de explorar y analizar el impacto medioambiental de las monedas digitales donde se introduce el concepto de criptomonedas “sucias” y “limpias”, concluyendo que es necesario que la efectividad técnica del blockchain se complemente con el fomento de la sostenibilidad medioambiental.

El segundo artículo, escrito por este servidor, explora los fundamentos conceptuales de los criptoactivos y analiza al menos siete tendencias del uso de la tecnología DLT (*Digital Ledger Technology* –Tecnología de libro mayor digital–) que a la fecha vienen avanzando a nivel internacional y, que prometen cambiar la dinámica de la actividad financiera mundial para comenzar una transición de las tradicionales lecturas de valor, desde nuevas propuestas basadas en tecnología.

En resumen, se trata de un panorama renovado de nuevas transformaciones, retos y propuestas alrededor de los criptoactivos, que tensionan las certezas de los saberes y prácticas existentes en las finanzas globales. Su contenido invita a todos los profesionales en las diferentes áreas del saber a explorar las nuevas realidades de un mundo digital y tecnológicamente modificado, sin perjuicio de los nuevos desafíos políticos, económicos, sociales, tecnológicos, legales y ecológicos, en los que el concepto del valor, las criptomonedas, los *tokens* y una realidad aumentada y extendida, revelan nuevas incertidumbres y potencian el desarrollo de capacidades de negocio inexistentes, de cara a los riesgos que aún no aparecen en sus mapas estratégicos.

## Referencias

Gore, K. & Camp, C. (2022). *Cryptoassets and Dispute Resolution: Four Things to*

Know. European Financial Review. March.  
<https://www.europeanbusinessreview.com/cryptoassets-and-dispute-resolution-four-things-to-know/>

Banco de España (2022). Especial Criptoactivos. Informe de estabilidad financiera. Primavera.  
[https://www.bde.es/f/webbde/Secciones/Publicaciones/InformesBoletinesRevistas/InformesEstabilidadFinanciera/22/IEF\\_2022\\_1\\_CapE.pdf](https://www.bde.es/f/webbde/Secciones/Publicaciones/InformesBoletinesRevistas/InformesEstabilidadFinanciera/22/IEF_2022_1_CapE.pdf)

Houben, R. & Snyers, A. (2020). Cryptoassets. Key developments, regulatory concerns and responses. Think Tank European Parliament. Study requested by the European Parliament's Committee on Economic and Monetary Affairs.  
[https://www.europarl.europa.eu/thinktank/en/document/IPOL\\_STU\(2020\)648779](https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2020)648779)

**Jeimy J. Cano M., Ph.D, CFE, CICA.** Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes. Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Ph.D en Business Administration por Newport University, CA. USA. y Ph.D en Educación por la Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.

## ¿Cómo están actuando los líderes de TI para proteger sus aplicaciones?

El Informe de Seguridad en la Nube de Fortinet presenta datos relevantes sobre las tendencias de seguridad en la nube en las organizaciones:

**38%**

detectó amenazas/brechas de seguridad.

**43%**

admitió que descuida la seguridad por "la prisa por el lanzamiento".

**46%**

reconoció que necesita personal capacitado.

¿Está utilizando un WAF basado en la nube para proteger tanto las instalaciones locales como la nube?



**EL 46%**

utiliza un WAF basado en la nube para proteger tanto las instalaciones locales como en la nube

SÍ

39%

NO

15%

No está seguro

# Criptoactivos y su esencia

DOI: 10.29236/sistemas.n163a2



*La innovación financiera  
impulsada por su desarrollo.*

Erick Rincón Cárdenas

Corría el mes de noviembre de 2008 un mensaje enviado a la lista de correo sobre criptografía de metzdowd.com firmado con el alias Satoshi Nakamoto y titulado «Bitcoin P2P e-cash paper»<sup>1</sup>. Este mensaje contenía un protocolo para un nuevo sistema de efectivo electrónico denominado Bitcoin. 13 años después este protocolo es la principal referencia que tiene el público en general para entender e ingresar al mundo de los criptoactivos digitales. Esta acción desenca-

deno en forma poderosa toda una serie de tecnologías que han evolucionado y apalancado la innovación financiera a nivel mundial. En sus inicios estaba circunscrito a un conjunto de expertos programadores y entusiastas de la criptografía, sus métodos realmente eran novedosos y revolucionarios, reservados para tan solo un puñado de co-

---

<sup>1</sup> Vigna, Paul; Casey, Michael J. (January 2015). The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order (1 edición). New York: St. Martin's Press. ISBN 978-1-250-06563-6.

nocedores y expertos. 2 meses después de aquel mensaje, el 2 de enero de 2009 entra a funcionar la primera red basada en el protocolo de bitcoin, iniciando de esta manera una revolución que aún no se ha detenido, todo inicio con el primer bloque minado por el propio Nakamoto. A continuación podemos observar el comportamiento del precio del bitinio en los últimos 7 años<sup>2</sup> (Figura 1).

Pasaron casi 8 años para que el valor de la moneda comenzara a tener una demanda importante y a volverse visible en el entorno mundial. Muchas situaciones ocurrieron dentro del ecosistema en este tiempo. Cada vez más empresas y usuarios empezaron en forma tem-

prana a utilizar la moneda y con el tiempo se desarrolló toda una economía alrededor de la criptomoneda.

Esta tecnología fue acuñada a partir de la conceptualización de la cadena de bloques un sistema de registro contable distribuido que permite soportar y garantizar la seguridad del dinero digital.<sup>3</sup>

Este enorme aporte permite alcanzar un consenso sobre la integridad de los datos por parte de todos los participantes de la red sin necesidad de recurrir a una entidad de confianza que centralice la información. Este concepto es la base fundamental del mundo de los criptoactivos.

Basado en esta tecnología y fiel al pasado innovador de los criptoactivos Vitalik Buterin comenzó el desarrollo de Ethereum en diciembre de 2013 a partir de lo construido en Bitcoin, desarrollo las bases de lo que sería la segunda generación de los criptoactivos digitales. El

<sup>2</sup> <https://finance.yahoo.com>

<sup>3</sup> Orcutt, Mike (1 de marzo de 2018). «Ethereums smart contracts are full of holes» (html). TechnologyReview (en inglés). Archivado desde el original el 6 de marzo de 2018. Consultado el 18 de abril de 2018. «A blockchain is essentially a shared accounting ledger that uses cryptography and a network of computers to track assets and secure the ledger from tampering.»

Figura 1



despliegue de este proyecto sentó las bases necesarias para una serie importante de innovaciones. El propósito inicial del proyecto Ethereum es el de descentralizar la web mediante la introducción de cuatro componentes como parte de la hoja de ruta de su Web 3.0: publicación de contenido estático, mensajes dinámicos, transacciones confiables y una interfaz de usuario integrada y funcional. Estos componentes están diseñados para reemplazar algunos aspectos de la experiencia Web que damos por sentado actualmente, pero haciéndolo de una manera completamente descentralizada y anónima<sup>4</sup>. A continuación podemos observar el comportamiento del Ether en los últimos 4 años<sup>5</sup> (Figura 2).

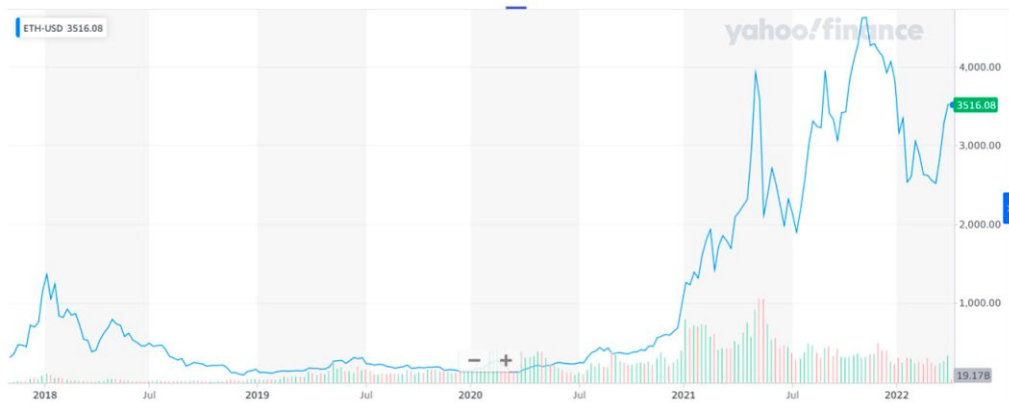
Es importante indicar que la evolución de los criptoactivos está enmarcada en estos dos casos de uso realmente exitosos y que han sido una evolución natural en la innovación desde esa primera propuesta

anónima para una red descentralizada y una moneda electrónica. Sobre estas dos tecnologías y algunas predecesoras han surgido una importante cantidad de proyectos innovadores que buscan afinar y mejorar las características, niveles de uso, velocidad, costo, protocolos, aplicaciones y se ha generado un inmenso ecosistema de criptoactivos digitales. Hay podemos contabilizar más de 10.000 monedas digitales. Según el portal especializado <https://www.coingecko.com> con una capitalización de mercado que supera los 2 billones de dólares. Es importante tener en cuenta que el Producto Interno bruto de Brasil para el 2020 era de 1.445 Billones de dólares. A continuación se muestra la capitalización de mercado para los 10 cripto-

<sup>4</sup> Winters, Tristan (25 de abril de 2014). «Web 3.0 A Chat With Ethereum's Gavin Wood». Consultado el enero de 2015.

<sup>5</sup> <https://finance.yahoo.com>

Figura 2



activos más importantes en este momento<sup>6</sup> (Figura 3).

A continuación podemos observar un histórico de la capitalización de mercado del Bitcoin<sup>7</sup> (Figura 4).

Podemos observar que en los dos últimos años el Bitcoin se ha casi triplicado en capitalización de mercado. Esto no evita la importante volatilidad del criptoactivo.

Detallando estas gráficas podemos observar el enorme crecimiento del











mercado de los criptoactivos a nivel mundial, estimulado en una gran parte por la crisis sanitaria de los últimos 2 años y por el interés tanto de los países, las empresas y las personas de este tipo de tecnología y de sus casos de uso.

Como lo indicamos anteriormente el mundo de los criptoactivos ha

<sup>6</sup> <https://www.coingecko.com>

<sup>7</sup> <https://es.statista.com/estadisticas/1236380/bitcoin-valor-de-capitalizacion-bursatil-a-nivel-mundial/>

Figura 3

#	Moneda		Precio	Volumen en 24 h	Cap. de mercado
☆ 1	 <b>Bitcoin</b>	BTC	46.471,67 US\$	29.713.225.843 US\$	882.669.232.528 US\$
☆ 2	 <b>Ethereum</b>	ETH	3512,01 US\$	18.000.167.966 US\$	423.704.133.031 US\$
☆ 3	 <b>Tether</b>	USDT	1,00 US\$	67.225.212.772 US\$	82.525.173.017 US\$
☆ 4	 <b>BNB</b>	BNB	446,01 US\$	1.932.432.668 US\$	75.198.791.270 US\$
☆ 5	 <b>USD Coin</b>	USDC	1,00 US\$	4.137.550.862 US\$	51.607.737.029 US\$
☆ 6	 <b>Solana</b>	SOL	131,13 US\$	2.508.165.762 US\$	42.813.122.794 US\$
☆ 7	 <b>Terra</b>	LUNA	115,49 US\$	2.451.762.760 US\$	40.655.939.725 US\$
☆ 8	 <b>XRP</b>	XRP	0,827848 US\$	2.347.931.438 US\$	39.810.211.092 US\$
☆ 9	 <b>Cardano</b>	ADA	1,20 US\$	2.261.744.166 US\$	38.548.147.957 US\$
☆ 10	 <b>Avalanche</b>	AVAX	94,86 US\$	1.202.565.612 US\$	25.364.087.815 US\$

crecido de forma exponencial a través de la innovación y la cadena de bloques. Esto ha generado importantes proyectos de aplicación práctica como son: los contratos inteligentes, las monedas estables, las finanzas descentralizadas. Entre otros. A continuación presento la capitalización de mercado de los 10 principales proyectos y casos de uso del ecosistema de criptoactivos a nivel mundial<sup>8</sup> (Figura 5).

El mundo de los criptoactivos tiene como su base fundamental la innovación, el despliegue tecnológico y el uso abierto de la tecnología, así como en varios casos la descentralización.

Por último, los recientes conflictos de carácter militar han elevado el interés de los países y de sus bancos centrales en el ecosistema crip-

to. El Dólar digital y Yuan digital, son solo algunos ejemplos de posibles casos de uso aplicado en bancos centrales y países. Los gobiernos han determinado acelerar su despliegue y regulación, esto traerá nuevas oportunidades y retos al ecosistema y sus actores.

## Implicaciones tecnológicas económicas y sociales.

Después de revisar y evidenciar el crecimiento acelerado de los criptoactivos en los 3 últimos años podemos extraer las siguientes conclusiones.

- La tecnología asociada a la cadena de bloques y orientada a

<sup>8</sup> <https://www.coingecko.com/en/categories>

Figura 4

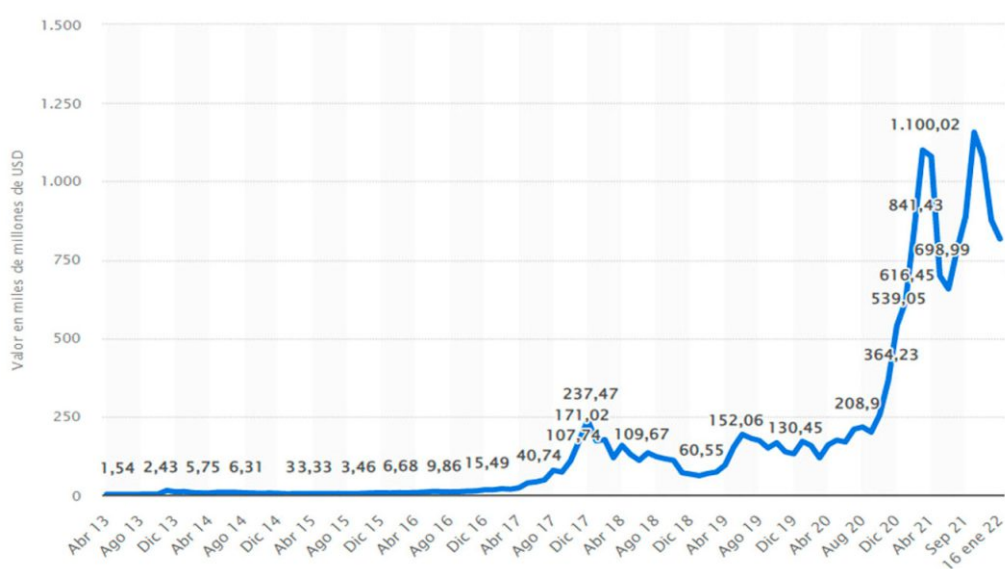














Figura 4

#	Categoría	Monedas principales	Capitalización de mercado	Volumen en 24 h
1	Smart Contract Platform		791.911.735.198 \$	45.003.511.653 \$
2	BNB Chain Ecosystem		359.813.284.594 \$	97.787.160.953 \$
3	Polygon Ecosystem		346.876.709.159 \$	90.475.140.777 \$
4	Avalanche Ecosystem		314.895.063.808 \$	86.943.596.031 \$
5	Moonriver Ecosystem		299.025.503.129 \$	84.754.834.597 \$
6	Fantom Ecosystem		242.850.491.252 \$	85.902.561.721 \$
7	Stablecoins		190.845.715.297 \$	79.247.422.897 \$
8	Arbitrum Ecosystem		188.370.383.790 \$	77.202.324.211 \$
9	Near Protocol Ecosystem		183.248.851.103 \$	76.942.781.427 \$
10	Decentralized Finance (DeFi)		147.486.097.659 \$	10.036.437.592 \$

los activos digitales ha tenido un enorme crecimiento en los últimos 5 años. En diferentes proyectos y casos de uso. esto lo podemos ver en la capitalización de mercado del ecosistema Cripto cercano a los 2 billones de dólares. El tamaño del PIB de una economía desarrollada.

el traslado de recursos y la exploración de nuevos métodos de ahorro, así como la solicitud de préstamos y el otorgamiento de los mismos. El ecosistema Cripto ha tenido un enorme interés por parte de las empresas, los países y las personas.

- La inclusión financiera ha crecido en forma acelerada específicamente en las generaciones más recientes que encuentran dentro de los criptoactivos soluciones para la inversión, el pago,
- La innovación financiera, el pensamiento exponencial, las soluciones disruptivas, la aplicación de software, la cadena de bloques, el desarrollo ágil y un carácter global, hacen del ecosistema cripto una solución de alto

impacto que trasciende las fronteras físicas en favor de la facilidad de uso y la descentralización.

- La banca tradicional ha invertido importantes recursos para desplegar sus proyectos de innovación financiera con el propósito de no quedarse atrás en el desarrollo de nuevos productos y servicios que faciliten el uso de sus clientes. Esto ha generado una importante dinámica económica apoyada por la competencia, el liderazgo y la usabilidad. En última instancia beneficia a todos los actores de la cadena.
- El ecosistema cripto ha generado una gran cantidad de soluciones no convencionales que

han ido adquiriendo una importante tracción y crecimiento. Apoyado por el amplio interés que desarrollan. Ejemplos como los contratos inteligentes y los criptoactivos estables desarrollan amplias industrias basadas en la innovación y la creatividad. Soluciones que generan crecimiento económico a través del acceso universal y se convierte en alternativas al modelo tradicional.

- Colombia resultó el tercer país con mayor crecimiento de propietarios de bitcoin (BTC) y otras criptomonedas a nivel mundial<sup>9</sup>.

---

<sup>9</sup> <https://www.criptonoticias.com/comunidad/adopcion/colombia-tercer-pais-mayor-crecimiento-adopcion-criptomonedas-mundo/>

**Erick Rincón Cárdenas.** Abogado de la Universidad del Rosario (Colombia), con posgrados en Derecho Financiero y Derecho Contractual de la Universidad del Rosario; diplomado en Comercio Electrónico Internacional de la Universidad Externado de Colombia; diploma de Estudios Avanzados D.E.A.; maestría en Derecho Mercantil de la Universidad Alfonso X de España; doctor en Derecho de la Universidad Europea de Madrid. En la actualidad es socio de Rincón Cárdenas & Moreno, presidente de la Asociación Colombia Fintech desde el año 2018 y profesor asociado de la Facultad de Jurisprudencia de la Universidad del Rosario.



27  
Años



Somos  
**MÁS QUE SEGURIDAD**

Somos  
**TRANSFORMACION DIGITAL**

Contamos con 27 años de experiencia protegiendo los activos digitales y los datos sensibles de nuestros clientes y gracias a nuestra especialización en RPA - Robotic Process Automation, hemos desarrollado numerosos proyectos orientados a habilitar la Transformación Digital y la Seguridad de la Información, por medio de herramientas y marcos metodológicos basados en estándares de reconocimiento global.



**Sede Administrativa:**

Calle 44 No. 67a - 58  
Salitre Greco - Bogotá - Colombia

**Tels:** (+57) 601 4108004 - (+57) 310 233 5760  
info@globalteksecurity.com

[www.globaltek.co](http://www.globaltek.co)

# Experto en criptoactivos

DOI: 10.29236/sistemas.n163a3

*Pablo Sanz Bayón señala a Colombia entre las diez economías del mundo más grandes en criptomonedas.*

Sara Gallardo M.

Una de las voces más importantes en el mundo digital es Pablo Sanz Bayón, profesor de Derecho Mercantil en la Facultad de Derecho (ICADE) de la Universidad Pontificia Comillas de Madrid. Investigador consagrado en el derecho de sociedades, en el análisis económico del derecho y en la regulación de las tecnologías financieras (FinTech/RegTech).

Ha sido ponente en muchos foros internacionales y su investigación actual está centrada en la regulación de la digitalización del dinero y de los medios y redes de pago, incluyendo las capacidades de la tec-

nología de registros distribuidos (DLT/Blockchain) y las posibilidades jurídicas de la denominada “tokenización” y programabilidad del dinero.

Su actividad se centra en analizar la digitalización del dinero y los pagos en el contexto regulatorio y digital de la Unión Europea y promover los cambios de política legislativa para salvaguardar la estabilidad financiera y la seguridad jurídica, así como la integridad del mercado interior.

Esa pasión por el mundo digital la acompaña de autores como Her-



mann Hess, Rudyard Kiplin y las imágenes de Kubric y Francis Ford Coppola.

Así responde a las inquietudes formuladas:

**RS:** *¿Cómo define usted los cryptoactivos?*

**Pablo Sanz Bayón:** Los cryptoactivos son, como la propia palabra indica, activos criptográficos, es decir, tokens o archivos protegidos criptográficamente mediante clave asimétrica dentro de una red DLT/Blockchain y que dotan a sus titulares y a los usuarios y miembros de esa red de diversas funcionalidades y ventajas. Desde una clave jurídico-económica, los cryptoactivos están creando mercados donde se negocian e intercambian y por ello requieren ser regulados porque son activos digitales que pueden representar distintos derechos de contenido patrimonial, diversas cla-

ses de propiedades, créditos, obligaciones, derechos de uso y de voto, dinero digital programable etc.

**RS:** *Considera que en el contexto colombiano ¿existe la cultura del cryptoactivo para el intercambio de bienes, servicios y activos? De ser así ¿cuál es su alcance?, ¿podría sugerir algunas cifras?*

**PSB:** La realidad colombiana con respecto a los cryptoactivos no difiere de las tendencias mundiales y está recorriendo las mismas etapas que el resto de los principales países y de su entorno regional. En lo que sí destaca singularmente es por su volumen, toda vez que Colombia está entre las diez economías más grandes en criptomonedas en el mundo, realizando según algunas estimaciones, más de 100.000 millones de dólares en operaciones de criptomonedas al mes. Además, el papel de los supervisores y del legislador está

siendo muy notable. De hecho, los ecosistemas de criptoactivos han pasado de tener mucha opacidad y riesgo a experimentar una progresiva regularización y supervisión.

**RS:** *¿Qué tipo de activos se manejan en Colombia en el marco de los criptoactivos? ¿Cómo se determina su valor?*

**PSB:** Bitcoin es con mucha diferencia el criptoactivo estrella, porque se lleva aproximadamente más de 70% de capitalización de mercado crypto actual. Muchas plataformas en Colombia, como sucede en España y otras partes de Europa, sólo ofrecen las de mayor capitalización de mercado: bitcoin, ether, bitcoin cash y litecoin, etc., pero a través de otros medios y canales los inversores pueden acceder a todas las demás. De hecho, según CoinMarketCap, existen 9.953 tipos de criptomonedas distintas en circulación. Respecto a su valor, los criptoactivos carecen de un valor fijo. Son activos muy fluctuantes y volátiles, y dependen mayormente de procesos de oferta y demanda. Así, por ejemplo, cuando se genera un pequeño volumen de criptomonedas con mucha demanda, el valor de éstas será alto y viceversa. Su valor también dependerá de las utilidades que el criptoactivo en cuestión ofrezca a sus usuarios y el número de plataformas en que se comercialice, que es lo que podría proporcionarle una mayor demanda y generar que su precio aumente. No obstante, cabe advertir, al igual que ya hizo el Banco de España

y la Comisión Nacional del Mercado de Valores (CNMV) de España, hace cuatro años, que los criptoactivos al día de hoy son activos de alto riesgo, debido a su extrema volatilidad, complejidad y falta de transparencia.

**RS:** *¿Qué impacto tienen en el sector financiero, considerando que los individuos funcionan de manera directa y no necesitan una entidad bancaria para su manejo y transacciones?*

**PSB:** Los criptoactivos cada vez tienen más impacto en el sector financiero, a pesar de que su capitalización es modesta teniendo en cuenta el volumen de otros activos e instrumentos de los mercados bursátiles, de divisas y de deuda, o del sector asegurador. No obstante, su crecimiento no sólo se está debiendo a que estén atrayendo cada vez a inversores minoristas, sino que grandes bancos y fondos se han metido de lleno en estos ecosistemas y comienzan a mover grandes volúmenes de compras. No sería extraño que bancos y fondos introduzcan en sus carteras de productos de inversión para el mercado minorista a los criptoactivos, si estos consiguiesen regularizarse y estabilizar su valor. El auge de las stablecoins puede contribuir a ello, también el crecimiento de las finanzas descentralizadas (DeFi) y el futuro Reglamento europeo del mercado de criptoactivos (Reglamento MiCA), que tendrá un papel muy relevante para este fin. De hecho, Europa representa actualmen-

te el 25% de toda la negociación global de criptoactivos (unos 845.000 millones de euros), por delante de Norteamérica (18%). Casi el 12% de los hogares españoles posee criptoactivos, según la encuesta de expectativas de consumo que publica el Banco Central Europeo. Este porcentaje sitúa a España como la segunda economía de la zona euro con mayor inversión, adelantada por Holanda, con más del 14%.



**RS:** *Se habla de intermediarios especializados ofreciendo servicios en ese campo, ¿podría citar algunos?*

**PSB:** Es verdad que una parte de la tecnología DLT/Blockchain que se está desarrollando está basada en protocolos criptográficos que pretenden la descentralización de las relaciones y desintermediar los procesos de transmisión y custodia de la información dentro de una red. Sin embargo, la dinámica del mercado de criptoactivos está dejando ver que también están proliferando nuevos servicios que a su vez implican la aparición de redes

permisionadas o con organizaciones y otros intermediarios, que cumplen una función demandada en este mercado por parte de los usuarios e inversores. Por tanto, será difícil que se produzca una total desintermediación y descentralización. Pueden mencionarse principalmente el amplio sector de los proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónicos. Además, hay que añadir a los proveedores de infraestructura, ciberseguridad, consultoría, servicios de confianza (privacidad e identidad digital), propiedad intelectual (muy relevante para el mercado NFT), E-Commerce, pagos y todos los sectores relativos a la computación, desarrollo de aplicaciones descentralizadas (Dapps), smart contracts, etc.

**RS:** *¿El consumidor está protegido? De ser así, ¿cómo?*

**PSB:** Está protegido parcialmente. Hay una legislación de defensa de los consumidores, normativa contractual, tributaria y sobre publicidad de las cripto-emisiones, regulación sobre protección de datos, entre otros, pero en la práctica, estamos en un mercado muy difuso, complejo y dinámico, que se mueve en la extraterritorialidad íntimamente vinculada a jurisdicciones offshore, con mucha opacidad en cuanto a registros oficiales, identificación personal, bancaria y fiscal de los promotores y directores de estos proyectos, donde no cabe la invocación de una legislación na-

cional concreta en caso de incumplimientos de contratos, fraudes, estafas u otras irregularidades. Por tanto, la eficacia del derecho queda en entre dicho si algo falla, como por ejemplo con la insolvencia de una plataforma (exchange), el error en la ejecución de un código informático o el robo de unas criptomonedas. Hace falta una armonización de los ordenamientos para llegar a cubrir los vacíos y escapatorias legales tanto en materia penal como de responsabilidad contractual y extracontractual.

**RS:** *Considerando que son un medio de intercambio digital ¿Colombia cuenta con legislación específica al respecto?*

**PSB:** Recientemente ha entrado en vigor en Colombia la Resolución 314, promulgada el 15 de diciembre de 2021 por la Unidad de Información y Análisis Financiero (UIAF), que obliga a las plataformas de intercambio de criptoactivos a reportar sus operaciones. Esto representa un cambio sustancial en el panorama de los criptoactivos en Colombia porque todos aquellos operadores que presten servicios de activos virtuales por un valor individual de US\$ 150, o por un valor mensual de US\$ 450 en nombre de terceros, tienen ya que reportar estos movimientos desde el primero de abril de 2022.

**RS:** *¿Es posible imaginar el uso masivo de los criptoactivos?*

**PSB:** Es muy posible que en unos años nos asomemos a una realidad

marcada por los criptoactivos a todos los niveles, con redes blockchain que permitan almacenar e intercambiar documentación de todo tipo y activos económicos. Una de las promesas de la “tokenización” será facilitar el acceso a la inversión, uso y disfrute de activos que antes estaban vedados a una gran parte de los inversores. Creo que los criptoactivos, si están regulados y supervisados adecuadamente, podrán ayudar a la democratización de la economía y a la inclusión financiera. No obstante, habrá que resolver varios desafíos aún pendientes como la fiscalidad, el anclaje de la identidad digital en los monederos electrónicos y la ciberseguridad “offchain”.

**RS:** *En términos de seguridad ¿qué se puede esperar? ¿Cómo anticipar el futuro en esa dirección? ¿Son una amenaza?*

**PSB:** Los sistemas de cadenas de bloques y la criptografía de clave asimétrica gozan de una seguridad muy alta. Fue una tecnología inventada precisamente para dotar a los miembros de la red de un mejor nivel de seguridad, sin hacerlo depender de un único nodo y unos pocos servidores. El problema está en lo que sucede fuera de este tipo de redes, en las redes convencionales y en los propios dispositivos de los usuarios. Estamos asistiendo a un crecimiento muy considerable de *phishing* y *ransomware*. Los *crackers* o *hackers* de sombrero negro son cada vez más sofisticados y actúan con total impunidad desde



cualquier rincón del mundo y en las profundidades de Internet, la *Dark Net*. Además, en unos años, con el surgimiento de la computación cuántica, los sistemas de cifrado que hoy poseemos serán fácilmente hackeables, en cuestión de décimas de segundo, por lo que habrá que replantear todos los esquemas y sistemas de ciberseguridad, no sólo de estos ecosistemas *Crypto*, sino de todo el mundo digital.

**RS:** *En las condiciones actuales ¿qué recomendaciones puede haber? ¿Cómo y sobre qué se debe alertar a los ciudadanos?*

**PSB:** La mejor recomendación es no hacer nada que uno no entienda. Si un producto de inversión, como es un activo criptográfico, no se comprende analizando sus características técnicas y financieras (la *tokenomics*), lo mejor es no proceder a su inversión, porque seguramente sea un producto o unos servicios complejos, no convenientes para alguien sin conocimientos cualificados en esta materia. La segunda premisa es asesorarse con anterioridad a la toma de cualquier decisión al respecto, cuando uno se adentra como inversor o miembro en empresas que desarrollan tecnología y modelos de negocio dentro de este ecosistema tan dinámico. Por otra parte, los ciudadanos deben exigir la tutela del Estado, que para eso existe. Esto se debe materializar en normas realmente eficaces, portales de transparencia y obligaciones de registro y auditoría de los operadores de es-

tos mercados, para conocer la identificación de sus responsables a efectos jurídicos.

**RS:** *Y, para finalizar la entrevista se refiere al presente y al futuro.*

**PSB:** El mayor desafío al que hacemos frente como humanidad es sin lugar a dudas el riesgo de incrementar la deshumanización debido a la tecnificación y digitalización de nuestras relaciones personales. El mundo virtual y la excesiva informatización pueden hacer que las sociedades desarrollen más individualismo y menos sentido social, moral y cultural. Que nos acabemos desconectando aún más de la realidad circundante para refugiarnos en el ciberespacio, “enredarnos” en las redes sociales y en los futuros Metaversos.

Es por ello que la ciudadanía debe prestar mucha atención al modo en que las grandes corporaciones tecnológicas y los gigantes de Internet van a programar y desarrollar sus innovaciones de software, los robots y sus máquinas inteligentes, porque estará comprometido el futuro de la sociedad. Será necesario exigir un enfoque ético a todos los actores involucrados en la industria de la Inteligencia Artificial, Aprendizaje Automático (Machine Learning) y la robótica, que se refleje en el derecho, en el ordenamiento jurídico, pero también en la educación.

Por esta razón, necesitamos más cultura humanística a todos los niveles y también en las escuelas,

durante las etapas de primaria y secundaria, y por supuesto en la Universidad. Las humanidades constituyen la fuente genuina de la experiencia cívica y de la trayectoria histórica de una sociedad humana desarrollada, cultivada y madura. A fin de cuentas, en un mundo que será dominado muy pronto por la computación, la automatización y

las máquinas inteligentes, los humanos tendremos que dedicarnos precisamente a todo aquello que las máquinas y robots no puedan hacer nunca -aunque sí puedan simularlo-; de ahí la importancia de los valores y sentimientos morales, la noción de justicia, el cultivo de las artes, de la afectividad, de la familia y los amigos. 🌐

**Sara Gallardo M.** Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas *Uno y Cero*, *Gestión empresarial* y *Acuc Noticias*. Editora de *Aló Computadores* del diario *El Tiempo*. Redactora en las revistas *Cambio 16*, *Cambio* y *Clase Empresarial*. Coautora del libro "Lo que cuesta el abuso del poder". Ha sido corresponsal de la revista *Infochannel* de México; de los diarios *La Prensa de Panamá* y *La Prensa Gráfica de El Salvador* y corresponsal de la revista *IN de Lanchile* e investigadora en publicaciones culturales. Se ha desempeñado también como gerente de *Comunicaciones y Servicio al Comensal* en *Inmaculada Guadalupe y amigos en Cía. S.A. (Andrés Carne de Res)* y editora de *Alfaomega Colombiana S.A.*; En la actualidad es asesora y editora en escritura y producción de libros. Es editora de esta revista.



# NADA BUENO SUCEDE CUANDO ESTÁS EN CONTACTO CON EL ADVERSARIO

Tanto en la naturaleza como en **ciberseguridad**, el resultado de estar en contacto con el adversario es catastrófico. **Lumu te ayuda** a identificar las conexiones entre tu empresa y criminales **en tiempo real**.

[www.lumu.io](http://www.lumu.io)

# XXII Encuesta Nacional de Seguridad Informática

*Aprendiendo del futuro de la ciberseguridad.*

DOI: 10.29236/sistemas.n163a4

Andrés R. Almanza J.

## Resumen

La encuesta de seguridad informática, capítulo Colombia, soportada por la Asociación Colombiana de Ingenieros de Sistemas (ACIS) y realizada a través de Internet, entre los meses de marzo y mayo de 2022, contó con la participación de 206 encuestados, quienes con sus respuestas permiten conocer la realidad del país en esta temática. La distribución se hizo a través de las diferentes redes sociales, comunidades y grupos. Sus resultados muestran la transformación de las prácticas de seguridad y control en el país, los cuales se contrastan con los referentes internacionales seleccionados para esta versión de la encuesta.

## Palabras clave

Seguridad de la información, encuesta, líder, perfil profesional, riesgos de información.

## Introducción

Entender la realidad nacional en materia de seguridad de la información y ciberseguridad, permite visualizar los retos a corto, mediano y largo plazo, además de construir mejores posturas de seguridad y control en las organizaciones.

Ese entendimiento, sumado a conocer el contexto internacional, proporciona una proyección al entorno nacional para enfrentar los retos y desafíos en ambientes cada vez más permeados por la realidad digitalmente modificada.

De la misma manera que en otras versiones, la Encuesta Nacional pretende medir las dinámicas y lógicas de las empresas del país, ver otros referentes mundiales en la búsqueda y construcción de los propios.

Año tras año, este estudio ha reflejado cómo ha venido desarrollándose en Colombia la protección de la información en los entornos digitales y cómo en los diferentes sectores (empresarial y académico), la seguridad y la resiliencia digital se convierten en valores estratégicos dentro de las organizaciones.

Como parte de los esfuerzos académicos para estudiar y entender la realidad de la Colombia, se resalta el análisis longitudinal de 10 años titulado “Reflexiones y retos para la academia en la formación de profesionales de seguridad/ciberseguridad en Colombia: 2010 – 2020”

(Cano & Almanza, 2021), que fue publicado en el 2021, como un registro analítico y documentado del pasado y una prospectiva sobre el futuro de la seguridad en Colombia, como un soporte más de los análisis realizados y situados de los resultados de esta nueva encuesta.

Como todos los años, se revisan para la realización de este informe, algunos de los reportes más representativos de la industria, para identificar convergencias, divergencias, contradicciones o complementos a los resultados propios de esta investigación.

## Estructura de la encuesta

El estudio contempla 39 preguntas repartidas en varias secciones sobre diferentes asuntos.

**Demografía:** Describe la información del encuestado, cuáles son las tareas que realiza, la visión de la seguridad, además de los roles que en tal sentido puedan existir dentro de su organización. Datos que permiten ubicar el sector al que pertenece, el tamaño y tipo de empresa.

**Presupuestos:** Relaciona todos los aspectos asociados con los recursos financieros destinados en materia de seguridad y, sobre todo, en qué se concentra la inversión de dichos recursos.

**Incidentes de seguridad:** Muestra los detalles y tipos de incidentes presentados, un barrido por las prácticas más importantes en el

manejo y diligencia de la evidencia digital, como herramienta en la persecución de los ciberdelincuentes.

**Herramientas y prácticas de seguridad:** Se refiere a las prácticas comunes en materia de seguridad, ese conjunto de acciones que permite a las organizaciones definir una postura clara en materia de protección.

**Políticas de seguridad:** Busca conocer el estado de las políticas de seguridad, la práctica de la gestión de riesgos y su integración en el contexto organizacional.

**Capital intelectual:** Busca definir cómo son las áreas de seguridad y las características básicas en materia de experiencia, formación y capacitación de los profesionales de seguridad. Muestra también la relación de las instituciones de educación superior frente a una realidad tan cambiante.

**Temas emergentes:** En esta sección se analizan varios aspectos, entre ellos: la percepción del futuro en materia de ciberseguridad; la vinculación de los directivos de la organización en la ciberseguridad empresarial, además de la responsabilidad y el papel del líder de seguridad en el desarrollo de la dinámica de protección de la empresa.

**Cambios:** Cada año luego de revisados los resultados de la encuesta, las opciones y los análisis correspondientes de pertinencia y re-

levancia, se cambian, adicionan, o modifican opciones. Este año no fue la excepción y se hace una pequeña variación en cuanto a la cantidad, pasando de 40 en el 2021 a 39 en el 2021. Así mismo, se agrupan preguntas en relación con los temas para motivar un análisis de datos más nutrido y la adición de nuevas opciones de respuesta de acuerdo con las tendencias existentes.

## Hallazgos principales

### Demografía

#### Sectores participantes

La Figura 1, refleja la participación de 13 sectores de la economía colombiana. Los tres segmentos con mayor participación de la encuesta para este año fueron Sector de Tecnología, Financieros, Educación y Consultoría especializada los más representativos en participación.

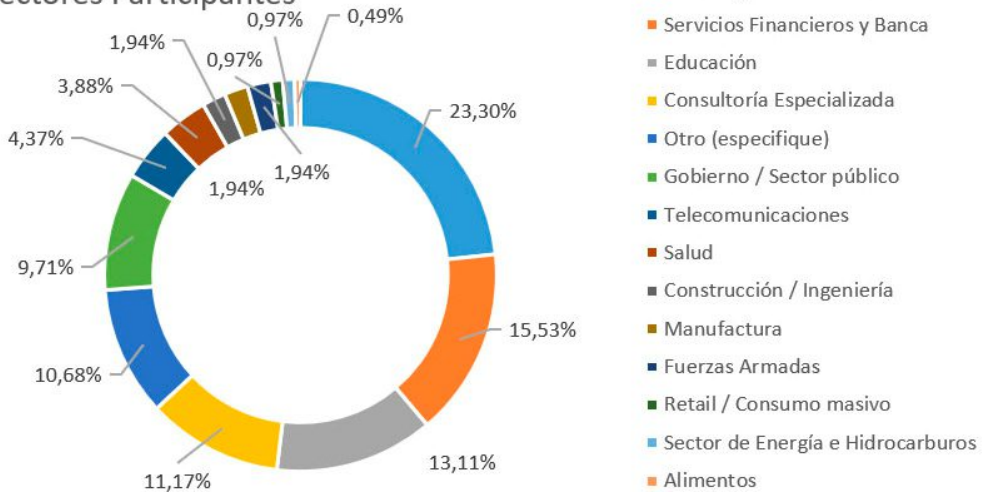
La figura 2, muestra el tamaño de las empresas en Colombia, de acuerdo con el número de empleados y se puede observar la participación de empresas de todos los tamaños y cómo la ciberseguridad ha impactado sus operaciones.

La Figura 3, muestra los cargos de los encuestados, entre los que se cuentan oficiales de Seguridad de la información, profesionales del departamento de seguridad, asesor y consultor externo auditores internos.

**Figura 1**

Sectores participantes

Sectores Participantes



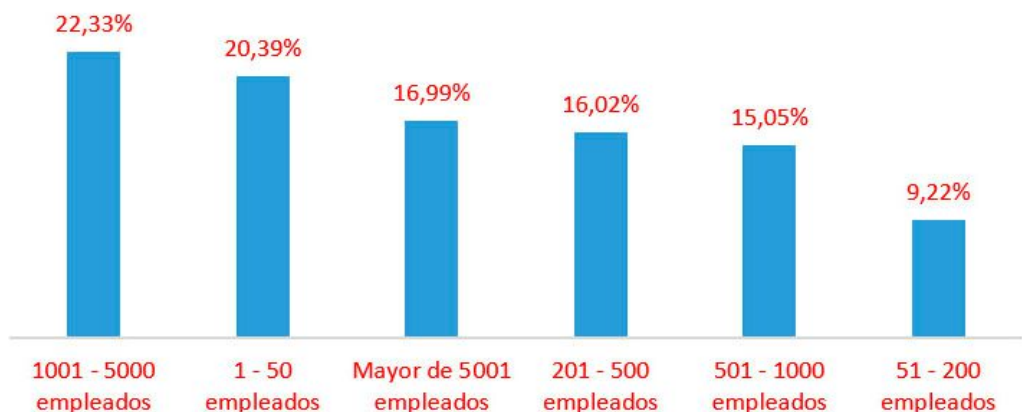
En la categoría de otros se encuentran a un variado universo de profesionales, entre otras están docentes universitarios, ingenieros del sector de la industria de TI, y algunos otros profesionales de ciber-

seguridad que no se identifican con las categorías de cargos que contiene la encuesta. Es importante considerar que existe una gran gama de roles que responden la encuesta y dan sus distintas visiones

**Figura 2**

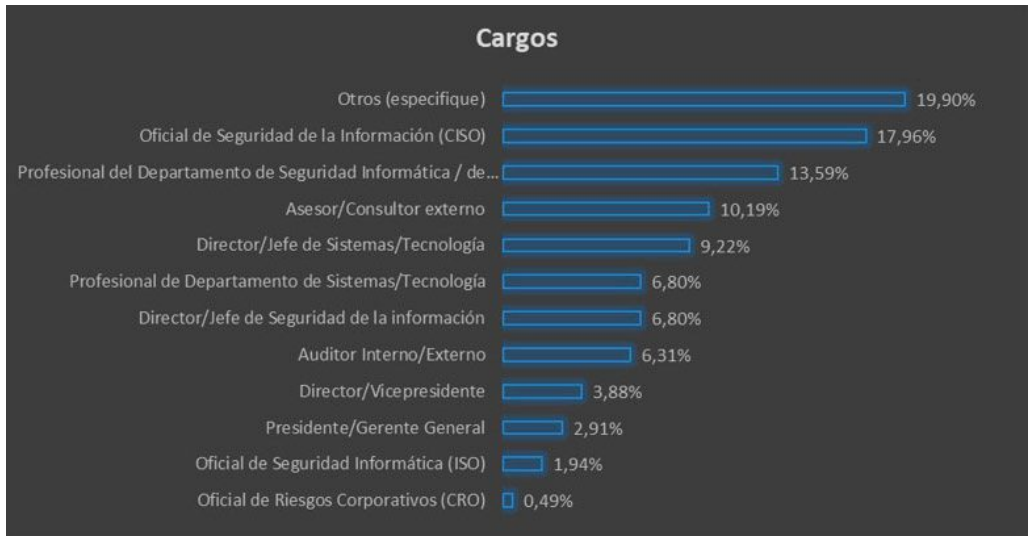
Tamaño de las empresas participantes.

Tamaño de las empresas



**Figura 3**

Cargos de los encuestados



acerca de lo que representa la ciberseguridad en sus organizaciones.

La Figura 4, se observan las tareas realizadas por los profesionales de seguridad dentro de las organizaciones. Para este año, el porcentaje más alto está representado por definir controles de TI en materia de seguridad 67%, seguido de establecer e implementar un modelo de políticas 61% y en tercer lugar la creación de programas de entrenamiento en materia de seguridad 57%.

La Figura 5, muestra de quién depende el área de seguridad. Los datos indican que el área de seguridad depende de una dirección propia, Director/Jefe de Seguridad de la Información 31%, seguido por la Vicepresidencia/Director Depar-

tamento de Tecnologías de la Información 18% y en tercer lugar del Director/Jefe de Seguridad Informática 12%.

La Figura 6, observan los roles dentro de una organización en materia de seguridad digital. El rol de analista de seguridad de la información es el rol más común que año tras año se manifiesta con un 58%, seguido de la posición CISO u Oficial de Seguridad de la Información 50% y analista de seguridad informática con un 41%.

**Consideraciones de los datos**

Según las reuniones sostenidas en la agenda global del Foro Económico Mundial en Davos del 2022, en la reunión dentro del foro “Global CyberSecurity Outlook” (WEF, 2022), en el panel se ha expresado



**Figura 4**

**Funciones del responsable de seguridad**



**Figura 5**

**Dependencia del área de Seguridad**



**Figura 6**

**Roles de Seguridad**



que no importa el tamaño de las empresas, todas están expuestas más allá de todos los esfuerzos que se hagan, el adversario digital está al acecho, y se debe adoptar como principio que el ataque va a suceder, desarrollar capacidades, desarrollar cooperación, y entender a la ciberseguridad como un desafío de alta complejidad puede ayudar a abordarlo.

Los roles, la responsabilidad y la visibilidad del profesional de ciberseguridad sigue evolucionando, cada vez se nota su presencia de alguna manera en los distintos niveles de la organización (DarkReading, 2022). En este año al revisar los datos, se puede notar como los distintos sectores de la industria en

Colombia tiene la presencia del profesional de seguridad y sus áreas definidas.

Al revisar la distribución de los cargos de los encuestados distribuidos en los sectores de la industria más representativos tenemos que el 22% de los profesionales en todos los sectores son llamados CISOs, siendo el sector financiero 4,24% y el sector de tecnologías de la información 3,64% los que mantienen esa figura. En la misma línea de cargos el 16,97% su cargo es ser profesional del área de seguridad informática o información siendo el sector de las tecnologías de información con un 5,45% el primer lugar y de segundo el sector público con un 3,64%. Al revisar el informe

anual de la Asociación de Control y Auditoría (ISACA) llamado “*State of Cybersecurity 2022*” (ISACA, 2022) se ratifica la tendencia de participación, las industrias o sectores más representativos son la industria de las tecnologías de información 25% y el sector financiero con un 21%. Sectores como el de salud, telecomunicaciones y otros, son sectores que la participación fue realizada por profesionales de las áreas de TI.

En cuanto a los roles y responsabilidades hay una gran variación de lo que hacen los profesionales de

seguridad en los distintos sectores de la industria, de tal manera que al revisar el top 3 de funciones o responsabilidades de los principales sectores de la industria se pueden evidenciar en la Tabla 1, en la cual se tiene.

El sector de las tecnologías de la información sus tareas principales están centradas en Definir el programa de privacidad de la información (32%) y la implementación del programa de protección de datos (31%) con el mismo valor revisar la arquitectura de seguridad de la información (31%). El sector finan-

## Tabla

Distribución de responsabilidades por sectores

Valores	Tecnologías de Información	Servicios Financieros y Banca	Otro (especifique)	Gobierno / Sector público	Educación	Consultoría Especializada
Aseguramiento de procesos de la organización	29%	19%	16%	11%	12%	13%
Velar por la protección de la información personal	26%	21%	16%	14%	12%	11%
Supervisar y gestionar los procesos de investigaciones forenses digitales	22%	24%	18%	14%	6%	16%
Seguimiento de prácticas en materia de protección de la privacidad de la información personal	29%	14%	20%	14%	10%	14%
Interacción con las diferentes áreas de negocio	28%	23%	17%	10%	12%	10%
Supervisar procesos de cumplimiento regulatorio en tecnología de información	26%	21%	18%	13%	9%	13%
Informar a la alta gerencia sobre el avance del programa de seguridad de la información	28%	27%	13%	14%	9%	11%
Implementación de controles de TI en materia de seguridad de la información	29%	17%	13%	12%	19%	9%
Gestionar el programa de gestión de incidentes de seguridad de la información	23%	19%	13%	17%	16%	12%
Evaluar la eficiencia y efectividad del modelo de seguridad de la información	27%	21%	14%	14%	10%	15%
Seguimiento de prácticas en materia de seguridad de la información	29%	18%	18%	14%	11%	10%
Establecer y revisar la arquitectura de seguridad de la información	31%	16%	15%	14%	11%	13%
Establecer e implementar un modelo de políticas en materia de seguridad de la información	28%	20%	15%	13%	11%	13%
Dirigir y supervisar los programas de riesgos de seguridad de la información de la organización	29%	21%	16%	12%	9%	12%
Definir o diseñar escenarios/simulaciones/Playbooks en relación con ciberriesgos	30%	28%	11%	15%	8%	8%
Definir, implementar y asegurar la estrategia de ciberseguridad de la empresa	27%	21%	15%	13%	11%	14%
Definir programas de resiliencia digital	23%	19%	21%	19%	9%	9%
Definir, implementar y asegurar el programa de protección de datos personales de la empresa	31%	20%	13%	13%	11%	11%
Definir, diseñar y velar por el programa de privacidad de la información de la organización	32%	18%	11%	15%	13%	12%
Definición de controles de TI en materia de seguridad de la información	26%	21%	15%	11%	14%	12%
Creación de programas de entrenamiento en materia de seguridad de la información	27%	21%	16%	12%	12%	13%
Creación de programas de gobierno y gestión en materia de seguridad de la información	27%	19%	16%	11%	11%	16%

ciero por su parte su principal tarea basado en los resultados es el diseño de los playbooks en relación con los Ciberriesgos (28%), informar a la alta gerencia sobre el avance del programa de seguridad (27%) y supervisar los programas de investigaciones forenses digitales (24%). El sector gobierno está enfocado en definir el programa de resiliencia digital (19%), el programa de gestión de incidentes (17%) y el programa de privacidad de la información (15%). El sector de salud está enfocado en la implementación de controles de TI para seguridad (19%), seguido por la gestión de incidentes (16%) y definir controles de TI para seguridad (14%). El sector de la consultoría está centrado en la creación de los programas de gobierno y gestión en materia de seguridad (16%), supervisión de

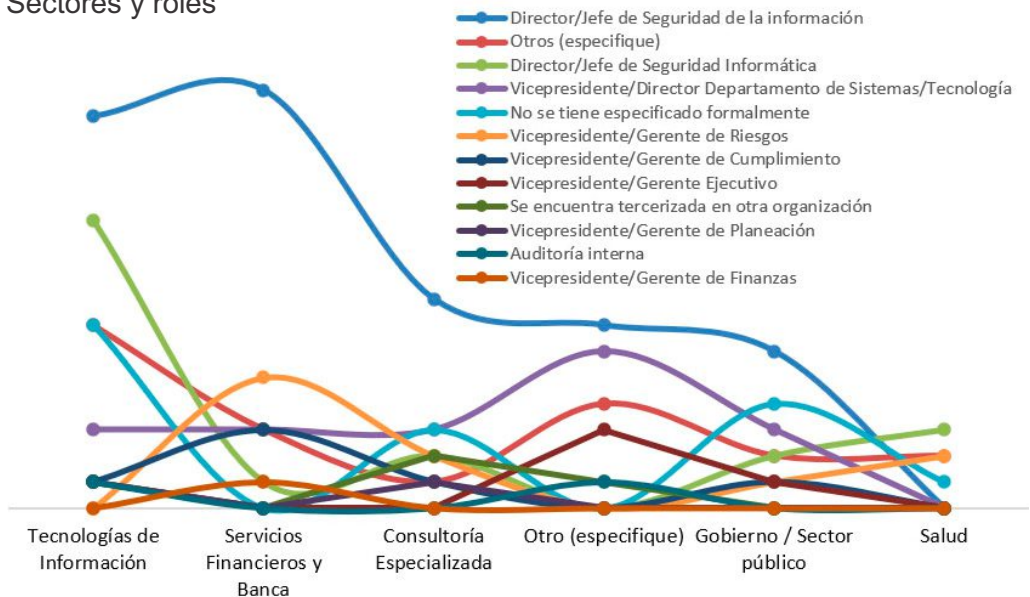
los procesos de investigaciones forenses (16%) y por último evaluar la efectividad y eficiencia del modelo de seguridad (15%).

Lo anterior muestra que cada sector de la industria está enfocando sus esfuerzos de acuerdo con sus niveles de madurez y la forma en como han evolucionado, ejemplo de esta afirmación es el caso del sector salud, que junto con el sector educación han sido los dos sectores que más han sido afectados durante el 2021 como lo mencionan informes de la industria (IBM, 20-22).

Han pasado 2 años desde que el mundo cambió significativamente, el trabajo remoto llegó para quedarse y esa realidad se ha plasmado en la vida de los profesionales

**Figura 7**

Sectores y roles



de seguridad de la información, ciberseguridad y privacidad, que le ha traído nuevos desafíos frente a la protección, la educación y los aprendizajes de la ciberseguridad.

La dependencia de la ciberseguridad en las organizaciones es otro de los elementos claves, en Colombia existen una variedad de representaciones de acuerdo con los sectores de la industria y su madurez. La Figura 7, muestra la distribución de los cargos en los distintos sectores de mayor representación, en primera instancia a excepción del sector Salud, todos los sectores muestran la figura de un director de seguridad como su principal figura, casos como el sector de tecnologías de la información con un 4.58% de representación que no tienen formalmente definido un rol ni una dependencia, el 3.27%

la dependencia de la seguridad está en la figura del gerente de riesgos.

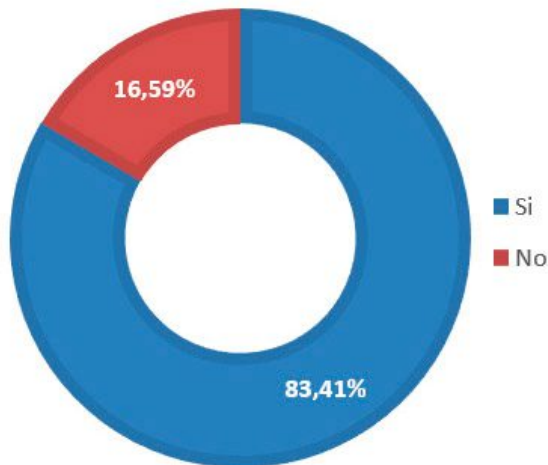
Las organizaciones que tienen la figura o posición de la función de la seguridad dependiendo de un director, muestran grandes avances en el desarrollo de las posturas de seguridad, esto puede ser el piso de apoyo para poder llegar a las instancias directivas y ejecutivas de las organizaciones y por tanto tener mayor visibilidad, en esa misma línea por tanto el rol del profesional líder de seguridad, así como la función debe transformarse (Fortinet, 2022; DarkReading, 2022).

Por tanto, en Colombia los datos para el año 2022 muestran alineación con las tendencias internacionales en relación a cómo la función de seguridad sigue su camino y

**Figura 8**

Presupuesto de Seguridad

### ASIGNACIÓN DE PRESUPUESTO



procesos de aprendizaje, cómo avanza su evolución con mayor énfasis en algunos sectores que en otros, donde cada uno de ellos tiene su propio nivel de aprendizaje. El desafío estará en qué tan rápido se avanza para que los retos en materia de protección digital no tomen más ventaja de la que ya existe.

### Presupuestos

Continúa la asignación de presupuestos para la ciberseguridad; en esta oportunidad el 83% manifiesta tener asignado un presupuesto de seguridad en la organización que se puede ver en La Figura 8.

La Figura 9, muestra el porcentaje que representa el presupuesto para la ciberseguridad del total del presupuesto de la organización.

Cerca del 50% de los encuestados lo conoce, mientras que el otro 50% dice no conocer o no tener la información. De quienes conocen los montos asignados se puede observar que los montos inferiores al 5% del presupuesto global de la compañía representan el 32%, mientras que el 15% están para los montos superiores al 5%. Entre el 0 y 2% representa un 15% mientras que entre 3 y el 5% representa el 16%, 8,6% es más del 11%, 5% está entre el 6 y 8% y entre el 9 y 11% es el 3,7%.

La Figura 10, refleja los montos asignados en las organizaciones para la ciberseguridad. Para este año cerca del 47% tiene un monto asignado para la seguridad; que aumenta, comparado con el año pasado cerca de un 3%, por su parte el 53% dice no conocer

**Figura 9**

Porcentaje del presupuesto Global



**Figura 10**

Presupuesto de Seguridad

### Montos asignados para la ciber-seguridad



cuánto es el presupuesto asignado para la ciber-seguridad. Al revisar los datos, el 17% dice que asigna un presupuesto mayor a \$US 130.000 dólares americanos, seguido de aquellos que asignan menos de \$US 20.000 y que representa casi el 11%, seguido de aquellos que asignan entre \$US 20.000 y \$US 50.000 (9%), casi el

4% asigna entre \$US 90.000 y \$US 110.000.

La Figura 11, muestra la forma cómo se está invirtiendo el dinero en materia de ciberseguridad. Sigue creciendo la inversión en tecnologías de seguridad informática. Renovación de licenciamiento, servicios de monitoreo, capacitación del

**Figura 11**

Inversión de Seguridad



profesional de seguridad y contratación de consultoría y auditoría.

## Consideraciones de los datos

En la Tabla 2, se muestra la distribución de sectores, montos de inversión y tipos de inversiones, de lo que se puede definir lo siguiente. El sector de la consultoría especiali-

zada centra las inversiones en la capacitación del personal de seguridad con inversiones menores de los \$US20.000 como su valor más alto, sin embargo, también tiene algunas inversiones en el rango de los \$US20.000 a los \$US50.000. El segundo frente de inversión es la Adquisición de tecnologías de seguridad informática, que no excede

**Tabla 2**

Distribución de presupuestos

	Menor de USD\$20.000	Más de USD\$130.001	Entre USD\$90.001 y USD\$110.000	Entre USD\$70.001 y USD\$90.000	Entre USD\$50.001 y USD\$70.000	Entre USD\$20.001 y USD\$50.000	Entre USD\$110.001 y USD\$130.000
<b>Consultoría Especializada</b>							
Contratación de servicios de asesoría/consultoría	3,6%	0,0%	0,0%	0,0%	3,6%	3,6%	0,0%
Adquisición e implementación de tecnología de seguridad informática	4,8%	0,0%	0,0%	0,0%	2,4%	4,8%	0,0%
Renovación de licenciamiento y mantenimiento de hardware y software	2,5%	0,0%	0,0%	0,0%	2,5%	2,5%	0,0%
Capacitación/Actualización del personal de seguridad de la información	10,7%	0,0%	0,0%	0,0%	0,0%	3,6%	0,0%
Servicios de monitoreo y gestión de seguridad con terceros	0,0%	0,0%	0,0%	0,0%	2,9%	2,9%	0,0%
<b>Educación</b>							
Contratación de servicios de asesoría/consultoría	0,0%	0,0%	7,1%	0,0%	0,0%	3,6%	3,6%
Adquisición e implementación de tecnología de seguridad informática	2,4%	2,4%	2,4%	0,0%	0,0%	2,4%	2,4%
Renovación de licenciamiento y mantenimiento de hardware y software	5,0%	2,5%	2,5%	0,0%	0,0%	0,0%	2,5%
Capacitación/Actualización del personal de seguridad de la información	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%
Servicios de monitoreo y gestión de seguridad con terceros	0,0%	2,9%	2,9%	0,0%	0,0%	2,9%	2,9%
<b>Gobierno / Sector público</b>							
Contratación de servicios de asesoría/consultoría	3,6%	3,6%	3,6%	3,6%	0,0%	3,6%	0,0%
Adquisición e implementación de tecnología de seguridad informática	0,0%	4,8%	2,4%	2,4%	0,0%	4,8%	0,0%
Renovación de licenciamiento y mantenimiento de hardware y software	2,5%	7,5%	2,5%	2,5%	0,0%	5,0%	0,0%
Capacitación/Actualización del personal de seguridad de la información	0,0%	10,7%	3,6%	0,0%	0,0%	3,6%	0,0%
Servicios de monitoreo y gestión de seguridad con terceros	0,0%	5,7%	2,9%	2,9%	0,0%	0,0%	0,0%
<b>Salud</b>							
Contratación de servicios de asesoría/consultoría	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%
Adquisición e implementación de tecnología de seguridad informática	2,4%	0,0%	0,0%	2,4%	0,0%	0,0%	0,0%
Renovación de licenciamiento y mantenimiento de hardware y software	2,5%	0,0%	0,0%	2,5%	0,0%	0,0%	0,0%
Capacitación/Actualización del personal de seguridad de la información	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%
Servicios de monitoreo y gestión de seguridad con terceros	2,9%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%
<b>Servicios Financieros y Banca</b>							
Contratación de servicios de asesoría/consultoría	3,6%	28,6%	0,0%	3,6%	0,0%	3,6%	3,6%
Adquisición e implementación de tecnología de seguridad informática	0,0%	21,4%	0,0%	0,0%	2,4%	2,4%	2,4%
Renovación de licenciamiento y mantenimiento de hardware y software	0,0%	17,5%	0,0%	2,5%	2,5%	2,5%	2,5%
Capacitación/Actualización del personal de seguridad de la información	0,0%	21,4%	0,0%	0,0%	3,6%	0,0%	3,6%
Servicios de monitoreo y gestión de seguridad con terceros	0,0%	28,6%	0,0%	2,9%	2,9%	0,0%	2,9%
<b>Tecnologías de Información</b>							
Contratación de servicios de asesoría/consultoría	0,0%	7,1%	0,0%	0,0%	0,0%	3,6%	3,6%
Adquisición e implementación de tecnología de seguridad informática	11,9%	9,5%	0,0%	0,0%	2,4%	2,4%	2,4%
Renovación de licenciamiento y mantenimiento de hardware y software	10,0%	10,0%	2,5%	0,0%	2,5%	2,5%	0,0%
Capacitación/Actualización del personal de seguridad de la información	14,3%	14,3%	3,6%	0,0%	3,6%	0,0%	3,6%
Servicios de monitoreo y gestión de seguridad con terceros	11,4%	11,4%	2,9%	0,0%	2,9%	0,0%	2,9%



en todo caso los \$US50.000 dólares americanos.

El sector de la educación tiene un comportamiento distinto, la consultoría es donde hay más concentración de la inversión y sobre todo entre los \$US90.000 y los \$110.000 dólares, otras franjas tienen valores importantes. El segundo frente de inversiones es el de renovación de licenciamiento que su valor mayor de inversión está por debajo de los \$US20.000 dólares americanos, aunque también tiene inversiones por encima de los \$US 130.000.

El sector del gobierno por su parte tiene elementos interesantes para revisar, se concentra en capacitar a las personas de las áreas de seguridad con inversiones por encima de los \$US130.000 dólares, sigue la renovación del licenciamiento y los servicios de monitoreo y gestión de seguridad por terceros en la misma franja de montos asignados.

El sector salud de otro lado asigna menos de \$US20.000 dólares en primera instancia para el monitoreo, y como segundo lugar la renovación de licenciamiento que está en la misma franja, así como también se asignan recursos económicos para este rubro en la franja de los \$US70.000 al \$US90.000 dólares americanos.

El sector financiero, ratifica la tendencia global, se invierte y es el que más invierte todos los elementos

analizados su rango de inversión están por encima de los \$US 130.000, que además se confirma a través de los distintos reportes de industria (Verizon, 2022).

En el sector de las tecnologías de la información se muestra que se está capacitando a las personas dedicadas a la seguridad en dos de los rangos, por un lado, se invierte en la franja menor de \$US20.000, así como en la franja de \$US130.000 dólares americanos, la adquisición de tecnologías es el segundo rubro en importancia donde se hace inversiones, sin embargo, estas están en la franja por debajo de los \$US 20.000 dólares.

Invertir en la ciberseguridad es importante, sin embargo, los datos de Colombia empiezan a mostrar que no solo es necesario, también es bueno empezar a hacer inversiones de manera razonable y que estén acordes con la realidad de las organizaciones (CyberEdge, 2022).

Hoy por hoy en Colombia se confirma que las organizaciones están asignando presupuesto, aun así, sigue siendo algo para observar porque los profesionales de seguridad manifiestan no conocer cuánto es el presupuesto asignado, montos, y sobre todo los valores, esto puede obedecer a que sean presupuestos compartidos con las áreas de tecnologías de la información o el rol del profesional de seguridad que diligencia la encues-

ta no tenga acceso a dicha información.

En Colombia en todos los tamaños de las empresas se invierte en ciberseguridad, está claro que las empresas grandes en el rango de 1000 a 5000 empleados invierten más (22%), sin embargo, las empresas pequeñas de 1 a 50 empleados ocupan el segundo lugar (21%), las empresas de más de 5000 empleados ocupan el tercer lugar (17%), seguido de las empresas de 201 a 500 empleados (16%), luego de 501 a 1000 (15%) y por último las de 51 a 200 empleados (9%). Tendencia que se ratifica a través de informes de industria (CyberEge, 2022).

El porcentaje de asignación de presupuesto con respecto al presupuesto global de la organización si-

gué siendo bajo al revisar las franjas dominantes, que se ratifican como tendencia que se ven en reportes de industria que sugiere que 8 de cada 10 empresas tienen un presupuesto menos del 10% del presupuesto de la organización (DarkReading, 2022).

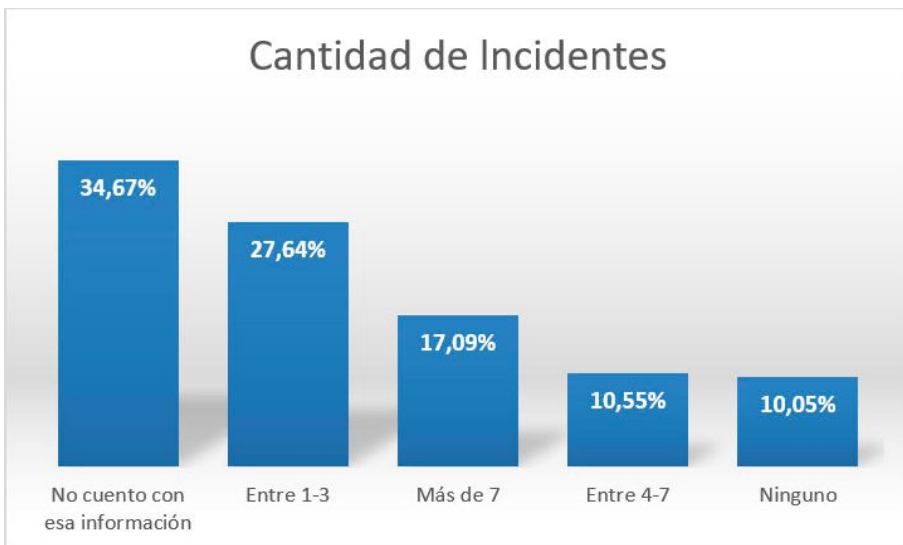
Si bien hoy por hoy es indispensable el presupuesto de seguridad, no es el único factor y en términos generales se ve de manera optimista la asignación del presupuesto para la ciberseguridad (ISACA, 2022). En reportes de industria se reitera esta tendencia, que en Colombia sigue evolucionando y sigue mejorando año tras año.

### Incidentes

La Figura 12, muestra la cantidad de incidentes que se presentan en

**Figura 12**

Cantidad de Incidentes



Colombia, según los participantes. Para este año cerca del 56% de los encuestados manifiesta que ha estado en contacto con algún incidente de seguridad en su empresa, en comparación con el año inmediatamente anterior, donde el 72% lo ha manifestado. El 33% manifiesta no tener información al respecto de los incidentes en sus organizaciones, el 28% manifiesta haber experimentado entre 1 y 3 incidentes, el 17% comenta que ha experimentado más de 7 incidentes, cerca del 11% informa que ha experimentado entre 4 a 7 incidentes, y

solo el 10% señala que no ha experimentado ningún incidente.

La Figura 13, relaciona los tipos de incidentes que se presentaron en las organizaciones, Errores humanos (38%), Phishing (32%) y los ataques de ingeniería social (25%) son las tres primeras posiciones del listado.

La figura 14, representa el costo promedio de los incidentes, el 87% manifiesta que los costos estimados totales luego de sufrir un incidente están por debajo de los

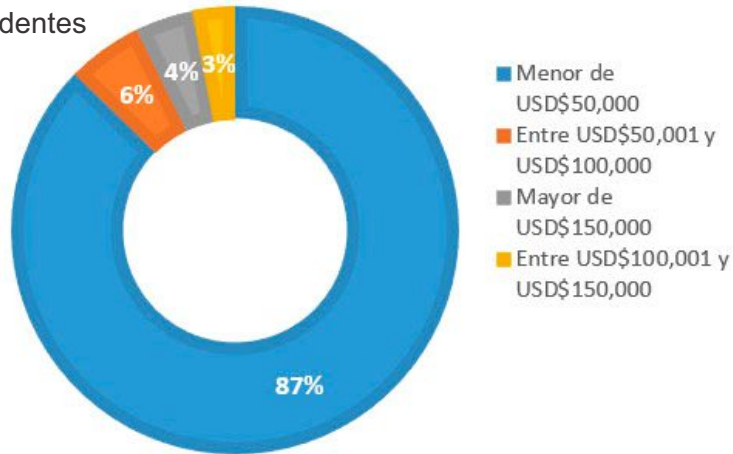
**Figura 13**

Tipos de Incidentes de Seguridad



**Figura 14**

Costos de los Incidentes



\$US50.000 dólares americanos, entre \$US50.000 y \$US100.000 solo el 6%, más de \$US150.000 el 4% y entre \$US100.000 y \$US-150.000 dólares americanos el 3%.

La Figura 15, muestra ante quién se reportan los incidentes de seguridad.

El 61% lo reporta directamente a los directivos de la organización, el 47% lo reporta al equipo de atención de incidentes (CSIRT), el 33% a las autoridades nacionales, el 23% a los asesores legales, el 15% a autoridades locales o regionales y solo el 5% manifiesta que no se denuncia.

**Figura 15**

A quién se reportan los incidentes

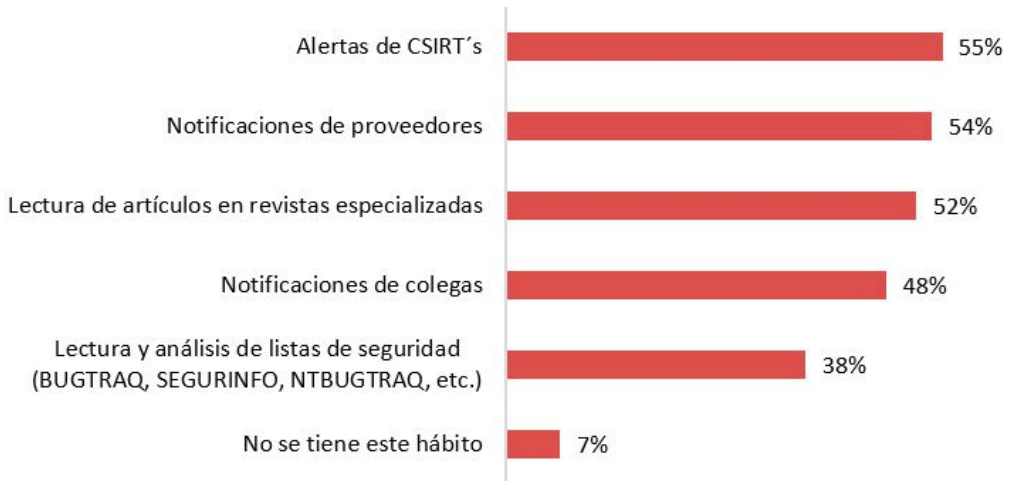
### Notificación de los incidentes



**Figura 16**

Razones para no denunciar los incidentes

### Notificación de las fallas de seguridad



La Figura 16, muestra como los profesionales de ciberseguridad se mantienen informados sobre las vulnerabilidades y fallas de los sistemas. El 55% de los profesionales de seguridad se enteran o están conectados con CSIRTs, el 54% se notifican de su relación con sus proveedores, la lectura de revistas especializadas es la tercera fuente 52%, el 48% se notifica a través de

colegas, el 38% lee listas de seguridad, y solo el 7% no tiene ese hábito.

La Tabla 3, se resalta que el 63% de las personas encuestadas si tienen contacto con las autoridades, mientras que el 37% no lo posee.

En cuanto la evidencia digital, los datos muestran que, 81% de los

**Tabla 3**

Contacto con autoridades

Contacto con autoridades	Porcentaje
No	37,10%
Si	62,90%

Contacto con autoridades	Porcentaje
No	37,10%
Si	62,90%

encuestados si es consciente del manejo de la evidencia digital y que es requerida como parte del proceso de la gestión de incidentes, el 55% no posee un procedimiento formal para la gestión de incidentes, el 44% afirma si tenerlo, solo el 38% ha implementado el procedimiento de gestión de evidencia digital, que dicen tener formalmente definido.

### Consideraciones de los datos

Explorando la forma en como en Colombia los distintos sectores de la industria experimentan los distintos incidentes, y en que invierten sus recursos financieros asignados de presupuesto a los desafíos que presenta la ciber-seguridad, la Tabla 4, resalta la cantidad de incidentes que se presentan en los diferentes sectores de industria y adi-

cional los relaciona por el tamaño de la empresa.

Lo que se puede ver en primera instancia es que, en todos los sectores a excepción del sector financiero, las empresas manifiestan que han podido identificar que sufren de 1 a 3 incidentes, resulta de interés que en el global del sector financiero es ningún incidente el mayor valor.

Llama la atención que el sector salud y el sector educación no solo tienen en la franja de 1 a 3 incidentes, su segundo valor más de 7 para el sector educación y entre 4 y 7 para el sector salud, esto confirma la tendencia global que se ha venido experimentando de ser los sectores hoy más apetecidos en la industria por parte del adversario digital como lo menciona IBM en su informe reciente (IBM,2022).

**Tabla 4**

Distribución de incidentes de seguridad por sectores y tamaños de industria

	Entre 1-3	Más de 7	Ninguno	Entre 4-7
<b>Consultoría Especializada</b>	<b>4,35%</b>	<b>1,74%</b>	<b>3,48%</b>	<b>0,87%</b>
1 - 50 empleados	3,48%	0,87%	2,61%	0,00%
201 - 500 empleados	0,00%	0,00%	0,87%	0,87%
Mayor de 5001 empleados	0,00%	0,87%	0,00%	0,00%
51 - 200 empleados	0,87%	0,00%	0,00%	0,00%
<b>Educación</b>	<b>4,35%</b>	<b>2,61%</b>	<b>1,74%</b>	<b>1,74%</b>
201 - 500 empleados	1,74%	0,00%	0,87%	0,87%
Mayor de 5001 empleados	1,74%	1,74%	0,00%	0,00%

501 - 1000 empleados	0,87%	0,87%	0,00%	0,87%
51 - 200 empleados	0,00%	0,00%	0,87%	0,00%
<b>Gobierno / Sector público</b>	<b>6,09%</b>	<b>2,61%</b>	<b>1,74%</b>	<b>2,61%</b>
1001 - 5000 empleados	2,61%	0,87%	0,00%	1,74%
501 - 1000 empleados	0,87%	0,87%	1,74%	0,00%
Mayor de 5001 empleados	0,87%	0,87%	0,00%	0,87%
201 - 500 empleados	0,87%	0,00%	0,00%	0,00%
51 - 200 empleados	0,87%	0,00%	0,00%	0,00%
<b>Otro (especifique)</b>	<b>9,57%</b>	<b>6,09%</b>	<b>0,00%</b>	<b>0,87%</b>
201 - 500 empleados	1,74%	1,74%	0,00%	0,87%
Mayor de 5001 empleados	1,74%	1,74%	0,00%	0,00%
1001 - 5000 empleados	1,74%	0,87%	0,00%	0,00%
1 - 50 empleados	1,74%	0,87%	0,00%	0,00%
501 - 1000 empleados	2,61%	0,00%	0,00%	0,00%
51 - 200 empleados	0,00%	0,87%	0,00%	0,00%
<b>Salud</b>	<b>1,74%</b>	<b>0,00%</b>	<b>0,00%</b>	<b>1,74%</b>
501 - 1000 empleados	0,87%	0,00%	0,00%	0,87%
51 - 200 empleados	0,00%	0,00%	0,00%	0,87%
1001 - 5000 empleados	0,87%	0,00%	0,00%	0,00%
<b>Servicios Financieros y Banca</b>	<b>2,61%</b>	<b>4,35%</b>	<b>5,22%</b>	<b>2,61%</b>
1001 - 5000 empleados	1,74%	0,87%	1,74%	0,87%
Mayor de 5001 empleados	0,00%	0,87%	1,74%	1,74%
501 - 1000 empleados	0,00%	2,61%	0,00%	0,00%
201 - 500 empleados	0,00%	0,00%	1,74%	0,00%
51 - 200 empleados	0,87%	0,00%	0,00%	0,00%
<b>Tecnologías de Información</b>	<b>13,91%</b>	<b>7,83%</b>	<b>4,35%</b>	<b>5,22%</b>
1 - 50 empleados	6,09%	3,48%	2,61%	0,87%
201 - 500 empleados	4,35%	2,61%	0,00%	1,74%
1001 - 5000 empleados	2,61%	0,87%	0,87%	0,00%
51 - 200 empleados	0,87%	0,00%	0,87%	1,74%
Mayor de 5001 empleados	0,00%	0,87%	0,00%	0,87%

Al explorar por tamaños de las empresas y el comportamiento de este podemos encontrar los siguientes datos.

En las empresas de 1 a 50 empleados, los sectores de consultoría especializada y tecnologías de la información son los que predominan en la franja de 1 a 3 incidentes, sin embargo, el sector de tecnología su segundo reglón son la presencia de más de 7 incidentes, tendencia que se ratifica a través del informe de Verizon y CyberEdge (Verizon, 20-22; CyberEdge, 2022).

En las empresas de 201 a 500 empleados, son los sectores de la educación y de las tecnologías quienes evidencia la presencia mayor de 1 a 3 incidentes en sus ambientes.

En las empresas de 1000 a 5000 empleados, es el sector de las tecnologías de información, gobierno y el sector salud los que manifiestan los valores más altos de presencia de incidentes en la banda de 1 a 3 incidentes.

Las empresas de más de 5000 empleados, es el sector educación quien está en la primera posición al manifestar la presencia de incidentes de seguridad en sus ambientes operacionales.

Para las empresas de 500 a 1000 empleados, es donde el sector financiero manifiesta que ha experimentado más de 7 incidentes en sus ambientes operacionales.

Por último, en la banda de las 50 a 200 empleados, es el sector de las tecnologías de la información el que ha experimentado incidentes entre 4 a 7 incidentes en sus infraestructuras tecnológicas.

Todos los datos apuntan a sostener la idea que el adversario está atento a todos los sectores, tamaños de la industria. Se observa según los datos que el sector financiero no es el primer sector objetivo por el adversario, explicado por la madurez del sector que entiende el adversario y que prefiere atacar a otros sectores como el de salud, educación, tecnologías inclusive o gobierno como primeras líneas (CyberEdge, 2022; Fireeye, 2022).

En relación con la forma en como los distintos eventos se presentan en las empresas colombianas se puede visualizar en la Tabla 5.

Errores humanos, Phishing y Ataques de Ingeniería Social, son marcados incidentes que suceden en todos los sectores de la industria, sin embargo, en el sector financiero donde los errores humanos no ocupan el primer lugar, lo ocupa el Phishing que es un flagelo que se mantiene como tendencia significativamente importante (Barracuda, 20-22; Zscaler, 2022).

Los errores humanos son un desafío de las empresas, no solo porque se requiere el entrenamiento de las personas de manera permanente y consistente, adicional porque es un



**Tabla 5**

Distribución de los incidentes de seguridad en los sectores de la industria

Valores	Sectores													
	Alimentos	Construcción / Ingeniería	Consultoría Especializada	Educación	Fuerzas Armadas	Gobierno / Sector público	Manufactura	Otro (especifique)	Retail / Consumo masivo	Salud	Sector de Energía e Hidrocarburos	Servicios Financieros y Banca	Tecnologías de Información	Telecomunicaciones
Ninguno	0%	20%	5%	2%	6%	2%	0%	0%	0%	6%	0%	5%	2%	13%
Accesos no autorizados al web	6%	20%	6%	9%	11%	9%	7%	4%	0%	6%	0%	4%	9%	0%
Otro: Especifique	0%	0%	2%	0%	0%	2%	0%	1%	0%	0%	0%	0%	1%	0%
Virus/Caballos de Troya	0%	20%	2%	2%	11%	7%	7%	9%	0%	6%	0%	4%	8%	0%
Robo de elementos críticos de hardware (notebooks, discos, etc.)	0%	0%	3%	4%	6%	0%	4%	1%	20%	0%	17%	0%	1%	0%
Robo de datos	0%	0%	3%	2%	6%	0%	4%	1%	0%	0%	0%	0%	1%	0%
Ransomware	0%	0%	2%	9%	6%	5%	7%	4%	0%	12%	0%	0%	6%	7%
Pharming	6%	0%	3%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	7%
Phishing	6%	0%	14%	19%	6%	10%	11%	13%	20%	6%	33%	15%	10%	20%
Pérdida/Fuga de información crítica	6%	0%	2%	4%	0%	2%	11%	1%	0%	6%	0%	4%	2%	0%
Suplantación de identidad	0%	0%	2%	0%	6%	3%	7%	3%	0%	0%	0%	4%	3%	7%
Manipulación de aplicaciones de software	6%	0%	5%	0%	6%	2%	0%	3%	0%	0%	0%	2%	2%	0%
Negación del servicio (DOS/DDoS)	6%	0%	5%	2%	0%	2%	0%	0%	0%	0%	0%	7%	2%	0%
Espionaje	6%	0%	3%	0%	6%	3%	0%	3%	0%	0%	0%	2%	2%	7%
Incidentes relacionados con la privacidad de los datos personales (publicación de información personal, solicitudes de eliminación de datos personales, etc.)	6%	0%	6%	2%	0%	5%	0%	9%	0%	0%	0%	4%	2%	7%
Fraude electrónico	6%	0%	2%	11%	6%	0%	11%	7%	20%	6%	0%	9%	6%	7%
Errores humanos	6%	40%	6%	13%	11%	19%	15%	24%	20%	24%	17%	7%	15%	20%
Ciberataques (APT o ataques dirigidos, denegación de servicios masiva)	6%	0%	6%	2%	6%	5%	0%	4%	0%	6%	0%	5%	6%	0%
Brecha de seguridad provocada por terceras partes (p.e Cloud Access Security Broker)	6%	0%	5%	0%	0%	2%	0%	1%	0%	0%	17%	5%	5%	0%
Ataque de aplicaciones Web (XSS, SQL Injection, Directory Transversal, etc.)	6%	0%	6%	6%	0%	5%	4%	3%	0%	6%	0%	11%	7%	0%
Acciones de ingeniería social	6%	0%	8%	13%	11%	16%	11%	7%	20%	6%	17%	11%	8%	7%
Monitoreo no autorizado del tráfico	6%	0%	2%	0%	0%	0%	0%	0%	0%	0%	0%	0%	2%	0%
Pérdida de integridad de la información	6%	0%	3%	0%	0%	2%	0%	0%	0%	12%	0%	2%	1%	0%

frente que el adversario ha entendido que puede ser un vector que se expande y permite diseminar otras formas de ataques, ejemplo Ransomware, Phishing, ataques de cadena de suministro, distribución de malware, creación de personas como *insiders*, entre otros (Proofpoint, 2022; FS-ISAC, 2022).

Datos interesantes, el sector de manufactura relaciona la pérdida/fuga de información y el fraude electrónico son su segunda fuente de incidentes de seguridad, el sector de hidrocarburos y energía ve al robo de elementos críticos, y las brechas de terceras partes como fuentes importantes de incidentes en sus ambientes, en el sector de Tecnologías, así como en otros sectores, el acceso no autorizado a aplicaciones es una fuente importante de presencia de incidentes en las empresas de Colombia, la clara tendencia de que el Ransomware está afectando a sectores de la educación y la salud (TrendMicro, 2022; FBI, 2022; Keeper, 2022).

Los incidentes de manera general los costos totales estimados están por debajo de los \$US50.000, tendencia que se aleja de los informes de industria como el de IBM (IBM, 2022), hay puntos que se resaltan sobre los incidentes y sus costos, por ejemplo el robo de datos, y el Pharming estuvieron en la franja de los \$US50.000 a \$US100.000, por encima de los \$US150.000 robo de datos, Pharming, Denegación de

servicio, pérdida o fuga de información crítica, ransomware, robo de elementos críticos y suplantación de identidad, caso que si se adhiere a la tendencia global en relación con el costos del Ransomware y las Denegaciones de servicio, que son los incidentes con costos muy elevados.

La fortaleza de un proceso de gestión de incidentes no solo radica en tener herramientas o personas, es importante la evidencia digital como fundamento, por tanto, manejar, gestionar, e implementar los procesos relacionados con este componente. La tendencia se confirma a través del informe de CyberEdge Group, que manifiesta que el 13% de los encuestados no considera usar alguna solución de esta naturaleza, el resto o ya las tiene en uso, o planea usarlas (CyberEdge, 2022).

## Herramientas

La Figura 17, muestra el comportamiento de la práctica de la frecuencia con que se evalúa la postura de seguridad en la organización. El 36% manifiesta que se hace una vez al año, el 32% afirma que la hace entre 2 y 4 veces al año, más de 4 veces al año lo relaciona el 19% y ninguna evaluación 13%.

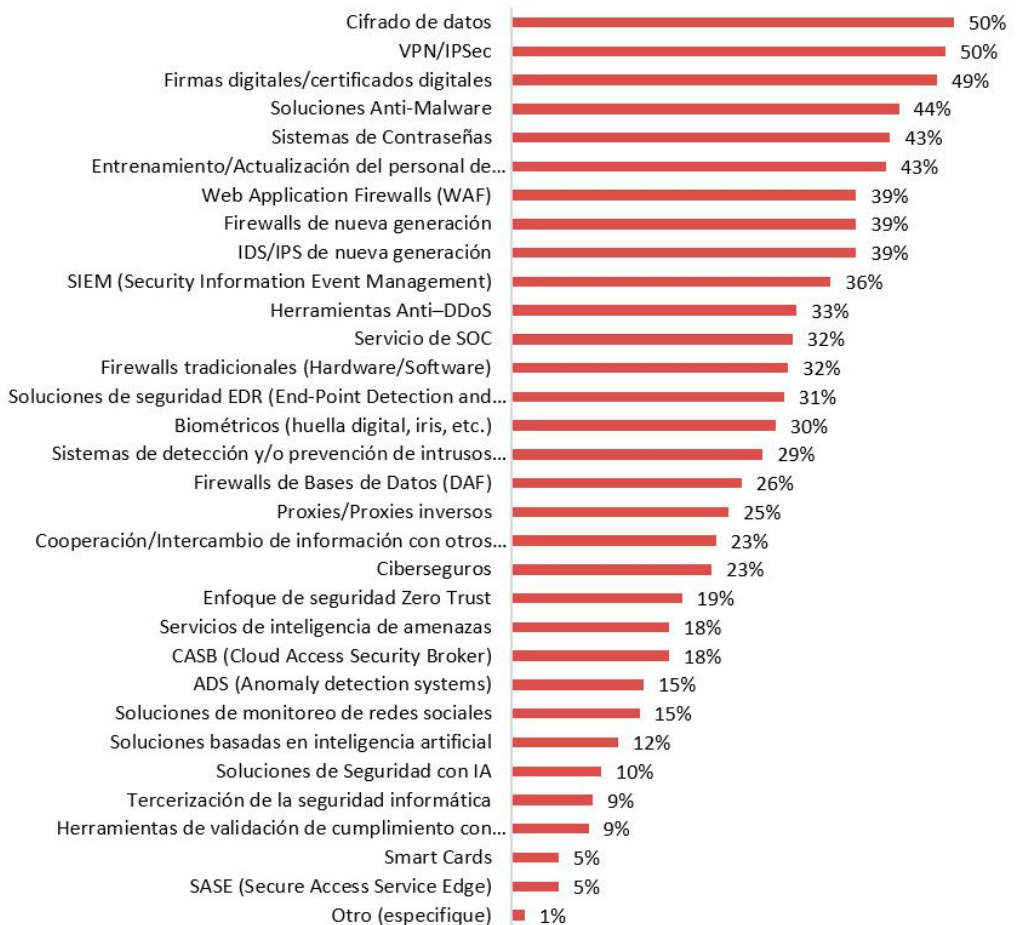
La Figura 18, muestra la distribución del uso de las herramientas de seguridad, Cifrado de datos y VPN son las herramientas primariamente usadas con el 50% ambas,

Figura 17



Figura 18

### Herramientas de Seguridad



siguen las firmas digitales, soluciones antimalware y los sistemas de contraseña.

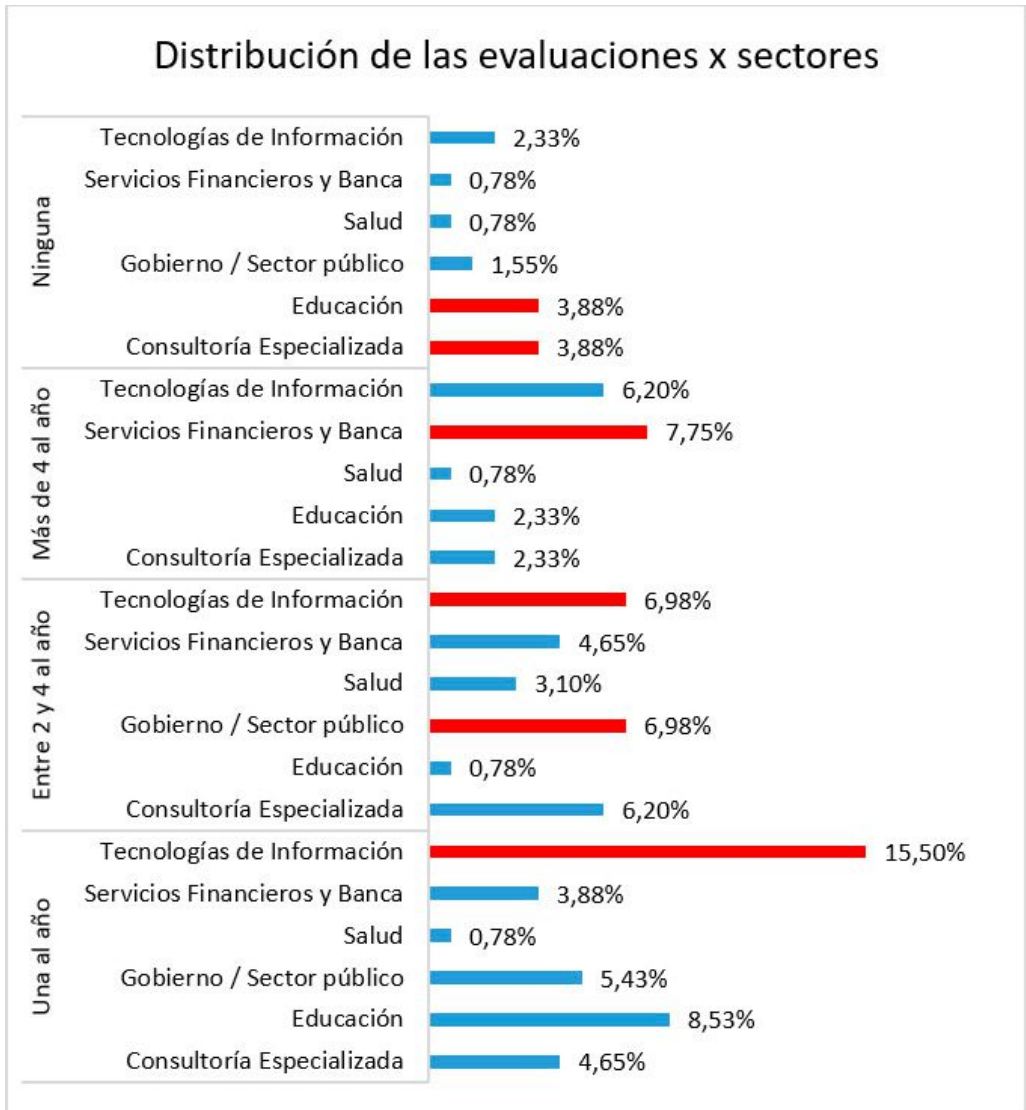
### Consideraciones de los datos

Al revisar los datos y ver como los distintos sectores de la industria

realizan la valoración de la postura de seguridad, está reflejado en la Figura 19, que muestra, los sectores de la educación y la consultoría especializada como valor más importante resalta que no ejecuta ninguna valoración de la postura de seguridad, el sector financiero eje-

**Figura 19**

Sectores y Evaluaciones de seguridad



cuta más de 4 evaluaciones de seguridad por año, entre 2 y 4 evaluaciones al año el sector de tecnología y gobierno, el sector de tecnología lo hace 1 vez al año.

La industria de manera general resalta la necesidad de realizar los procesos de valoración de la postura de seguridad como mecanismo de dirección y revisión de los trazos y visos definidos a través de las distintas estrategias de seguridad de las empresas.

La medición en términos generales depende mucho de la madurez de las empresas y de sus relaciones con la ciberseguridad, el sector financiero a través de muchos esfuerzos propios y también por las presiones de la regulación, los adversarios y las partes interesados aportan para que estos ejercicios se realicen. Otros sectores como el sector de salud, educación, empiezan a consolidar las valoraciones como ejercicios necesarios e indispensables, que con el paso de los años y de acuerdo con las tendencias internacionales seguirá apuntando a crecer.

Al revisar la forma en como los mecanismos y herramientas de seguridad son usados en los distintos sectores de la industria se visualiza en la Tabla 6. El sector de la consultoría especializada ve a las soluciones de seguridad con IA, las Smart cards y las soluciones basadas en IA, como los principales mecanismos. El sector salud, ve en las

Smart cards, los sistemas de detección de anomalías y los proxis los mecanismos más usados. El sector del gobierno ve en las herramientas de validación de cumplimiento con regulaciones internacionales, las firmas digitales y la cooperación e intercambio de información son sus principales mecanismos. El sector de la salud usa la tercerización, las herramientas de validación del cumplimiento y los firewalls de bases de datos como los primeros mecanismos a ser usados. El sector financiero deja claro que el monitoreo de las redes sociales, el cifrado de datos y las soluciones SASE (*Secure Access Service Edge*) ocupan los primeros lugares. El sector de las tecnologías ve en las soluciones SASE, las contraseñas y las herramientas sus principales mecanismos de uso.

En el estudio de IBM (IBM, 2022), se resalta que las empresas están tendiendo a usar herramientas de automatización para la seguridad, tales como herramientas de inteligencia artificial y máquinas de aprendizaje, movimiento que también se ve como tendencia de Colombia.

El incremento en soluciones de seguridad orientadas a la red como IDS/IPS, Firewall de nueva generación, soluciones de Data Loss Prevention (DLP), están en los principales rubros de inversión.

En relación con la protección de estaciones de trabajo el mismo infor-

**Tabla 6**

Distribución de las herramientas de seguridad usadas en los sectores de industria

Valores	Consultoría Especializada	Educación	Gobierno / Sector público	Salud	Servicios Financieros y Banca	Tecnologías de Información
Sistemas de Contraseñas	10,14%	13,04%	13,04%	5,80%	21,74%	36,23%
VPN/IPSec	11,54%	14,10%	17,95%	6,41%	24,36%	25,64%
Web Application Firewalls (WAF)	7,81%	10,94%	21,88%	4,69%	29,69%	25,00%
Tercerización de la seguridad informática	18,18%	18,18%	0,00%	18,18%	36,36%	9,09%
Soluciones de Seguridad con IA	26,67%	6,67%	6,67%	0,00%	26,67%	33,33%
Soluciones de seguridad EDR (End-Point Detection and Response)	15,22%	17,39%	6,52%	2,17%	26,09%	32,61%
Soluciones de monitoreo de redes sociales	4,76%	14,29%	9,52%	4,76%	52,38%	14,29%
Soluciones basadas en inteligencia artificial	23,53%	5,88%	17,65%	0,00%	29,41%	23,53%
Soluciones Anti-Malware	9,86%	12,68%	19,72%	2,82%	21,13%	33,80%
Smart Cards	25,00%	25,00%	12,50%	0,00%	25,00%	12,50%
Sistemas de detección y/o prevención de intrusos						
IDS/IPS tradicionales	12,77%	12,77%	10,64%	0,00%	31,91%	31,91%
Firewalls de nueva generación	14,06%	12,50%	17,19%	3,13%	23,44%	29,69%
SIEM (Security Information Event Management)	12,07%	8,62%	20,69%	3,45%	25,86%	29,31%
Servicios de inteligencia de amenazas	15,38%	3,85%	19,23%	0,00%	30,77%	30,77%
Servicio de SOC	16,33%	8,16%	20,41%	0,00%	36,73%	18,37%
SASE (Secure Access Service Edge)	12,50%	0,00%	0,00%	0,00%	37,50%	50,00%
Proxies/Proxies inversos	7,69%	20,51%	17,95%	2,56%	23,08%	28,21%
IDS/IPS de nueva generación	15,63%	14,06%	15,63%	3,13%	23,44%	28,13%
Herramientas de validación de cumplimiento con regulaciones internacionales	7,69%	0,00%	23,08%	7,69%	30,77%	30,77%
Herramientas Anti-DDoS	12,73%	12,73%	10,91%	1,82%	27,27%	34,55%
Firmas digitales/certificados digitales	13,92%	8,86%	22,78%	3,80%	24,05%	26,58%
Firewalls tradicionales (Hardware/Software)	8,00%	18,00%	18,00%	6,00%	18,00%	32,00%
Firewalls de Bases de Datos (DAF)	21,43%	4,76%	19,05%	7,14%	16,67%	30,95%
ADS (Anomaly detection systems)	18,18%	22,73%	9,09%	0,00%	27,27%	22,73%
Enfoque de seguridad Zero Trust	23,33%	6,67%	6,67%	3,33%	26,67%	33,33%
Cooperación/Intercambio de información con otros (estado, proveedores, aliados, sectores, pares)	11,11%	13,89%	22,22%	2,78%	27,78%	22,22%
Entrenamiento/Actualización del personal de seguridad/ciberseguridad	21,43%	8,57%	8,57%	4,29%	24,29%	32,86%
Cifrado de datos	17,65%	8,24%	14,12%	2,35%	23,53%	34,12%
Ciberseguros	8,82%	17,65%	5,88%	0,00%	41,18%	26,47%
CASB (Cloud Access Security Broker)	20,00%	10,00%	10,00%	0,00%	26,67%	33,33%
Biométricos (huella digital, iris, etc.)	18,00%	14,00%	16,00%	0,00%	22,00%	30,00%

me resalta que las soluciones *anti-malware*, cifrado de discos, antivirus avanzados basados en inteligencia artificial también están considerados.

ción de APIs son los controles que más se están usando y se tiene proyectado utilizar.

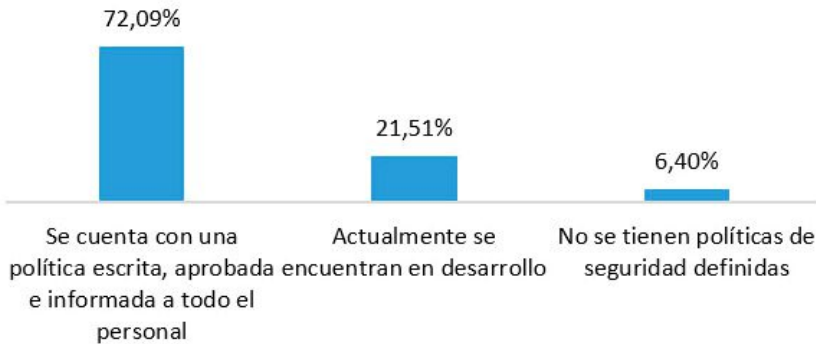
### Políticas

En cuanto a la protección de la capa de aplicaciones, los *Firewalls Web*, de bases de datos la protec-

La Figura 20, refleja el estado de las políticas de seguridad en las organizaciones colombianas, el 72%

**Figura 20**

Estado de las Políticas



**Figura 21**

Obstáculos de la seguridad



de los encuestados manifiesta que tienen formalizada sus políticas de seguridad, el 22% actualmente en desarrollo y solo el 7% señala no tener políticas de seguridad de la información.

La Figura 21, resalta cuales son los obstáculos para tener una postura de seguridad en las organizaciones, en primer lugar, la falta de cultura o ausencia de esta con un 44%, la falta de colaboración entre áreas y departamentos 27%, falta de tiempo es el tercer lugar 26%.

La Figura 22, refleja el nivel de consciencia de los directivos en materia de seguridad, encontrando que, la alta dirección entiende participa y toma decisiones relacionadas con la seguridad de la información en 42%, la dirección entiende y atiende las recomendaciones en materia de seguridad de la información 28%,

la dirección entiende y atiende recomendaciones en materia de seguridad, el 18% considera que la dirección poco se involucra en el tema, y el 10% manifiesta que la alta dirección solo delega y espera avances e informes.

La gestión de riesgos de seguridad es un elemento esencial, en esa línea el 78% de los encuestados tiene un proceso de gestión de riesgos y solo 22% no lo posee.

En la Figura 23, que resalta cada cuanto son ejecutados dichos ejercicios, el 50% manifiesta que al menos la ejecuta 1 vez al año, el 27% más de dos y solo dos el 23%.

Dentro de las personas que contestaron que no lo hacen, al indagar en las razones de por qué no es realizada la gestión de riesgos. El primer motivo que resaltan los partici-

**Figura 22**

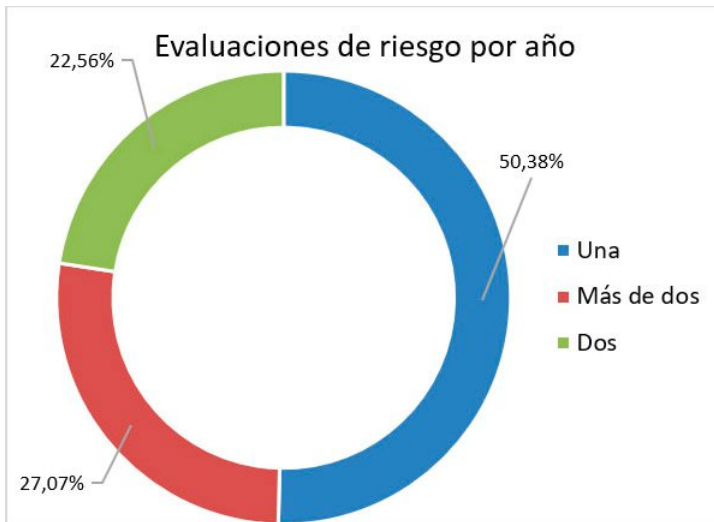
Consciencia de los directivos





**Figura 23**

Evaluaciones de Riesgos



pantes está relacionado con no tener un proceso formal de gestión de riesgos (37%), seguido de que ya está incluido en el proceso de gestión de riesgo empresarial 24%, el desconocimiento del tema 11% es el tercer lugar, la falta de presu-

puesto el 4 lugar con 11% y por último el no tener asociados riesgos con el tratamiento de la información 11%.

La Tabla 7, muestra las metodologías de gestión de riesgos usadas

**Tabla 7**

Uso de metodologías de gestión de riesgos

Metodología de Gestión de Riesgos	Porcentaje
ISO 27005	43%
ISO 31000	36%
SARO	14%
GRC ( Governance, Risk & Compliance)	13%
No se cuenta con metodología	12%
Magerit	7%
ERM(Enterprise Risk Management)	7%
Otra (especifique)2	4%
Octave	1%
AS/NZ 4360	1%
Otra (especifique)	0%

por los participantes del estudio. En primer lugar, está ISO 27005 como la más usada con el 43%, seguido de ISO 31000 36%, SARO 14%, como las tres primeramente usadas, llama la atención que comparado con el año inmediatamente anterior hay un cambio significativo en el uso de ISO 31000 frente a ISO 27005.

La Figura 24, muestra la forma en como las organizaciones hacen las asociaciones entre incidentes de seguridad y el riesgo. El 67% asocia los incidentes de seguridad con riesgos de ciberseguridad, el 58% los asocia con riesgos operacionales, el 43% los asocia con riesgos reputacionales, el 40% con riesgos legales, el 37% con riesgos económicos, el 30% los asocia a riesgos transversales y otros solo es usado con el 1% de las veces.

La Tabla 8, muestra la distribución del uso de los distintos marcos de trabajo (*frameworks*) aplicados en

las organizaciones colombianas: ISO/IEC 27001, NIST, ITIL y COBIT son los más usados. Disminuye contra el año anterior el no usar ningún marco de buenas prácticas.

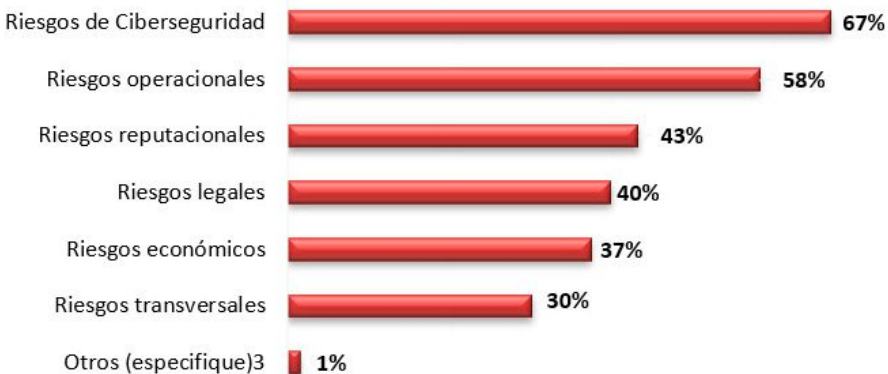
En cuanto a las regulaciones que las organizaciones deben cumplir, el caso colombiano menciona que, el 60% de los participantes manifiesta que sí existen regulaciones que son aplicables a sus modelos de negocio, el 25% considera que no está sujeto a cumplir ningún marco regulatorio o normativos, el 12% debe cumplir con marcos regulatorios internacionales y solo el 4% menciona a otros elementos de regulación.

### Consideraciones de los datos

Los riesgos de seguridad de la información y ciberseguridad en definitiva son una realidad como lo es ratificado en el informe del Foro Económico Mundial (WEF, 2022), el cual manifiesta que la prioridad

**Figura 24**

Tipos de Riesgos



**Tabla 8**

Uso de marcos de trabajo de ciber-seguridad

Marco de referencia	Porcentaje
ISO 27001	69%
Guías del NIST (National Institute of Standards and Technology) USA	37%
ITIL	26%
COBIT	20%
PCI-DSS	17%
Ninguna	6%
Guías de la ENISA (European Network of Information Security Agency)	6%
ISM3 - Information Security Management Maturity Model	3%

de estos tipos de ataques es alta en las organizaciones del mundo.

Al revisar como las juntas directivas en los distintos sectores de la industria están involucradas con los temas de la ciberseguridad, tenemos elementos interesantes a considerar a través de la Figura 25.

Las juntas directivas que se involucran y toman decisiones en el mundo de la ciberseguridad, primeramente, están en el sector de las tecnologías de la información, y en el sector financiero. Al revisar con aquellos cuerpos directivos que entienden y reciben recomendaciones, pero no toman decisiones, el sector de la educación ocupa el primer lugar, seguido del sector financiero y el de las tecnologías de la información. Al ver aquellos cuerpos ejecutivos que poco o nada se involucran tenemos al sector del gobier-

no como el primero en la lista y al sector de la educación en segundo lugar. Para aquellos equipos directivos que solo delegan y esperan resultados, se tiene que el sector de la educación y las tecnologías de la información ocupan los primeros lugares.

Esto resalta la idea de que la madurez de las organizaciones se ve reflejada desde la posición que decide asumir la dirección en relación con la ciberseguridad, cuando los líderes de riesgo y de seguridad vuelven a la seguridad un asunto de los negocios, se crea un compromiso en la dirección y cuerpos directivos no solo se involucran en ellos (Accenture, 2020).

Es claro que existen obstáculos para que la postura de seguridad de una organización se de en los ambientes organizacionales, la postu-

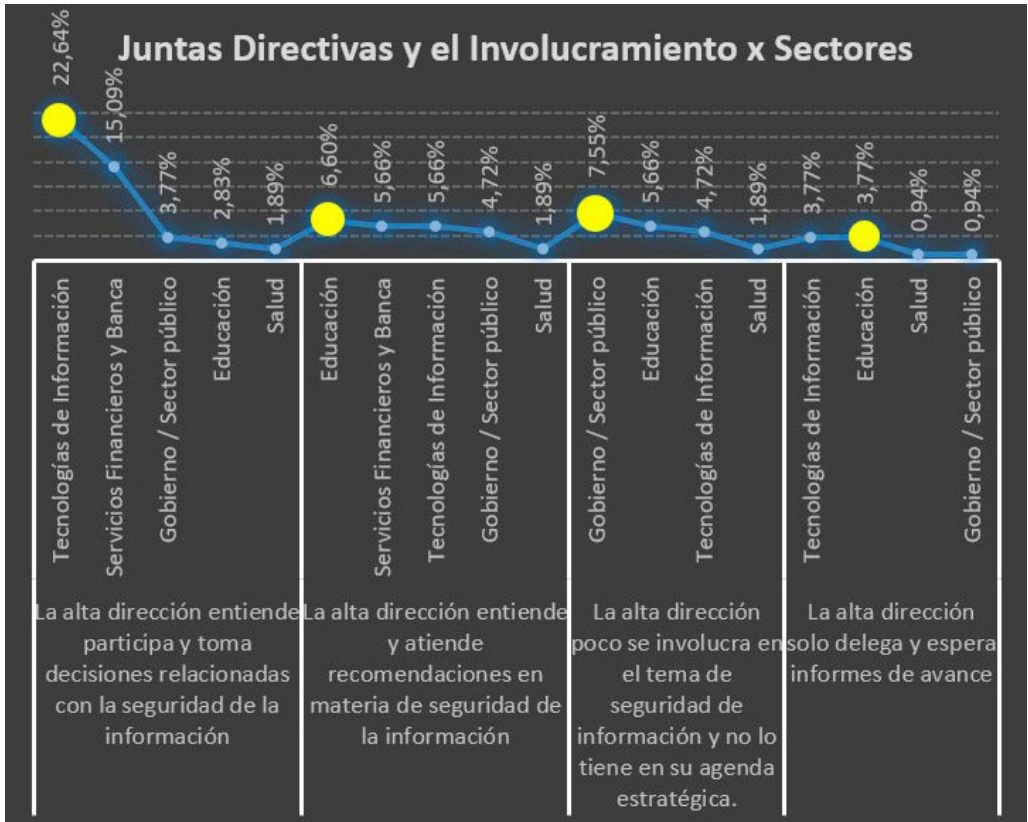
ra de ciberseguridad tiene muchos componentes que deben trabajar de manera unida, alineados a una gran estrategia basada en la gestión de los ciberriesgos, de tal manera que alimente el trabajo colaborativo y cooperativo (Marsh, 20-22).

En la realidad de Colombia la Tabla 9, expresa cuales son los obstáculos más representativos que los distintos sectores de la industria ha experimentado. En el sector de Educación vemos a la falta de formación técnica, la poca visibilidad a

nivel ejecutivo y la escasa formación en gestión segura de la información los primeros tres obstáculos, por su parte en el sector del gobierno la poca visibilidad en el sector en el nivel ejecutivo, el poco entendimiento de los flujos de la información en la organización, y otros factores. En el sector salud está la escasa formación en gestión segura de la información, las limitaciones de las habilidades gerenciales y capacidades de liderazgo de los cisos y la complejidad tecnológica son los primeros obstáculos relacionados. El sector finan-

**Figura 25**

Juntas directivas por sectores



**Tabla 9**

Obstáculos de la ciberseguridad por sectores

Obstáculos para la ciberseguridad	Educación	Gobierno / Sector público	Salud	Servicios Financieros y Banca	Tecnologías de Información
Ausencia o falta de una cultura en seguridad de la información	20,31%	20,31%	9,38%	12,50%	37,50%
Otros (especifique)	12,50%	25,00%	0,00%	37,50%	25,00%
No se tienen obstáculos	0,00%	0,00%	0,00%	60,00%	40,00%
Poca visibilidad del tema a nivel ejecutivo	34,62%	26,92%	3,85%	7,69%	26,92%
Poco entendimiento de los flujos de la información en la organización	26,32%	26,32%	10,53%	21,05%	15,79%
Poco entendimiento de la seguridad de la información					
Limitadas habilidades gerenciales y de liderazgo de los CISO's	30,77%	7,69%	15,38%	7,69%	38,46%
Inexistencia de política de seguridad					
Falta de tiempo	27,59%	20,69%	6,90%	17,24%	27,59%
Falta de formación técnica	47,37%	15,79%	5,26%	15,79%	15,79%
Falta de colaboración entre áreas/departamentos	21,88%	25,00%	6,25%	15,63%	31,25%
Escasa formación en gestión segura de la información	34,38%	12,50%	15,63%	6,25%	31,25%
Falta de apoyo directivo	27,59%	24,14%	10,34%	13,79%	24,14%
Complejidad tecnológica	30,43%	13,04%	13,04%	26,09%	17,39%

ciero por su parte señala no tener obstáculos, otros y la complejidad tecnológica como sus primeros desafíos. En el sector de las tecnologías manifiestan no tener obstáculos, seguido de las limitaciones de los cisos en las habilidades de gerencia y las capacidades de liderazgo y en tercer lugar la falta de cultura de ciberseguridad.

Todos los sectores de la industria colombiana no ven o asocian sus incidentes de seguridad de la misma manera, hay una variedad interesante que se ve reflejada en la Figura 25, que resalta cosas interesantes. El sector de las tecnologías de la información relacionan sus incidentes con riesgos de tipo económico como primera alternativa,

mientras que el sector financiero los tiene enmarcados como riesgos de ciberseguridad igual que lo hace el sector educación, interesante pues la madurez del sector de educación comparado con el sector financiero no son iguales pero si manejan la misma forma de hacer visible el desafío de la ciberseguridad. El sector salud asocia sus incidentes de seguridad con riesgos operacionales, mientras que el sector gobierno como primera opción los asocia a riesgos transversales, también interesante pues si bien muestra un avance importante en la relevancia que tiene el riesgo en las entidades del gobierno, la madurez de sus prácticas basado en los datos no es la más avanzada. La consultoría especializada enmarca los incidentes de seguridad y ciberseguridad en los riesgos reputacionales.

Lo cierto de todos los datos es que todos los sectores a su manera resaltan la necesidad de hacer un buen gobierno de seguridad a través del modelamiento de los riesgos y tenerlos presentes como herramientas claves para orientar los esfuerzos de la ciberseguridad es un factor esencial para poder estar

cerrando la brecha frente a un adversario digital que cada vez más tiene presencia, posición, intención, intensidad e impacto (WEF, 2022).

## Capital intelectual

La Tabla 10, relaciona la cantidad de personas que conforman las áreas de seguridad, la primera posición la ocupa las áreas con un tamaño de 1 a 5 personas, seguido de aquellas que son mayores de 15 personas, seguido de las que tienen entre 6 a 10 personas, ninguna persona dedicada en el 4 lugar y por último las que tienen entre 11 a 15 personas.

La Figura 26, representa la comparación de las certificaciones que los profesionales de seguridad han alcanzado en la actualidad y que desean alcanzar en el tiempo. CISM, CISSP, CRISC, CEH y CISA, son las certificaciones que muestran mayor deseo de ser alcanzada al revisar la diferencia frente a quienes las han alcanzado.

La Figura 27, representa que tipo de información entrega el profesional de seguridad en la organiza-

**Tabla 10**

Tamaño de las áreas de seguridad

Tamaño	Porcentaje
1 a 5	61,01%
Más de 15	18,24%
6 a 10	10,69%
Ninguna	5,66%
11 a 15	4,40%

**Figura 26**

Certificaciones alcanzadas vs deseadas



ción. La entrega de información para la toma de acciones, seguido de la entrega de información para la toma de decisiones son las dos principales.

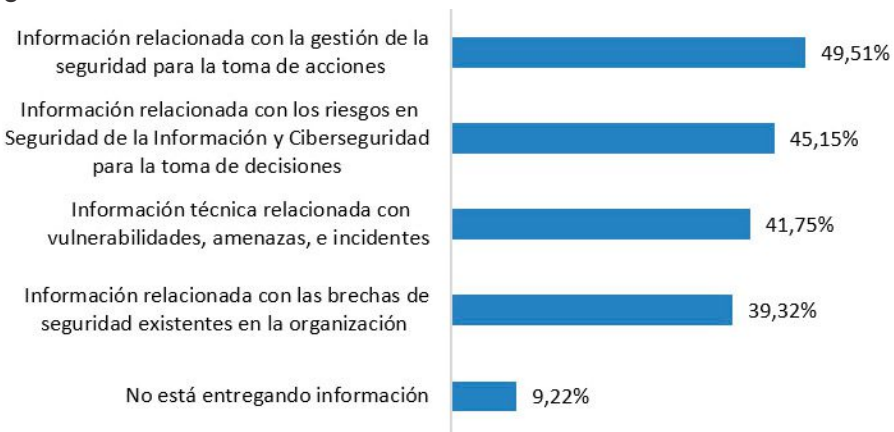
El CISO, es la figura más representativa como cabeza visible para

guiar y orientar la ciberseguridad en las organizaciones. La Figura 28, muestra la forma en que las organizaciones ven o identifican el tipo de CISO que existe en ellas.

Los profesionales de seguridad, especialmente los CISOs tienen

**Figura 27**

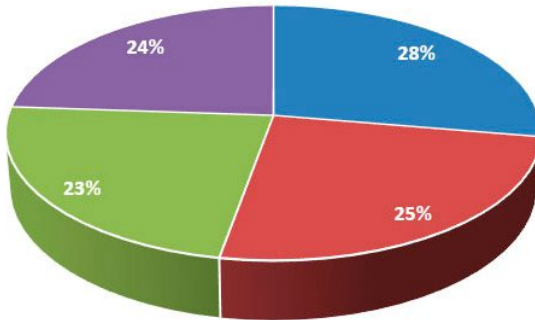
Entrega de información



**Figura 28**

Tipo de CISO

Tipos de CISOs



- CISO como Asesor (Integrado al negocio, educa, influencia, teniendo clara las implicaciones de todo con los ciber riesgos, relaciona nuevas visiones con riesgos emergentes, vela por el desarrollo de capacidades para manejar y enfrentar riesgos en toda la o
- CISO como Estratega (Integra operación, riesgos y negocio, entiende la relación de negocio, activo y operación y vela por ella)
- CISO como Implementador (Vela por la implementación de las tecnologías de protección y su correcto funcionamiento, está pendiente de los detalles de toda la infraestructura de seguridad)
- CISO como Supervisor ( Vela por la eficacia y eficiencia del programa de seguridad, su visión del control es la que rige como principio, Vela por los riesgos, y el cumplimiento)

preferencias para su crecimiento y formación, la Figura 29 representa la forma en como escogen formarse, en primer lugar, están las certificaciones, segundo lugar la educación formal, seguido de las charlas especializadas, los cursos cortos, diplomados y en el último lugar la formación ejecutiva.

De igual manera todo profesional de seguridad tiene oportunidades en las que puede crecer y mejorar, es por esa razón que se revisa cuales pueden ser los puntos de mejora en términos de capacidades, en primer lugar, están las capacidades de liderazgo, seguido de las capacidades de gestión, luego de las capacidades intelectuales, seguido por las humanas, y por último la experiencia profesional, como lo muestra la Figura 30.

### Consideraciones de los datos

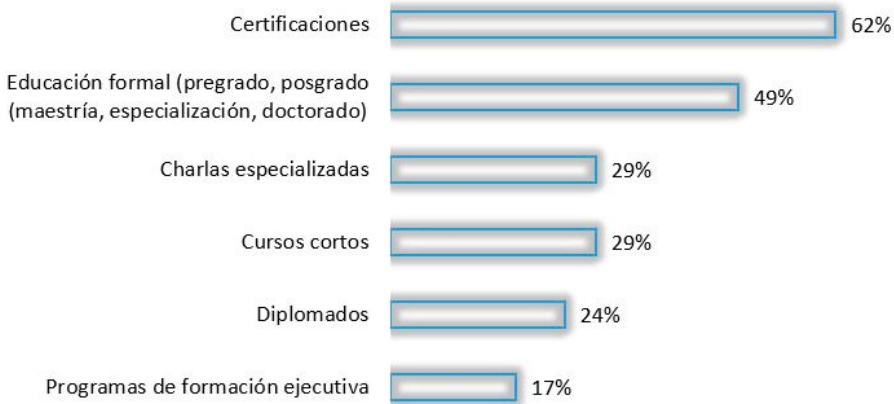
El talento humano en seguridad tiene cada vez más tensiones y presiones que lo han puesto en el centro de muchos análisis y observaciones, muchos profesionales sienten la tensión de los movimientos de la ciberseguridad y dicha tensión hace que el fenómeno llamado gran renuncia producido como efecto colateral de la pandemia los haga considerar salir de sus empresas, pensando más en la tranquilidad y bienestar (Deepinstinct, 2022).

Hay una gran controversia sobre la escasez de talento, mientras unos defienden que no existe talento, otros están defendiendo la tesis que es la escasez de habilidad y conocimiento del profesional de segu-



**Figura 29**

Preferencias de formación



**Figura 30**

Capacidades por mejorar



ridad lo que se debe trabajar, diciendo que talento humano si existe, pero no preparado para enfrentar los nuevos desafíos de la ciberseguridad (ISACA, 2022).

Al revisar los datos para Colombia y ver como se desenvuelven las áreas de seguridad en los sectores de la industria y los tamaños de es-

ta, hay datos muy interesantes, como los expuestos en la Tabla 11. Los datos revelan que en primer lugar la madurez de las empresas del sector financiero que, en ninguna de sus franjas de tamaño de empresa, no tiene reportado que no exista área de seguridad. De hecho, los valores altos y representativos están en las áreas de más de

15 personas, para empresas de más de 1000 empleados. Consultoría especializada, sector salud, sector de las tecnologías y sector educación manifiestan que no tienen ninguna persona para atender los desafíos de seguridad, el sector del gobierno es variado, llama la atención que las empresas de 1000 a 5000, su área de seguridad es de 1 a 5 como su mayor valor, y entre 11 y 15 en una mucho menor proporción. Así mismo el sector manifiesta que sin importar el tamaño de la empresa, no existe organizaciones que no tengan talento de seguridad asignado. Otro dato llamativo es el tema del sector salud su área predominante es la de 1 a 5 personas sin importar el tamaño de la empresa.

El reporte de MarlinHawk (2020) muestra que el promedio de los profesionales estudiados del mundo de la seguridad tiene 4 años en una posición en esta área. Desde el mismo informe resalta que el 94%

de los profesionales de seguridad tienen un grado obtenido en la universidad, que el 84% está relacionado con ciencias de la computación, que cerca del 44% surgen de las áreas de TI.

Los distintos roles que contestan la encuesta tienen distintas preferencias en relación con las certificaciones, lo que si es cierto es que el profesional de seguridad más allá del rol tiene intención de seguir creciendo y formándose en materia de ciberseguridad, precisamente para estar disponible frente a la demanda de trabajo que existe en la actualidad (ISACA, 2022).

Al revisar los datos de Colombia y ver las preferencias más y menos apetecidas en materia de certificaciones por los roles definidos, se encuentran reflejadas en la Figura 31.

En la figura 31 los asesores y consultores muestran no estar intere-

**Tabla 11**

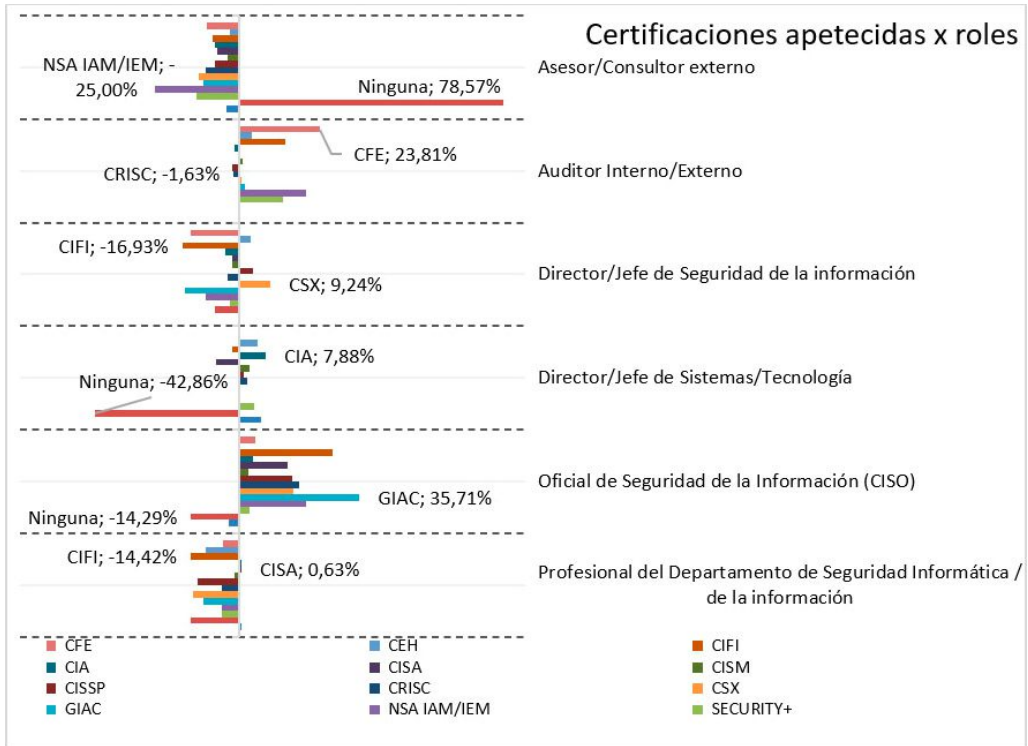
Distribución del tamaño de las áreas de seguridad por sectores y tamaño de empresa

Tamaño del Area/Sector - Tamaño empresa	1 a 5	Más de 15	6 a 10	Ninguna	11 a 15
<b>Tecnologías de Información</b>					
1 - 50 empleados	10,17%	0,00%	0,00%	1,69%	0,00%
201 - 500 empleados	4,24%	0,85%	2,54%	0,00%	0,00%
1001 - 5000 empleados	1,69%	3,39%	0,00%	0,00%	0,00%

51 - 200 empleados	3,39%	0,85%	0,00%	0,00%	0,00%
Mayor de 5001 empleados	0,00%	2,54%	0,00%	0,00%	0,00%
501 - 1000 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
<b>Servicios Financieros y Banca</b>					
1001 - 5000 empleados	0,85%	3,39%	0,85%	0,00%	0,85%
Mayor de 5001 empleados	0,00%	3,39%	0,85%	0,00%	0,00%
201 - 500 empleados	3,39%	0,00%	0,00%	0,00%	0,00%
501 - 1000 empleados	0,85%	0,85%	0,00%	0,00%	0,00%
1 - 50 empleados	0,00%	0,00%	0,85%	0,00%	0,00%
51 - 200 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
<b>Consultoría Especializada</b>					
1 - 50 empleados	7,63%	0,00%	0,85%	0,85%	0,00%
Mayor de 5001 empleados	0,00%	1,69%	0,00%	0,00%	0,00%
1001 - 5000 empleados	0,85%	0,85%	0,00%	0,00%	0,00%
201 - 500 empleados	0,00%	0,00%	0,85%	0,85%	0,00%
501 - 1000 empleados	0,00%	0,85%	0,00%	0,00%	0,00%
51 - 200 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
<b>Educación</b>					
501 - 1000 empleados	1,69%	0,00%	0,85%	1,69%	0,00%
Mayor de 5001 empleados	1,69%	0,85%	0,85%	0,00%	0,00%
1001 - 5000 empleados	2,54%	0,00%	0,85%	0,00%	0,00%
201 - 500 empleados	3,39%	0,00%	0,00%	0,00%	0,00%
1 - 50 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
<b>Gobierno / Sector público</b>					
1001 - 5000 empleados	5,08%	0,00%	0,00%	0,00%	1,69%
501 - 1000 empleados	3,39%	0,00%	0,85%	0,00%	0,00%
Mayor de 5001 empleados	0,00%	0,85%	0,00%	0,00%	0,85%
201 - 500 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
51 - 200 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
<b>Salud</b>					
501 - 1000 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
Mayor de 5001 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
51 - 200 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
1001 - 5000 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
1 - 50 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
201 - 500 empleados	0,85%	0,00%	0,00%	0,00%	0,00%

**Figura 31**

Preferencias de certificaciones por roles



sados en tener este compendio de certificaciones, bien sea porque ya las tienen, o porque están interesadas en otros motivos, así mismo en ese grupo lo menos apetecido es la certificación NSA/ISA. El rol auditor prefiere la certificación CFE con el 23,81% y la que menos apetece es el CRISC, los directores jefes de seguridad lo que más apetece es la certificación CSX (ISACA's Cybersecurity Nexus), mientras que es CIFI (Certified Information Forensics Investigator) es la menos apetecida. El director jefe de Tecnología aprecia la CIA (Certified Internal Auditor), mientras que no tener ninguna no es una opción

viable. Para los oficiales de seguridad CISO todas están en rangos positivos, destacándose las certificaciones GIAC del Sans Institute, y no es una opción viable el no tener alguna certificación. Para el profesional de seguridad del compendio de certificaciones está en su radar CISA (Certified Information System Auditor) y la que menos le llama la atención es CIFI.

Definitivamente las certificaciones tienen un impacto significativo en los profesionales de seguridad, aumentando su nivel de consciencia de la ciberseguridad, su nivel de conocimiento, y mejora de las tareas

(Fortinet, 2022), sin embargo, no significa siempre que estar certificado represente ser el mejor rol para una determinada posición, aprender y tener capacidad para seguir aprendiendo se convierte definitivamente en un factor fundamental (Martínez, 2022), para crecer en el mundo de la ciberseguridad.

Ser CISO definitivamente representa un desafío en todas las organizaciones, sin importar la naturaleza de esta, o sus condiciones principales es un rol que demanda esfuerzos, resistencia, preparación y consistencia (Proofpoint, 2022). La siguiente Tabla 12, detalla que tipo de información el profesional de seguridad entrega a las distintas instancias de la organización por sectores. Tanto el sector de consultoría especializada, educación y salud hablan de un CISO que no está entregando información de

ningún tipo, y por tanto puede estar equivocándose la organización a la hora de tomar decisiones, bien sea por que no haya definido que se necesite, o porque el CISO no tenga su voz definida. La importancia de la comunicación de los aspectos de seguridad en todas las esferas de la organización es clave, ganarse un espacio es un desafío que debe hacerse y son de las apuestas importantes que los cisos deben realizar (Accenture, 2020). Por otro lado tenemos en el sector de gobierno que el CISO se dedica a entregar información de las vulnerabilidades, como el primer tipo de información que entrega, en el sector financiero se manifiesta que lo que más entrega el ciso es información para la toma de decisiones, que adicional muestra y ratifica el nivel de madurez del sector en la materia, por su parte en el sector de las tecnologías de la información vemos que el ciso entrega informa-

**Tabla 12**

Entrega de información del CISO por sector de la industria

Entrega de Información del CISO en los sectores principales	Consultoría Especializada	Educación	Gobierno / Sector público	Salud	Servicios Financieros y Banca	Tecnologías de Información
Información relacionada con la gestión de la seguridad para la toma de acciones	12,82%	14,10%	16,67%	2,56%	17,95%	35,90%
No está entregando información	16,67%	16,67%	8,33%	25,00%	0,00%	33,33%
Información técnica relacionada con vulnerabilidades, amenazas, e incidentes	12,90%	11,29%	19,35%	3,23%	24,19%	29,03%
Información relacionada con los riesgos en Seguridad de la Información y Ciberseguridad para la toma de decisiones	12,68%	15,49%	14,08%	1,41%	25,35%	30,99%
Información relacionada con las brechas de seguridad existentes en la organización	15,25%	8,47%	13,56%	3,39%	23,73%	35,59%

ción para la acción, es decir una posición táctica para la implementación de acciones o posibles controles que estos requieran.

Al revisar la forma en como se espera que se comporte el CISO en las empresas de los distintos de la industria, hay datos interesantes relacionados en la Tabla 13. siguiente.

En el sector de la consultoría, educación y financiero se ve como un asesor, que está integrado al negocio y se espera que lo esté, sin embargo, al revisar la información que entrega, solo se ve que en el sector financiero cumple su rol acorde a lo que se espera del mismo. Por el otro lado, en el sector de las tecnologías y el sector salud, es visto como un estratega y su lenguaje se espera que sea de ries-

gos, sin embargo, en el sector de tecnologías lo que predomina es la entrega de información para la acción, y en el sector salud no está entregando información, lo cual hace ver que hay desfases en lo que sucede con el rol. Por último, el sector del gobierno lo ve como un supervisor, una persona que sigue un programa y por su cumplimiento, y al revisar el tipo de información que entrega se puede evidenciar que es el más consistente, puesto que lo ven como un supervisor y responde en la misma medida entregando información técnica que puede ayudar a cumplir con un programa de ciberseguridad.

Los profesionales de seguridad saben que hay que fortalecer tanto sus habilidades y sus capacidades, las habilidades a través de las certificaciones como lo resaltan los da-

**Tabla 13**

Visibilidad del CISO por sector de la industria

Visibilidad del CISO	Consultoría Especializada	Educación	Gobierno / Sector público	Salud	Servicios Financieros y Banca	Tecnologías de Información
CISO como Asesor (Integrado al negocio, educa, influencia, teniendo clara las implicaciones de todo con los ciber riesgos, relaciona nuevas visiones con riesgos emergentes, vela por el desarrollo de capacidades para manejar y enfrentar riesgos en toda la organización)	5,93%	5,93%	4,24%	0,85%	5,93%	6,78%
CISO como Estratega (Integra operación, riesgos y negocio, entiendo la relación de negocio, activo y operación y vela por ella)	3,39%	1,69%	0,85%	1,69%	4,24%	11,86%
CISO como Implementador (Vela por la implementación de las tecnologías de protección y su correcto funcionamiento, está pendiente de los detalles de toda la infraestructura de seguridad)	3,39%	3,39%	4,24%	1,69%	4,24%	5,93%
CISO como Supervisor ( Vela por la eficacia y eficiencia del programa de seguridad, su visión del control es la que rige como principio, Vela por los riesgos, y el cumplimiento)	3,39%	4,24%	5,08%	0,85%	2,54%	7,63%

tos de este año. Las siguientes Tablas (14,15) relacionan como los tipos de cisos prefieren formarse y en que prefieren hacerlo.

Es interesante, mientras que los CISOs tipo Asesor y Estratega prefieren la formación ejecutiva, el ciso implementador prefiere los diplomados y el supervisor las charlas especializadas.

Ahora al revisar las razones por la que toman estos programas, bus-

cando las oportunidades de mejora en su carrera profesional, se puede visualizar en la Tabla 15. El CISO tipo asesor, toma programas para gestionar las capacidades humanas, entendido como la necesidad de poder integrarse mejor con las organizaciones en las que trabaja y darle un nuevo sentido a la función que desempeña, el ciso estrategia toma en primera instancia los programas para mejorar su capacidad de gestión, requiere de comunicación y entendimiento de negocios

**Tabla 14**

Tipo de CISO y sus preferencias de formación

Tipo de CISO	Educación formal (pregrado, posgrado (maestría, especialización, doctorado))	Charlas especializadas	Diplomados	Certificaciones	Cursos cortos	Programas de formación ejecutiva
CISO como Asesor	30,00%	27,12%	22,00%	25,00%	27,12%	33,33%
CISO como Estratega	25,00%	23,73%	20,00%	25,00%	20,34%	27,78%
CISO como Implementador	23,00%	22,03%	32,00%	25,00%	28,81%	25,00%
CISO como Supervisor	22,00%	27,12%	26,00%	25,00%	23,73%	13,89%

**Tabla 15**

Tipo de CISO y las capacidades que puede mejorar

Tipo de CISO	Capacidades estratégicas (liderazgo, comunicación, rendición de cuentas, proyecciones financieras, pensamiento estratégico, pensamiento sistémico, visión (prospectiva y pronóstica))	Capacidades intelectuales (formación académica, conocimientos técnicos, análisis, síntesis)	Experiencia profesional	Capacidades Humanas (Empatía, Inteligencia Emocional, Creatividad, Curiosidad, Imaginación, Proactividad)	Capacidades de gestión (Habilidades para comunicar e interconectar negocios y necesidades en materia de seguridad de la información, entender el negocio, entender a las partes interesadas)
CISO como Asesor	25,99%	28,57%	23,33%	29,73%	28,57%
CISO como Estratega	26,85%	26,19%	25,00%	31,08%	32,97%
CISO como Implementador	23,15%	21,43%	28,33%	18,92%	18,68%
CISO como Supervisor	24,07%	23,81%	23,33%	20,27%	19,78%

como algo necesario para el desarrollo de la función. El CISO tipo implementador quiere mejorar su saber hacer, por eso mejorar la experiencia profesional es lo más adecuado, y el CISO tipo supervisor, está buscando poder llegar a los otros tipos de CISO, por eso buscar mejorar sus capacidades estratégicas para poder conectar todo lo aprendido de la gestión y llevarlo a un siguiente nivel.

Todos estos datos ratifican la situación de Colombia en relación con el desarrollo del profesional de segu-

ridad, sus capacidades, competencias y habilidades que deben ser desarrolladas continuamente y más ahora que los entornos cambiantes requieren de una acelerada capacidad para ser abordados.

### Temas emergentes

La Figura 32, muestra los temas relevantes y emergentes que tienen en la mira los profesionales de seguridad. Para este año el tema más relevante tiene que ver con la seguridad y control en la nube, seguido de las amenazas persistentes a-

**Figura 32**

Temas emergentes





vanzadas, la fuga de información sensible, los ataques a infraestructuras críticas, y el talento humano de seguridad como el quinto lugar.

y visualiza los desafíos, acorde con la realidad del sector, la madurez de este, y en esa línea sus capacidades y oportunidades.

### Consideraciones de los datos

Al revisar los temas emergentes y disgregarlos por sectores, podemos encontrar como cada sector ve

En la Tabla 16, se evidencian como los sectores más relevantes de la industria ven sus temas y ponen atención y seguro esfuerzos por entenderlos y manejarlos.

**Tabla 16**

Distribución de temas emergentes por sectores de industria

Temas emergentes por sectores	Tecnologías de Información	Servicios Financieros y Banca	Salud	Gobierno / Sector público	Educación	Consultoría Especializada
Fuga de información sensible	28,17%	16,90%	7,04%	18,31%	15,49%	14,08%
Seguridad en Dispositivos Médicos	35,00%	5,00%	15,00%	10,00%	20,00%	15,00%
Robótica	27,27%	27,27%	9,09%	18,18%	9,09%	9,09%
Talento Humano de Seguridad	34,43%	16,39%	4,92%	19,67%	16,39%	8,20%
Ransomware de las Cosas (RasoT)	33,33%	10,53%	7,02%	21,05%	17,54%	10,53%
Redes Sociales	40,00%	12,50%	5,00%	17,50%	12,50%	12,50%
Noticias y videos falsos (Fake news)	35,29%	11,76%	5,88%	14,71%	23,53%	8,82%
Malware en dispositivos móviles	37,50%	12,50%	7,14%	16,07%	16,07%	10,71%
Internet de las cosas – IoT	34,09%	6,82%	9,09%	13,64%	20,45%	15,91%
Inteligencia de amenazas	35,85%	18,87%	1,89%	16,98%	13,21%	13,21%
Seguridad y control en la computación en la nube	32,50%	18,75%	6,25%	16,25%	11,25%	15,00%
Inteligencia Artificial	44,44%	17,78%	4,44%	11,11%	13,33%	8,89%
Grandes datos y analítica	35,29%	20,59%	11,76%	11,76%	14,71%	5,88%
Geopolítica global	52,63%	10,53%	0,00%	10,53%	10,53%	15,79%
Internet Industrial de las Cosas (IIoT)	50,00%	14,29%	0,00%	7,14%	21,43%	7,14%
Ciberseguridad Industrial	38,89%	13,89%	5,56%	8,33%	13,89%	19,44%
Desinformación	37,21%	11,63%	9,30%	11,63%	16,28%	13,95%
Drones	66,67%	16,67%	16,67%	0,00%	0,00%	0,00%
Ciberguerra	39,02%	19,51%	0,00%	14,63%	12,20%	14,63%
Amenazas persistentes avanzadas	35,44%	17,72%	5,06%	15,19%	12,66%	13,92%
Ciberespionaje	41,51%	11,32%	0,00%	15,09%	13,21%	18,87%
Ciber armas	44,00%	4,00%	0,00%	12,00%	12,00%	28,00%
Blockchain	35,71%	14,29%	7,14%	19,05%	14,29%	9,52%
Ataques a infraestructuras críticas	31,25%	12,50%	6,25%	20,31%	12,50%	17,19%

El sector de las tecnologías de la información ve a la geopolítica global, así como al internet industrial de las cosas y los drones como sus primeros lugares para prestar atención. El sector financiero ve en la robótica, los grandes datos y la analítica y la ciberguerra factores de alerta que deben ser considerados. Por su parte el sector salud, ve en los drones, la seguridad de los dispositivos médicos y los grandes datos y analítica sus principales retos. El sector gobierno ve en el ransomware de las cosas, los ataques a infraestructuras críticas y el talento humano de seguridad, como las principales fuentes de desafío. El sector de la educación por su parte considera las fake news, al internet industrial de las cosas, y al internet de las cosas, sus principales retos. Por último, el sector de consultoría especializada ve en las ciberarmas, la ciberseguridad industrial y el ciberespionaje, las fuentes principales para atender el presente y el futuro, al menos el cercano.

## Reflexiones finales

Año tras año, el estudio muestra un afianzamiento de la seguridad digital como un instrumento corporativo en las empresas colombianas. En este contexto, cada vez más incierto, son necesarias perspectivas más incluyentes que involucren a los actores y los lleven a repensar o pensar de manera distinta la protección de la información, sin perder de vista lo ya alcanzado, y así

enfrentar y superar la realidad del mundo en que se desenvuelven.

Este último período evaluado ha venido cargado del afianzamiento producido por el fenómeno denominado pandemia que ha revolucionado y cambiado la forma en cómo la seguridad se tiene que plantear en las organizaciones, si bien es cierto que se habla de volver a los niveles prepandemia, lo claro es que la vida y la ciberseguridad nunca volverán a dichos estadios, pues las organizaciones no tienen muchos planes para perder el terreno ganado en materia de transformación digital.

En un primer momento vimos a las empresas volcadas al contexto digital y aprendiendo de muchas maneras lo que significaba entrar por completo en una realidad virtual. Luego un período de afianzamiento en el mundo digital que ha empezado a mostrar un poco de lo que vendrá en ambiente postpandemia, donde los entornos de trabajo, las fuerzas laborales y los procesos organizacionales serán diferentes (Davis, 2021).

La confianza en los entornos digitales y la construcción de la capacidad de ciberresiliencia se fundamenta en una estructura de gobierno de la seguridad, en la que las políticas, la gestión de riesgos y el conjunto de buenas prácticas se convierten en elementos centrales para dirigir los programas de ciberseguridad. La conexión entre una

estrategia de seguridad y los objetivos de seguridad que sean claros ayudaran a construir y fomentar la ciberresiliencia (World Government Summit – EY, 2020).

Confianza digital, va más allá de las tecnologías que puedan ser de utilidad para protegerse del adversario digital, implica componentes como la gestión de riesgos, como la ética en el manejo de los datos, el uso de buenas prácticas, y la participación de todos los actores de un ecosistema digital que cada vez es más complejo (Deloitte, 2021).

Situaciones como la evolución de los adversarios, la pandemia y la realidad digital de las organizaciones han cambiado la forma de ver la ciberseguridad, y así mismo la necesidad de repensar las prácticas de gestión de riesgos. Entender que es necesario evolucionar de la protección de una infraestructura, a la defensa y anticipación de un adversario digital, para ello se requiere que las prácticas estándares se consoliden en las organizaciones y así poder dar pasos más importantes que permitan evolucionar en las capacidades de la ciberseguridad, que desarrolle mejores posturas de seguridad y que repercutan en una adecuada ciberresiliencia.

Crear valor en un contexto digital, implica crear nuevos y novedosos esfuerzos por desarrollar programas de ciberseguridad que atiendan a las necesidades de las orga-

nizaciones, por un lado mejorar la práctica y el proceso al interior de las organizaciones para fortalecer lo que se debe hacer, en ello la seguridad de la información es un elemento clave, así como la seguridad informática. La primera desarrolla los procesos y refuerza la práctica, y la segunda apoya desde la vista tecnológica el diseño de esa arquitectura que busca proteger y asegurar. Por el otro lado, la ciberseguridad juega un papel indispensable para defender una organización en un ecosistema digital extremadamente denso, y anticiparse a un adversario cada vez más complejo.

Las discusiones alrededor de como se ve la ciberseguridad hacia adelante y cuáles son los temas emergentes que tienen en la mente no solo los profesionales de la seguridad, sino aquellos que tratan de visualizar el futuro, está centrado en ver a la ciberseguridad como un “*wicked problem*”<sup>1</sup> (WEFb, 2022).

Otro de los temas que trae gran preocupación a la mesa es el tema del talento de ciberseguridad (Stottandmay, 2022). Los ciberriesgos en general están en la agenda de todos los CEO de las organizacio-

---

<sup>1</sup> *Wicked Problem*: Un problema complejo es un problema social o cultural que es difícil o imposible de resolver por cuatro razones: conocimientos incompletos o contradictorios, el número de personas y opiniones implicadas, la gran carga económica y la naturaleza interconectada de estos problemas con otros. Fuente: [https://www.wickedproblems.com/1\\_wicked\\_problems.php](https://www.wickedproblems.com/1_wicked_problems.php)

nes de todo el mundo y eso no es una sorpresa, realmente es una constante de los últimos años (PwC, 2022). Las tensiones geopolíticas, la reciente guerra en Ucrania, y los conflictos posteriores que se divisaran en el espacio digital son parte de lo que se visualiza no solo para el largo, también en el corto plazo (Infosecurity, 2022).

Los adversarios cada vez más orientados, especializados y distribuidos, con mayor intensidad, intención y recursos para hacer su trabajo, estarán a la orden del día, en el mismo sentido, la línea delgada entre adversarios y Estados apoyándolos hará de la zona gris un lugar más denso para estar alerta (Fireeye, 2022). Las ciberoperaciones están a la orden del día, y con el conflicto en el cual se encuentra el mundo aún más. Es por ello, que se verán mayores movimientos por parte de gobiernos y naciones en el manejo de sus operaciones cibernéticas, de tal manera que debe haber un especial cuidado del ecosistema en el que se desenvuelven no solo las naciones, sino las organizaciones (Mandiant, 2022).

Definitivamente los riesgos que se presentan e incrementan por las cadenas de suministro serán otro de los juegos a atender en un espacio de trabajo cada vez más complejo, no solo para las organizaciones financieras, en todos los sectores de la industria la tensión y presión es importante pues no tra-

bajar con los terceros y no hacerlos parte de un modelo integrado de protección puede traer consecuencias desafortunadas (FS-ISAC, 2022). Claramente la pandemia y estos dos años de vivir en ella ha mostrado el valor del mundo digital, sin embargo, también ha mostrado por un lado el aumento sostenido de los riesgos, ha visibilizado aún más la capacidad del adversario por hacer daño, así mismo ha acelerado el desarrollo de las capacidades organizacionales tanto para asegurar y proteger, como para anticipar y defenderse de un adversario cada vez más dotado (Trendmicro, 2022).

El mundo OT (Tecnología de Operación), ha tenido grandes impactos por diferentes anomalías, no por nada está en las preocupaciones de sectores como el de las fuerzas armadas, tendencia que también se puede ver advertir en el informe de IBM (2022) y que muestra que este es un escenario complejo que debe ser protegido por las implicaciones que tiene en las múltiples industrias.

Los ejecutivos de seguridad de esta nueva era se enfrentan de una manera más directa a otros escenarios dinámicos que demandan reacciones rápidas y prospectivas arriesgadas. Estos implican desarrollar espacios para anticiparse y observar los entornos cambiantes y superpuestos, en procura de la protección de la información y los nuevos activos digitales.

Por tanto, esta nueva realidad hace que los líderes de seguridad necesiten evolucionar, no solo por desarrollar nuevas habilidades, a su vez capacidades y competencias que los posibiliten para enfrentar los desafíos actuales. Los Líderes de seguridad seguirán siendo líderes de niveles medios (Fireeye, 2022; Proofprint, 2022; Navisite, 2021), que deben poder actualizar el conjunto de herramientas como la comunicación para que puedan interactuar con mayor determinación en los equipos de trabajo.

En la realidad colombiana, los datos muestran que los esfuerzos se vienen haciendo y las demandas de la realidad digitalmente modificada aceleran la transformación de la visión de la seguridad de la información. El contexto internacional ratifica algunas de las tendencias de Colombia

En la realidad nacional se pueden concluir los siguientes aspectos:

1. Sectores como el sector financiero han mostrado una evolución y madurez que se ve reflejada en sus capacidades para atender los desafíos de la ciberseguridad, no significando por supuesto que son invulnerables al adversario, sino que pueden estar mejor preparados para enfrentarlo.
2. Las áreas de seguridad siguen ganando terreno, espacio, posición, poder e influencia, todos

los sectores de la industria a su ritmo lo ven y siguen aprendiendo, a lo mejor no con la velocidad que debería ser, pero al menos los marcadores e indicadores muestran progreso en todos ellos.

3. Las compañías de gran tamaño, con más de 1000 empleados, son las que tienen mayor claridad en torno a un área independiente y a un director de seguridad. En tales empresas grandes, el área de seguridad depende de las direcciones como la de gestión de riesgos. Es interesante observar entre las organizaciones de todos los tamaños, el bajo porcentaje que no tiene un cargo o responsabilidades definidas.
4. La posición del profesional de seguridad continúa su proceso de afianzamiento dentro de las organizaciones, cada vez se ven más plazas creadas de profesionales de seguridad como CISOs y directores de seguridad en las organizaciones, estos movimientos demandan la creación de nuevas y actualizadas conjunto de competencias, capacidades y habilidades que le permitan desarrollar mejor sus nuevas funciones. La formación, crecimiento y aprendizaje del CISO, sigue estando presente, no se puede sustraer su esfuerzo por seguir asimilando lo que significa la función, el rol y sobre todo la adaptabilidad en un en-

torno tan cambiante como el actual.

5. Entre más disruptivos son los entornos de trabajo, las nuevas capacidades como las estratégicas, las humanas y las técnicas necesitan ser desarrolladas de manera integral para atender la demanda de nuevas responsabilidades.
6. La confianza digital que los negocios actuales necesitan muestra cada vez más que es necesario un profesional de seguridad más empoderado, más desarrollado y preparado; por tanto, eso invita al profesional de ciberseguridad salir de su zona de confort de manera permanente, entrenarse y adicional aprender es la clave para enfrentar el desafío (Martínez, 2022).
7. La práctica básica, como la gestión de riesgos, el uso de marcos de referencia, son una realidad en Colombia, su afianzamiento es requerido, para que el fundamento de la ciberseguridad esté acorde con las necesidades de las empresas, y así poder avanzar en el desarrollo de capacidades que lleven a las organizaciones a un estado de ciberresiliencia que soporte las operaciones del negocio.
8. La realidad digital hace que todos los sectores e industrias lleven su mirada al tema de ciberseguridad. A los sectores como el financiero, la consultoría especializada y el gobierno les interesa participar y conocer la realidad de la seguridad, tendencia observada en diferentes informes publicados sobre seguridad y ciberseguridad.
9. Los riesgos es el lenguaje común de los negocios y a su vez es un instrumento catalizador de un programa de seguridad. Los Líderes de seguridad digital están considerando este instrumento como una valiosa oportunidad para elevar su interlocución con los niveles directivos y ejecutivos, para poder tomar caminos acordes a la realidad digital de la empresa.
10. La confianza digital y la ciberresiliencia se convierten en un generador de nuevos negocios; tendencias internacionales también sostienen que dicha confianza es una fuente que motiva a cultivar las relaciones entre consumidores y quienes ofrecen los servicios, para configurar un activo valioso a la hora de manejar y maniobrar en los ecosistemas digitales actuales.
11. A nivel nacional, se mantiene la sólida tendencia de usar mecanismos tecnológicos como las principales herramientas de protección. Si bien las tendencias internacionales dan esto por sentado, se debe hacer un llamado tanto a los responsables de seguridad como a las organi-

zaciones para que vean a la seguridad como un tema inherente a la dinámica empresarial. Las tendencias internacionales ratifican que es necesario extender la visión de la seguridad como una fuente generación de valor para la organización y los objetivos de su negocio.

12. El poder de las anomalías digitales, de los adversarios y de la realidad digital se entiende cada vez más en el marco de las organizaciones colombianas. Más allá de lo técnico, se registran los errores humanos y, en tal sentido, es necesario pasar de procesos de sensibilización al cambio de comportamientos, liderado por los responsables de la seguridad, con el ánimo de crear una nueva cultura alrededor de entornos digitalmente modificados. Así mismo, es necesario gestionar un programa de seguridad que permee todos los niveles organizacionales basados en prácticas dirigidas a los diferentes grupos de interés, y orientadas a construir posturas de seguridad diferenciadas y articuladas desde los desafíos que debe asumir el talento humano.
13. Las nuevas tecnologías como Cloud, IoT, IA, *machine learning*, *Zero Trust* y otras, están cambiando la concepción del mundo, la forma de interactuar y los retos a los que se enfrentan las organizaciones a nivel nacional e internacional. De ahí que los

profesionales de seguridad deban tener claridad para profundizar en estas nuevas tendencias y su uso.

14. Es claro que el cisne negro (o ¿sorpresa predecible?) denominado Covid-19, ha cambiado por completo no solo la forma de ver la vida, sino ha resaltado la importancia de la ciberseguridad y la gestión de las tecnologías de la información. Hoy más que nunca se observa a la ciberseguridad como una capacidad empresarial, que ofrece y aporta en el desarrollo de negocios digitales, y que se enfrenta y enfrentará las tensiones geopolíticas y de cumplimiento con mucha más profundidad. Esta capacidad deberá apalancar la confianza digital necesaria para ofrecer servicios y desarrollar modelos de negocio en el ecosistema digital de hoy como fundamento del nuevo normal que empezamos a construir.
15. No es viable predecir el futuro, pero si es necesario crear escenarios, desarrollar libros de jugadas (*Playbooks*), hacer ejercicios de simulaciones, revisiones y auditorías a las cadenas de suministro, entre muchas otras acciones que le ayuden a la organización a estar preparada y a sus líderes de seguridad a ser tomadores de inciertos, y en la misma línea poder ayudar a la organización a gestionar y disminuir los posibles riesgos que

la incertidumbre trae (Cocron & Aronhime, 2022).

En resumen, el panorama general de la seguridad en Colombia muestra el sostenido proceso de cambios apalancados en la realidad actual empujada por una presencia de una pandemia que dos años después no termina y que sigue empujando a los negocios a un contexto digital cada vez más complejo.

El año 2021 fue un año que afianzó un nuevo modelo de vida y sociedad, el año 2022 es el momento para desarrollar nuevas formas de aprender y de seguro nuevos aprendizajes para los posibles futuros que tendremos que construir y donde la ciberseguridad tendrá parte esencial, como lo han mencionado en muchas reuniones e instancias internacionales.

Sea esta la oportunidad para decir que este es un ejercicio para repensar lo que creemos que sabemos y explorar aquello que no sabemos, para así, deconstruir muchas cosas en procura de nuevos aprendizajes que nos lleven por caminos distintos y conocimiento renovados.

## Agradecimientos

*Se hace un reconocimiento y mención especial a la cooperación recibida por parte de otras asociaciones tales como, TacticalEdge, CISOS.CLUB, Asociación Colombiana de Profesionales de Seguridad y CiberSeguridad (APSIC), CISObear (Pe-*

*rú), Consejo de Seguridad de la Información y Ciberseguridad (México), Sociedad Chilena de Seguridad de la Información (SOCHISI), así como a todas las personas que atendieron el llamado a través de los distintos medios digitales.*

## Referencias

- Accenture. (2020). The Cyber-Committed CEO and Board. [https://www.accenture.com/\\_acnmedia/PDF-132/Accenture-Cyber-Committed-CEO-And-Board.pdf](https://www.accenture.com/_acnmedia/PDF-132/Accenture-Cyber-Committed-CEO-And-Board.pdf)
- Barracuda. (2022). Spear Phishing: Top Threats and Trends. <https://assets.barracuda.com/assets/docs/dms/Spear-phishing-vol7.pdf>
- Cano, J. & Almanza, A. (2021) "Reflexiones y retos para la academia en la formación de profesionales de seguridad/ciberseguridad en Colombia: 2010 - 2020" (2021). ISLA 2021 Proceedings. 7 <https://aisel.aisnet.org/isla2021/7>
- Cocron, A. & Aronhime, L. (2022). Risk, Uncertainty, and Innovation. *Nato Review*. <https://www.nato.int/docu/review/articles/2022/04/14/risk-uncertainty-and-innovation/index.html>
- CyberEdge Group (2022). Cyberthreat Defense Report. <https://cyber-edge.com/wp-content/uploads/2022/04/CyberEdge-2022-CDR-Report.pdf>
- DarkReading. (2022). The state of CISO influence 2021. The maturing CISO role. <https://www.coalfire.com/documents/reports/the-state-of-ciso-influence>
- Davis. D. (2021). 5 Models for the Post-Pandemic Workplace. HBR. <https://hbr.org/2021/06/5-models-for-the-post-pandemic-workplace>



- Deloitte (2021). Building The Resilient Organization.  
[https://www2.deloitte.com/content/dam/insights/articles/US114083\\_Global-resilience-and-disruption/2021-Resilience-Report.pdf](https://www2.deloitte.com/content/dam/insights/articles/US114083_Global-resilience-and-disruption/2021-Resilience-Report.pdf)
- Deepinstinct. (2022). Voice of SecOps 2022.  
<https://info.deepinstinct.com/voice-of-secops-v3-2022>
- FBI. (2022). Internet Crime Report 2021.  
[https://www.ic3.gov/Media/PDF/AnnualReport/2021\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf)
- Fireeye (2022). M-Trends 2021.  
<https://www.arrow.com/ecs-media/16352/fireeye-rpt-mtrends-2021.pdf>
- Fortinet. (2022). 2022 Cybersecurity Skills Gap.  
<https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf>
- FS-ISAC. (2022). Navigating Cyber2022.  
<https://www.fsisac.com/hubfs/NavigatingCyber-2022/NavigatingCyber2022-TLPWHITE-FIN.pdf>
- IBM (2022). Cost of a Data Breach Report 2021.  
<https://www.ibm.com/downloads/cas/OJDVQGRY>
- INFOSECURITY (2022). State of cybersecurity report 2022.  
<https://www.infosecurity-magazine.com/white-papers/state-of-cybersecurity-report-2022/>
- ISACA (2022). State of Cybersecurity 2022. Global Update on Workforce Efforts, Resources and Cyberoperations.  
<https://www.isaca.org/go/state-of-cybersecurity-2022>
- Keeper. (2022). Ransomware impact report.  
<https://www.keeper.io/hubfs/PDF/2021-ransomware-impact-report.pdf>
- Mandiant. (2022). | MANDIANT M-TRENDS 2022.  
<https://www.mandiant.com/media/15671>
- Marsh. (2022). The state of cyber resilience.  
<https://www.marsh.com/us/services/cyber-risk/insights/the-state-of-cyber-resilience.html>
- Marlin Hawk (2020). Global Snapshot: The CISO in 2020. Recuperado de:  
<https://www.marlinhawk.com/docs/Marlin-Hawk-Global-CISO-Research-Report.pdf>
- Martinez, J. (2022). La información es inútil sin conocimiento.  
<https://www.linkedin.com/pulse/la-informaci%C3%B3n-es-in%25C3%25B3n-es-in%25C3%25BAtil-sin-conocimiento-javier-mart%25C3%25ADnez-aldanondo/?trackingId=%2F8Kotk%2BATGGJnh%2FuRNG70Q%3D%3D>
- Navisite. (2021). The State of Cybersecurity Leadership and Readiness.  
<https://www.navisite.com/resources/reports-1/state-of-cybersecurity-leadership-and-readiness-report>
- PwC (2022). 2022 Global Risk Survey Embracing risk in the face of disruption.  
<https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/assets/pwc-global-risk-survey-report-2022-main.pdf>
- Proofpoint. (2022). 2022 Voice of the CISO REPORT. Global Insights Into CISO Challenges, Expectations and Priorities.  
<https://www.proofpoint.com/sites/default/files/white-papers/pfpt-us-wp-voice-of-the-CISO-report.pdf>
- Stottandmay. (2022). Cyber Security in Focus 2022.

- [https://fs.hubspotusercontent00.net/hubfs/2529404/Research/Cyber\\_Security\\_in\\_Focus\\_22.pdf?\\_hsmi=201423978](https://fs.hubspotusercontent00.net/hubfs/2529404/Research/Cyber_Security_in_Focus_22.pdf?_hsmi=201423978)
- TrendMicro. (2022). Navigating New Frontiers Trend Micro 2021 Annual Cybersecurity Report.  
<https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf>
- Verizon (2022). Data Breach Investigation Report.  
<https://www.verizon.com/business/resources/reports/2022/dbir/2022-dbir-data-breach-investigations-report.pdf>
- WEF - World Economic Forum (2022) Global Cybersecurity Outlook 2022.  
[https://www3.weforum.org/docs/WEF\\_Global\\_Cybersecurity\\_Outlook\\_2022.pdf](https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf)
- WEFb - World Economic Forum (2022) Global Cybersecurity Outlook. Meeting of experts.  
<https://www.weforum.org/events/world-economic-forum-annual-meeting-2022/sessions/global-cybersecurity-outlook-1a06c9fd7d>
- World Government – EY. (2020) Cyber Resilience in the Digital Age.  
<https://www.worldgovernmentsummit.org/api/publications/document?id=24717dc4-e97c-6578-b2f8-ff0000a7ddb6>
- Zscaler. (2022). 2022 ThreatLabz Phishing Report.  
<https://www.zscaler.com/resources/industry-reports/2022-threatlabz-phishing-report.pdf>

**Andres R. Almanza J., Ms.C, CISM.** Chief Growth Officer en CISOS.CLUB, Investigador en Ciberseguridad SegInfo y Liderazgo. | Executive Certificate in Cybersecurity Leadership & Strategy by FIU University | Certificado como ISO 27001 Lead Implementer and 27005 Lead Manager from PECB | CISM, ITILv3, LPI | Certificado como Coach Profesional Internacional, Master in Leadership and Organizational Development with Coaching, Executive Master's in Leadership Skills Developed in Harvard, & Coach Profesional avalado por International Coach Federation | Profesional en Ingeniería de Sistemas | especialista en seguridad en redes y máster en seguridad de la información. Docente del programa de maestría de la Universidad Externado de Colombia y de la Universidad de las Américas en Ecuador. Creador de la Comunidad CISOS.CLUB, CISOS-COL y CISOS-LATAM (Linkedin) y Miembro del comité editorial de la revista sistemas de ACIS.

# Criptoactivos

DOI: 10.29236/sistemas.n163a5

*Implicaciones tecnológicas, económicas y sociales.*

Sara Gallardo M.

De los criptoactivos todavía no se habla con mucha fluidez en el país, razón suficiente para que en el tradicional foro se trate el tema con expertos, en la búsqueda de opiniones sobre los asuntos más relevantes.

Jeimy J. Cano Martínez, director de la revista y Andrés Almanza, miembro del Comité Editorial estuvieron presentes en la reunión. El director abrió el debate formulando la primera pregunta a los invitados Ana María Zuluaga Tafur, coordinadora del grupo de Innovación Tecnológica y Financiera en la Superintendencia Financiera; Fabio Mauricio Pinzón González, director general

de Tecnología del Banco de la República y Julio López Medina, gerente de Infuturo Proyectos.

*¿Qué son los criptoactivos? En el marco de los criptoactivos ¿cómo se define el concepto de "valor" de un objeto, producto y dinero, entre otras categorías?*

**Ana María Zuluaga T.**

*Grupo de Innovación Tecnológica y Financiera*

*Superintendencia Financiera*

Cuando surge algo nuevo la humanidad se acerca para manifestar si lo conoce o no, intenta definirlo y le pone un nombre. En el caso de los criptoactivos, inicialmente se seña-

ló que era algo parecido al dinero. Con el paso de los años, el tema ha motivado a las autoridades, a la empresa privada y a los académicos a estudiarlo para entender más de qué se trata y se ha entendido que este tipo de activo puede ser utilizado para diferentes fines: almacenamiento de información, intercambio de información, transferencia de valor, pagos o inversión. A la fecha, podemos decir que es un activo intangible representado en la tecnología de registro distribuido y con componentes criptográficos.

### **Fabio Mauricio Pinzón G.**

*Director general de Tecnología  
Banco de la República*

Se trata de una representación de valor en el mundo digital en la que se puede o no confiar. Como ha sido el oro en el mundo material, un metal que las personas pueden utilizar como una forma de inversión o de trueque a la que se le tiene confianza a nivel global. Tanto el oro como los criptoactivos, tienen po-

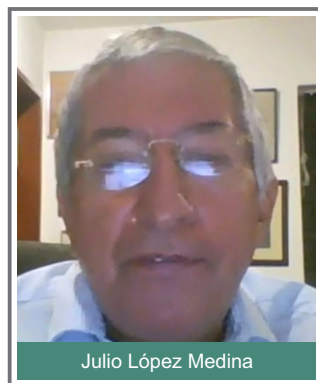
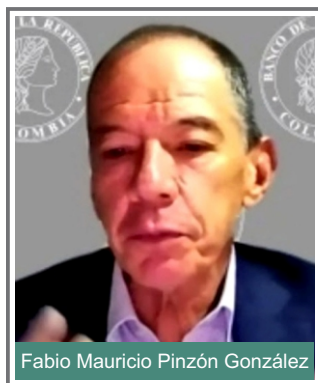
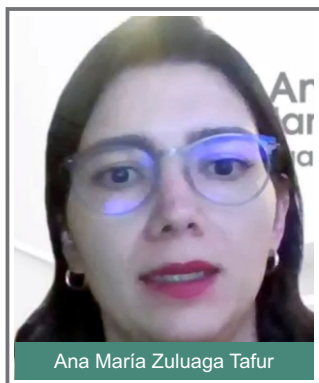
der de trueque como cualquier activo. Ninguno de los dos es moneda legal, o sea de aceptación forzosa por parte del que la recibe, en la mayor parte del mundo.

### **Julio López Medina**

*Gerente*

*Infuturo Proyectos*

El valor es un concepto subjetivo que las personas utilizan en el pago de un objeto; se puede tener algo muypreciado, pero si en el momento de venderlo me dan tres pesos, pues esa suma es el valor y la transacción es la que lo define. En la economía tradicional el valor está sujeto a la oferta y a la demanda. Valdría la pena analizar las diferencias entre economía tradicional y digital. Es sorprendente que haya economistas apoyando el tema de los criptoactivos y las seudomonedas, toda vez que en la economía tradicional no tiene sentido. Existen casos de seudomonedas lanzadas al mercado por estrellas de cine o deportivas, ofreciendo fantasías. Es necesario anotar lo que significa



el valor intrínseco de un objeto, inherente y esencial de un activo, independiente de su valor en el mercado. Anteriormente, las monedas estaban basadas en oro y el peso colombiano era un peso en oro cambiada en el Banco de la República por una medida específica en gramos de oro.

No es posible llamar al criptoactivo un activo porque no coincide con lo que significa en economía un bien fundamentado. Cuando se invierte en una acción su valor está representado en el patrimonio de la empresa y en la suma que la gente pague por ella con base en sus proyecciones a futuro.

En el caso de los criptoactivos la gente está dispuesta a pagar unas sumas absurdas sin ninguna base.

Otro concepto diferente y asociado es el de los NFTs (Non Fungible Token). Hay cosas que se consumen con el uso, por ejemplo, casas, productos agrícolas, lo que le resta valor al objeto. Los NFTs son medios digitales de intercambio, asociados a un objeto físico no consumible, y corresponden en su mayoría a obras de arte digitales, aunque lo están extendiendo a obras reales. Es en este caso que se utilizan los NFTs, basados en blockchain, como medio de certificación e intercambio.

Así como hablamos del universo real, hoy en día estamos hablando del universo digital que es todo lo

que es no presencial: videos, gráficas totalmente generadas por computador, videos manipulados por computador, que unidos a la interacción entre las personas, genera “una nueva realidad”. El primer ejemplo son los juegos electrónicos y hablando de criptoactivos resalto la existencia de objetos digitales (armas, escudos protectores, capacidad para poder desplazarse dentro del juego, por ejemplo) que son intercambiados por dinero real (vía seudomonedas normalmente) dentro de la interacción del juego en medios digitales. Este universo digital se denomina metaverso, y aunque no lo crean hoy se publicitan ofertas de “tierra” en el metaverso; debe ser digital y de todas las versiones de metaverso que hay, porque cada empresa puede armar su propia versión. Resalto que no necesariamente son criptoactivos porque no están siempre basados en criptografía fuerte (se pueden negociar en dólares de manera digital), pero si son activos digitales.

### **Jeimy J. Cano M.**

*¿Cuáles son los retos de seguridad y control en el uso de los criptoactivos para que puedan ser de uso masivo?*

### **Fabio Mauricio Pinzón G.**

No me atrevo aún a hablar de seguridad y control del uso masivo de criptoactivos si ni siquiera está resuelto el tema de cobertura. Si yo quiero que algo sea de uso masivo es porque en general voy a mejorar

el bienestar de la población. En la realidad colombiana, solo un 50% de la población tiene Internet de manera permanente en su celular y el resto compra paquetes de datos y minutos en prepago. Ese es uno de los retos, no solo de los criptoactivos, sino del dinero digital (*Central Bank Digital Currency - CBDC*) respaldado por la economía de un país, o incluso de los pagos inmediatos usando el celular. Si este mecanismo no es asequible a todos los colombianos, genero intermediarios para el uso del servicio que ponen en duda el logro del bienestar general. En mi opinión, el primer reto es cobertura para volver el sistema masivo. En paralelo con este despliegue masivo voy preocupándome de la seguridad: quién emitió el activo; quién es el dueño actual; autenticación y certificación de ambos; características de la transacción y controles sobre la misma; nivel de anonimato tanto de los involucrados, como de la transacción y su monto.

### **Jeimy J. Cano M.**

*Lo masivo es igual a bienestar para todos, para que todos estén incluidos. Desde esa perspectiva, ¿cuáles serían los retos de seguridad y control que habría que considerar o cuáles son los que habría que superar para que eso funcione?*

### **Fabio Mauricio Pinzón G.**

Sobre seguridad hablemos solo de la trazabilidad de las transacciones. Un ejemplo interesante es el proyecto Hamilton o el nacimiento

del Open-CBDC Project en Github. Presentado en su totalidad en un documento (busque “Project Hamilton whitepaper” en Google) preparado por MIT y el Federal Bank of Boston y que tiene dos aproximaciones sobre cómo se pueden manejar las transacciones de lo que sería una moneda digital emitida por un Banco Central.

Primero que todo, ambas aproximaciones heredan de Bitcoin y de nuestra billetera de efectivo el concepto de transacciones sin usar y transacciones usadas. Supongamos que Ana y Bernardo tienen ambos un celular con una App de billetera digital. Supongamos también que Ana tiene hoy en su billetera digital \$45000, producto de haber recibido digitalmente \$15000 y \$30000 desde dos fuentes. Ana tiene entonces en su billetera digital dos transacciones sin usar por un total de \$45000. Ahora, para pagarle a Bernardo un almuerzo de \$37500 ambos usan su billetera digital. El resultado final es que Bernardo queda en su billetera digital con una transacción sin usar de \$37500 y Ana con una transacción sin usar de \$7500, su cambio. Las dos transacciones de \$15000 y \$30000 que Ana tenía en su billetera se convirtieron en transacciones usadas. Ana ya no podrá adquirir nada con ellas.

En la primera aproximación de Hamilton, no se guardan las transacciones usadas, solo existen los \$37500 de Bernardo y los \$7500 de

Ana. En la segunda si se guarda que Ana tuvo \$45000, además de cómo y cuándo le dio \$37500 a Bernardo. En conclusión, la primera aproximación da más peso a la velocidad que a la trazabilidad. En la segunda aproximación, dado que se requiere el registro ordenado de todas las transacciones, se sacrifica velocidad en aras de este ordenamiento que refleja la historia transaccional de la persona, o sea toda la trazabilidad. En todo caso la velocidad mínima de la segunda aproximación sobrepasa las cien mil transacciones por segundo. La decisión de usar una u otra alternativa está directamente relacionada con la necesidad o no de tener trazabilidad de las transacciones.

### Ana María Zuluaga T.



Sobre el asunto de volverlos masivos, a nivel mundial diferentes jurisdicciones han empezado a desa-

rollar iniciativas para probar sus beneficios y evaluar los riesgos. Por ejemplo, se tienen proyectos para emitir criptoactivo de banco central, como lo hizo Bahamas. Así mismo, se destaca el Banco Central de China con su proyecto de Yuan Digital.

Existen unos temas de riesgos relacionados con la identidad de quienes son los dueños de las billeteras en donde se almacenan las claves de los criptoactivos. Conocer a las personas y sus hábitos transaccionales permite implementar medidas para gestionar los riesgos operacionales, de ciberseguridad y de lavado de activos. La tecnología de los criptoactivos pseudoanónimos ha permitido desarrollar herramientas de conocimiento del cliente y de las transacciones siguiendo los lineamientos del Grupo de Acción Financiera Internacional (GAFI) sobre proveedores de servicios de activos virtuales.

Hay un segundo tema y es el riesgo de fraude, que como ocurre con criptoactivos ocurre con cualquier cosa. Ustedes saben y más en Colombia, cómo vende la gente todavía de una forma tan ingenua, después de tantos temas de pirámides.

Y hay un tercer aspecto relacionado la protección al consumidor. Es importante que los participantes de las transacciones con criptoactivos informen a los consumidores los roles y responsabilidades de los pro-

veedores, revelen adecuadamente la información y los riesgos relacionados a las operaciones con criptoactivos.

### **Jeimy J. Cano M.**

Debería haber un trabajo en conjunto entre la Superintendencia Financiera, la Superintendencia de Industria y Comercio y la Superintendencia de Sociedades para darle mayor claridad y profundidad a estos temas, porque como bien decíamos muchas personas poco lo entienden y al no tener esa dimensión de lo que puede pasar o de lo que está pasando con este tipo de “medios de intercambios de valor” los ciudadanos pueden tomar decisiones no informadas.

### **Ana María Zuluaga T.**

La evolución en los avances tecnológicos, las nuevas disposiciones de las autoridades internacionales y el marco normativo local generan un entorno diferente para evaluar en un ambiente controlado, las operaciones de depósito con plataformas de intercambio de criptoactivos (exchange) utilizando productos de depósito del sistema financiero. Este proyecto se realiza con para propiciar un espacio de prueba conjunto entre el ecosistema digital y el Gobierno Nacional en materia de criptoactivos a través de una herramienta de innovación como el espacio controlado de pruebas regulatorio de la SFC.

Esta iniciativa se adelanta en coordinación con la Consejería Presi-

dencial para Asuntos Económicos y de Transformación Digital, el Ministerio de Hacienda y Crédito Público, el Ministerio de Tecnologías de la Información y Comunicaciones, el Banco de la República, la Unidad de Regulación Financiera (URF), la Superintendencia de Sociedades, la Superintendencia de Industria y Comercio, la Dirección de Impuestos y Aduanas Nacionales (DIAN) y la Unidad de Información y Análisis Financiero (UIAF).

Bajo este contexto se busca que todas las autoridades participantes en el proyecto piloto puedan medir la efectividad de los recientes desarrollos tecnológicos en la verificación de la identidad digital y de trazabilidad en las transacciones, dentro del ámbito de las competencias asignadas en el marco vigente.

El nivel de educación financiera del país aún es bajo. Es muy complicado explicarle una tasa de interés a una persona. El reto se vuelve más grande para tener avances en materia de educación financiera relacionada con criptoactivos.

### **Julio López M.**

El tema de protección al consumidor es muy importante y un requisito para el desarrollo de la economía digital; infortunadamente, ha habido casos que resultan en estafas, lo mismo que sucede cuando hay una promesa de un producto que, a la hora de la compra termina también siendo otro. Desafortunadamente



en el marco de estas situaciones el sistema judicial no ofrece una protección suficiente al consumidor; por ejemplo, en el caso de las inversiones en monedas digitales, normalmente recomiendan invertir “lo que a usted le sobra” y le previenen de que el valor a futuro puede ser cero o una fortuna. Si le agregamos la informalidad del mercado y la dispersión geográfica, es muy difícil que las entidades de protección al consumidor puedan actuar y vale la pena analizar más a fondo cómo se están vendiendo y cómo están ofertando esas pseudomonedas.

Volviendo al tema del uso masivo de los criptoactivos, con las definiciones actuales no pueden ser de uso masivo; tecnológicamente es imposible; en este momento generar un nuevo bloque dentro de la cadena *blockchain* de bitcoin que tiene un tamaño de 324 gb, toma 10 minutos.

Existen minas de más de 30.000 computadores, 30.000 CPU especializadas orientadas a esa tarea y se tardan 10 minutos en generar un nuevo bloque que puede contener una transacción o máximo 2048; por esta razón no es factible un uso masivo y en mi opinión persistirán las monedas normales para altos volúmenes de transacciones y las criptomonedas estarán restringidas a temas como los NFTs que son transacciones muy especializadas, y de bajo volumen. Recordemos que un banco colombiano puede llegar a soportar un millón de

transacciones en una hora, lo que no sería factible con la tecnología de blockchain.

Sobre los retos de seguridad y control existen en todos los elementos de la cadena de negociación. A pesar de que el anonimato es una característica de las criptomonedas, pensando en su protección como usuarios, las personas están acudiendo a intermediarios financieros informales y normalmente ese es el eslabón más débil de la cadena. Hay muchos casos documentados, aunque normalmente se manejan con mucho sigilo. Ha habido varios casos de robos a intermediarios de monedas digitales por valores de varios cientos de millones de dólares. En Q1 del año 2021 hay registro de nueve de estos casos con pérdidas superiores a los diez millones de dólares.

Con el fin de controlar las transacciones con monedas digitales robadas a estos intermediarios existe una lista negra de Bitcoins, de monederos, de direcciones, ilícitas. Este control no funciona en el darkweb, o en ventas directas persona a persona. Otra situación que sucede actualmente es que los hackers que están amenazando con “ensuciar” y llevar ese dinero o tokens mal habidos hacia otras billeteras o de usarlo políticamente. Considerando que no hay una autoridad de control en transacciones con criptomonedas y que hay muchas transacciones anónimas, la impunidad es total.

Otro riesgo frecuente es el hacking al dueño de la billetera, similar a como le roban a uno de su cuenta bancaria. Importante notar que si un hacker se mete a un teléfono y le sacan la plata del banco normalmente serán montos pequeños de acuerdo a los parámetros del banco y uno puede poner un denuncia. Eventualmente algún seguro responderá y en muchos casos se recupera el dinero. En el caso de las criptomonedas no hay manera de hacer ningún control, y una vez que le hackearon al dueño de una billetera su monedero electrónico, transan de manera inmediata su contenido y esos tokens no se podrá incluir en una lista negra.

Yo definitivamente considero que esta es una plataforma que tiene muchos riesgos, pocos controles, mucho anonimato, todo lo que conlleva a muchos riesgos. Finalmente otro tipo de casos, que debe ser el más frecuente, aunque no está documentado, es que a alguien se le olvide la clave de su billetera o de su monedero electrónico. Similar en caso de muerte del propietario, noten que estos valores no son heredables ni pueden ser transferidos por una entidad financiera responsable. Si el dueño de una billetera de criptomonedas fallece y no ha tenido la precaución de entregarla a alguien, “esa platica se perdió”. Caso similar es cuando se pierde el medio magnético, en el que están guardadas físicamente las billeteras (puede ser dentro de una llave USB). Si no existe copia es irrecu-

perable. Resalto que si se me pierden una tarjeta de crédito, me expiden una nueva y de paso me garantizan que nadie va a usar la anterior y cambian el número. En monedas digitales esa posibilidad no existe. Me pregunto si la gente es consciente de que no se puede heredar, de que tienen que tener muchos cuidados con las billeteras electrónicas, tienen que entregarle la llave a otra persona al menos, con el riesgo que eso significa.

### **Jeimy J. Cano M.**

Luego de estas tres intervenciones, que ilustran aspectos positivos y limitaciones sobre los temas de seguridad y control podemos concretar algunas ideas. Mauricio hace énfasis en la perspectiva del pago inmediato, en el tema de la privacidad como elemento fundamental. De otra parte, Ana María ubica el foco en los proveedores, en los intermediarios que son los que manejan este tipo de transacciones pues claramente se vuelven parte muy importante de la cadena en este ejercicio, así como el tema de protección al consumidor, que se debe repensar frente a esta nueva forma de intercambiar valor.

*¿Por qué el fraude con los criptoactivos es una amenaza emergente? ¿Son una forma para lavar dinero?*

### **Fabio Mauricio Pinzón G.**

Las billeteras digitales de criptoactivos manejan una llave pública que divulgan para poder recibirlos. Sin

embargo, saber quién es el dueño de la billetera es prácticamente imposible sin el consentimiento del dueño. Esto genera un pseudo-anonimato que puede facilitar el lavado de activos.

Por otra parte, falsificar un criptoactivo dada la cantidad de certificados y firmas digitales involucradas, en su emisión y posesión, es una labor de “hacking” extremadamente difícil. Los problemas de pérdida de criptoactivos están asociados principalmente al robo de la llave privada del dueño de los mismos. Por su longitud, esta llave privada normalmente esta guardada en un dispositivo que debe conectarse a internet para poder realizar cualquier pago en criptactivo. De manera similar a la llave privada de los criptoactivos, en Jamaica, por ejemplo, están emitiendo su moneda digital con una tecnología que maneja de una manera supremamente segura la llave privada del Emisor. Firma que será la que, en conjunto con la llave pública, finalmente prueban que es moneda digital emitida por el banco central y no una falsificación.

### **Ana María Zuluaga T.**

Un reto muy grande es cómo los consumidores aprenden de esta tecnología y entienden qué medidas de seguridad deben implementar para almacenar.

### **Julio López M.**

Con relación al fraude sobre la cadena de bloques para modificar

una cantidad o un propietario, considero que este es el punto más fuerte que tiene la tecnología del *blockchain*; por esta razón su éxito, porque no se puede manipular, no se puede falsificar, un bloque una vez que ya esté inscrito, que está metido dentro de la cadena ya no se le puede hacer nada más y de pronto la mejor muestra es que como hemos mencionado hoy en día la cadena de blockchain asociada específicamente con Bitcoin, que es de pronto la más documentada, tiene un tamaño de 350 gb y es pública. Las de todas las monedas son públicas, porque es parte de la definición de estas pseudomonedas: en teoría cualquiera puede “minar”, o sea encriptar el siguiente bloque de la cadena y se hace acreedor a 6 (seis) bitcoins, varios miles de dólares en un solo movimiento.

Los monederos electrónicos que comentaba anteriormente dentro de los riesgos, esos si se pueden probablemente manipular, eventualmente falsificar y hay un mercado negro de venta de monederos de Bitcoin que en mi concepto normalmente son estafas.

Con relación a la pregunta sobre el fraude con los criptoactivos como una amenaza emergente, y como bien lo han mencionado el principal problema, en mi concepto, es que el fraude normal es pagado con criptoactivos. El riesgo que tiene la sociedad es que se incrementa la ocurrencia de fraudes. Como mencionaste el 8% de casos de fraude

se paga con criptomonedas, y en el caso del ransomware o secuestro de datos, creo que el 100% de casos los están pagando con criptoactivos debido al anonimato y basados en las transacciones directas. Importante recordar la existencia del “darkweb”, ya que permite realizar trueques transfronteros sin que las autoridades se den cuenta. En mi concepto el problema principal es que se facilitan las actividades delincuenciales con base en estas seudomonedas.

### Jeimy J. Cano M.



Hay informes recientes de dos ataques a la cadena de blockchain, no para el blockchain público, sino para el blockchain privado donde es mucho más factible. El primero es el ataque del 51% donde crearon un bloque y lo incorporaron de manera exitosa dentro de una blockchain y el segundo un ataque directamente al *timestamp* (marca de

tiempo) para la firma de un nuevo bloque también con éxito. Es tecnología y falla en algún punto. Por tanto, es importante tener clara esta situación y qué precauciones debemos tomar cuando esos elementos no funcionan como están previstos. En una tesis de maestría en Europa se reporta un listado por lo menos de 25 posibles problemas de seguridad asociados con el blockchain.

### Ana María Zuluaga T.

En cuanto a los esquemas defraudatorios y las actividades ilegales con criptoactivos, existentes algunos estudios de entidades privadas que presentan cifras sobre las mencionadas actividades. En todo caso, es importante hacer énfasis en que esto no dista de lo que ocurre con otro tipo de activos, los cuales también tienen relacionados riesgos inherentes a su naturaleza.

### Jeimy J. Cano M.

En el mismo contexto quiero compartir una estadística publicada en el “Reporte a las Naciones” 2022 de la ACFE (*Association of Certified Fraud Examiners*) el cual señala que en el 8% de los casos globales de fraude estuvo involucrado el tema de criptoactivos, de criptomonedas, y entre esos casos, las criptomonedas las usaron para dos cosas: para hacer pagos por extorsiones y para convertirlos en otros activos.

La última pregunta está asociada con el ciudadano y las recomenda-

ciones alrededor del uso de estos criptoactivos. Esto es, ¿qué le podemos decir, ¿cómo lo podemos orientar cuando le hablan de criptoactivos?, ¿qué debe entender, ¿qué debe preguntarse, qué cosas debería tener en la cabeza cuando vienen y le dicen vamos a hablar de estos temas?

### **Ana María Zuluaga T.**

Lo primero es “infórmese, lea, aprenda pregúntese quién es el que se lo está vendiendo”. Si se va a meter en una plataforma que preveía de servicios de criptoactivos, no confíe tan ciegamente en una aplicación que tiene una experiencia de usuario muy bonita y que no gestione los riesgos relacionados con su actividad.

### **Jeimy J. Cano M.**

O sea, no confíe en la magia de los ingenieros.

### **Ana María Zuluaga T.**

Los consumidores también deben tener en cuenta que las operaciones con criptoactivos no cuentan con el Seguro de Depósito de Fogafin, y tampoco garantiza la puesta en marcha de sistemas de atención al cliente.

### **Julio López M.**

Para el ciudadano en general, yo apelaría al concepto de ética. Todas las inversiones ilegales son muy rentables, pero no se trata de enriquecerse, se trata de qué me están vendiendo, a qué estoy yo colaborando, en qué estoy yo par-

ticipando, cuando le dicen a uno que a través del darkweb todas las actividades de compra de drogas, de compra de armas, hay casos de prostitución que se están pagando y que se están manipulando alrededor de la darkweb, con base en esto, yo le diría a la gente: por favor no invierta. El hecho de que sea una inversión rentable no es justificación. Yo recomiendo otras opciones de inversión, como acciones en empresas colombianas; impulsemos empresas, impulsemos los innovadores, impulsemos los nuevos emprendedores, pero por favor no inviertan en seudomonedas.

Hay una supuesta ventaja de las monedas digitales que promocionan ya que no hay que declarar ni pagar impuestos. Creo que cada vez hay más conciencia en que pagar impuestos es la manera de distribuir a la sociedad los beneficios que nosotros tenemos y que hay que hacerlo. Tener una utilidad sin que sea impositiva, es algo que va a cambiar y que la gente también debería considerar. Cierro resaltando que la mayoría de la gente es ética y la mayoría de la gente estaría de acuerdo por esta razón en este tema: no invertir, no comprar monedas digitales.

### **Fabio Mauricio Pinzón G.**

Por el lado de la educación, yo tengo que informarme a quien le compro y qué estoy comprando. Por el lado de la ética, todo lo que yo gano alguien lo está perdiendo. ¿Para mí es ética esa transacción? Puede

ser algo tan simple como que yo gasto mi tiempo, un activo que yo usé, aprendiendo sobre criptoactivos. Educación y criptoactivos son activos que podré usar o gastar en el futuro.

### **Jeimy J. Cano M.**

Dos cosas son claves cuando al ciudadano común le hablan de criptoactivos: educación y ética. En este sentido, el Estado, los reguladores, el banco central deberían trabajar más en esta línea, es decir, hacer mucha más pedagogía de los criptoactivos, para que la gente comience a sensibilizarse acerca de esa realidad que va a estar circulando alrededor y que si bien no va a ser moneda de curso legal, va a estar presente como una tentación permanente. No obstante, en la medida en que las personas estén más informadas y educadas en el tema en torno a cómo funcionan y la ética sobre su uso, podría haber mucho más sentido crítico respecto a esta nueva realidad.

### **Conclusiones:**

#### **Fabio Mauricio Pinzón G.**

Como dijeron Julio y Ana María los criptoactivos son un medio de intercambio digital. Sin importar si son confiables, controlables o regulables, le han dado impulso a las tecnologías que llamamos DLT (*Digital Ledger Technology*), al conocimiento generalizado de criptografía, de llaves, de bloques, de impu- tabilidad, mejor dicho, hasta estructuras de datos nuevas que se crearon, tales como los árboles Merckle

o Patricia. El vaso medio lleno es que este impulso nos obliga a los ingenieros de sistemas a entender todas estas tecnologías que van a manejar nuestra billetera digital.

### **Ana María Zuluaga T.**

Tal como lo dijo Mauricio, es el potencial de la tecnología de registro distribuido y sus casos de uso en diferentes sectores de la economía. Para el sistema financiero ya se identifican múltiples aplicaciones a nivel global relacionados con el manejo de repositorios de información, compensación y liquidación de pagos o estructuración de productos financieros.

La DLT es como el internet en los años 90: una tecnología que viene a cambiar la forma de hacer las cosas y el desafío es aprender sobre sus beneficios y su funcionamiento, sin desconocer los riesgos involu- crados. Pensemos en los años 90



cuando se hablada del correo electrónico y cómo ese concepto y uso fue tan disruptivo para la sociedad. Hoy 20 años después, el correo electrónico es un medio de comunicación que está incorporado en el día a día de las personas. Lo mismo ocurre con el tema DLT, cripto y blockchain, pasaran unos años y nos vamos a habituar a eso bajo reglas de juego claras definidas por los gobiernos y la sociedad.

### Julio López Medina



Gracias Jeimy. No es fácil tratar de concluir, de pronto me voy a pegar

un poco a la reflexión que hacías sin desconocer lo que se ha comentado, lo que comentaban tanto Mauricio como Ana María, con relación a las ventajas específicas del blockchain. La tecnología del blockchain es un salto que nosotros todavía no hemos visto en aplicaciones comerciales y aplicaciones del día a día; creo que nos hemos dejado como oscurecer un poquito, por eso nos hemos retenido, nos hemos quedado únicamente en las monedas digitales, pero el potencial que tenemos de desarrollo del blockchain es muy alto y tenemos que trabajarle.

Y el otro tema es el de la educación de la gente que tu comentabas, tenemos que trabajarle mucho a la capacitación en general de todas las personas para que entendamos entre todos un poco más lo que son estos activos digitales y lo que representan; lo más importante es que no haya frustraciones por parte de las personas, y que sepan claramente en que se están metiendo. La educación es clave como comentaba Ana María y tenemos que trabajar principalmente en informar y en capacitar. 🌐

**Sara Gallardo M.** Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas Uno y Cero, Gestión empresarial y Acuc Noticias. Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Coautora del libro "Lo que cuesta el abuso del poder". Ha sido corresponsal de la revista Infochannel de México; de los diarios La Prensa de Panamá y La Prensa Gráfica de El Salvador y corresponsal de la revista IN de Lanchile e investigadora en publicaciones culturales. Se ha desempeñado también como gerente de Comunicaciones y Servicio al Comensal en Inmaculada Guadalupe y amigos en Cía. S.A. (Andrés Carne de Res) y editora de Alfaomega Colombiana S.A.; En la actualidad es asesora y editora en escritura y producción de libros. Es editora de esta revista.

# Criptoactivos

DOI: 10.29236/sistemas.n163a6

*Deconstruyendo los bienes, los valores y los medios de pago en un contexto digital.*

## Resumen

La acelerada innovación financiera habilitada por cuenta de la transformación digital de la experiencia de los clientes ha llevado tanto al sector bancario como a la sociedad en general a repensar la manera como se adquieren los bienes, cómo se concreta la experiencia del valor y cómo se constituyen los medios de pago. La emergencia sanitaria internacional con las restricciones impuestas por los contagios y las tensiones internacionales por cuenta de la inestabilidad geopolítica y los conflictos actuales, han marcado la agenda del desarrollo de los criptoactivos, los cuales se configuran como el nuevo referente de la desintermediación financiera. Este artículo desde una perspectiva académica y práctica hace una revisión conceptual de esta temática y analiza al menos siete tendencias que van transformar la dinámica de la sociedad actual en el mediano plazo, para reflexionar y anticipar posibles tendencias que terminen cambiando el status quo del mundo actual.

## Palabras claves

Criptoactivos, NFT, DeFi, Blockchain, DLT

Jeimy J. Cano M.

## Introducción

En un mundo de acelerada transformación digital, con mayor inte-

racción y negocios a través de la tecnología, se advierte una necesidad creciente de una menor inter-



mediación de los actores naturales como son las instituciones bancarias, comoquiera que ahora las personas pueden intercambiar valor entre ellas con mayor confianza y menor costo usando implementaciones tecnológicas recientes y novedosas como la cadena bloques (*blockchain*) basadas en la tecnología digital de libro mayor (*Digital Ledger Technology* – DLT).

Estas tecnologías como el DLT habilitan a las personas para realizar simultáneamente actividades financieras anónimas o seudónimas sin control centralizado, devolviendo a los participantes la responsabilidad de sus transacciones. Esta tendencia que se ha venido consolidando desde la crisis financiera de 2008, cuando surgen las criptomonedas como respuesta para proteger el valor o poder adquisitivo, crea nuevos retos para el sistema financiero actual que poco a poco pierde su lugar como intermediario natural de confianza, para que la tecnología basada en sistemas criptográficos y con bajos costos por transacción posicionen una nueva realidad en la dinámica de los negocios del mundo.

Esta nueva forma de intercambio digital habilitada por la tecnología DLT, donde los participantes pueden verificar cada transacción y confiar en el sistema, habilitan una economía global basada en “tokens” (testigos o fichas - estructuras de datos que pueden ejecutar transacciones de forma fiable sin

supervisión humana) con billeteras electrónicas, donde cada persona puede movilizar inversiones, hacer pagos, o generar un depósito de valor o constituir un instrumento financiero de carácter especulativo, que le permita crear negocios antes desconocidos y retadores que pueden escapar a los radares de los supervisores del mercado financiero global (BCG, 2021).

En este sentido, hablar de criptoactivos es concretar un movimiento global de negocios financieros y sociales que se caracterizan por su volatilidad, la descentralización, la desintermediación y deslocalización tanto de las personas como de los productos, que buscan crear un nuevo espacio de negociación entre pares, con el fin de darle mayor responsabilidad a los participantes en las transacciones, para lo cual la tecnología DLT actúa como garante de la interacción tanto en su registro como en su seguimiento y aseguramiento.

Por tanto, este artículo explora los fundamentos conceptuales de los criptoactivos y analiza al menos siete tendencias del uso de la tecnología DLT que a la fecha vienen avanzando a nivel internacional y, que prometen cambiar la dinámica de la actividad financiera mundial y así, comenzar una transición de las tradicionales lecturas de valor, a nuevas propuestas basadas en tecnología donde se habilitan estructuras de datos e infraestructuras tecnológicas para un intercam-

bio digital que para algunos podrían asemejarse a bienes muebles digitales.

### ¿Qué es un criptoactivo? Fundamentos conceptuales

Empecemos por desglosar la palabra “criptoactivo”. La primera parte de la palabra, “cripto”, significa “oculto” o “secreto”, lo que refleja la tecnología criptográfica utilizada para registrar quién es dueño de qué y para realizar pagos entre usuarios. La segunda parte de la palabra, “activo”, nos habla de un elemento u objeto que tiene la capacidad de almacenar, transferir, acumular o generar valor a su dueño, lo que le permite habilitar transacciones y movimientos de intercambio con iguales o terceros concretando una dinámica de comercio particular asociada con bienes o servicios (Bank of England, 2020).

Una definición más técnica para los criptoactivos, serían activos digitales, registrados en un libro mayor digital (DLT), que utiliza técnicas criptográficas para crear y asegurar nuevos registros, el consenso distribuido para asegurar y validar las transacciones, una red de pares (Peer to Peer - P2P) como infraestructura tecnológica para su interacción y los contratos inteligentes (*smart contracts*) para crear, realizar y verificar transacciones de forma descentralizada (Arkhyphenko, 2020).

Estos criptoactivos, que representan a la fecha un desafío para las

políticas monetarias, fiscales y bancarias estatales e internacionales, tienen entre otras las siguientes características que las hacen atractivas y populares en estos momentos: (Arkhyphenko, 2020)

- Crean sistemas de pagos descentralizados.
- Aumenta el control de las personas sobre su activo.
- Cuenta con un nivel aceptable de anonimato en las transacciones.
- Aumenta transparencia de las operaciones.
- Disminuye los costos en las transacciones.

Las polémicas que se presentan a la fecha a nivel internacional sobre el uso de los criptoactivos, no han permitido consensuar una definición concreta. Su naturaleza novedosa no facilita encuadrarla en un marco regulatorio específico lo que hace que se creen incertidumbres alrededor de su tratamiento y falta de confianza tanto en el público como en los reguladores para aceptar o motivar la dinámica de estos nuevos activos digitales.

De acuerdo con la literatura reciente, los criptoactivos jurídicamente se pueden clasificar en una taxonomía básica funcional como sigue: (Sanz, 2021)

- *Bienes muebles digitales*: bien susceptible de apropiación y que se pueden transportar o mover. Bienes de los que se puede

hacer un uso adecuado sin que se consuman, siendo no fungibles.

- *Valores mobiliarios digitales*: un título electrónico que para que su titular se le reconozca una cantidad de dinero, deberá acceder a una plataforma virtual para ofrecer sus criptoactivos en un mercado y obtener un reembolso en dinero fiduciario.
- *Medio de pago*: Poseen un atributo que se les asemeja al que tiene el dinero fiduciario de curso legal, con la característica de que no existe ningún banco central detrás de su funcionamiento o control.

Considerando lo anterior, en Colombia los supervisores del mercado financiero y las autoridades monetarias han venido adelantando reuniones de trabajo donde han dejado claras sus posiciones sobre el tema de los criptoactivos en el país.

Algunas de sus reflexiones a la fecha son: (Banco de la República, 2019)

- No es moneda:
- El peso colombiano (billetes y monedas) es la unidad monetaria y de cuenta del país, siendo el único medio de pago con poder liberatorio ilimitado.
- No es divisa:
- No cuentan con el respaldo o la participación de los bancos centrales.
- No han sido reconocidas como moneda legal de ningún país.

- No son reconocidas por el régimen cambiario colombiano como divisas.
- No son valor:
- No se les ha reconocido la calidad de instrumento financiero.
- No se les ha reconocido la calidad de derecho de contenido patrimonial.
- Tienen riesgo de ser usadas para captación de recursos del público.

Con estos fundamentos básicos desarrollados, sabiendo que las controversias desde el punto de vista de su uso y despliegue en el contexto de la dinámica de las naciones seguirán, en la orilla de la tecnología se advierten avances y tendencias de interés, que abrirán zonas novedosas para negocios y potenciarán posibilidades emergentes ahora con el concepto del Metaverso (Gupta, 2022), donde se esperan se transformen las realidades actuales y se potencie el uso de los criptoactivos.

### **Siete tendencias en el uso de la tecnología DLT. Una mirada en prospectiva**

De acuerdo con un estudio reciente del *Boston Consulting Group* (BCG, 2021), se advierten siete tendencias claves del uso de la tecnología DLT que retarán las actividades financieras y la dinámica global de las transacciones habida cuenta de una mayor aceptación por parte de la gente de los criptoactivos, una desmitificación acelerada de la tecnología que lo soporta

y el uso actual y masificación que se viene haciendo por parte no sólo de los inversionistas tradicionales, sino ahora de los artistas con los “Testigos no fungibles” (*Non Fungible Tokens – NFT*).

Las siete tendencias son: (BCG, 2021)

- *Contratos inteligentes*. Implementaciones digitales de acuerdos formales.
- *Ofertas iniciales de monedas*. Métodos alternativos para la obtención de fondos para empresas emergentes.
- *Tokens digitales respaldados por activos*. Criptodivisas negociables vinculadas a otras fuentes de valor.
- *Monedas digitales de bancos centrales* (Central Bank Digital Currencies - CBDCs). Propuestas de nuevas criptodivisas con respaldo nacional.
- *Tokens no fungibles* (NFT). Tokens de criptodivisas con su propio valor inherente.
- *Finanzas descentralizadas*. Aplicaciones bancarias y financieras basadas en blockchain.
- *Servicios de asesoramiento automatizado*. Orientación y apoyo automatizados para la actividad DLT.

Los “*contratos inteligentes*”<sup>1</sup> de acuerdo con el Banco Central Europeo son “arreglos de tipo contractual incorporados en un software que este último puede validar,

ejecutar y grabar de manera automática en una plataforma de tecnologías de registro distribuido (DLT), tan pronto como se cumplan ciertas condiciones preprogramadas y acordadas por humanos” (Athanassiou, 2017). Estos contratos tienen las siguientes características: (Chen et al., 2018)

- Incluyen intereses financieros y económicos
- Son impulsados por eventos.
- Cuentan con un historial de transacciones y resultados de la ejecución del contrato
- Se registran utilizando el libro de contabilidad distribuido (DLT).
- No tienen ninguna persona de confianza centralizada.
- Se basan en el consenso.

Ahora esta nueva realidad de la manifestación de la voluntad cuenta con un código programado que contiene las condiciones concretas de la validación de las obligaciones de las partes, las cuales se ejecutan y satisfacen una vez se ha materializado dicha condición, sin necesidad de la intervención humana. Si bien es una alternativa novedosa para materializar contratos como el de seguros, de arrendamiento, entre otros, cuenta con limitaciones y retos importantes que se deben tener en cuenta de cara a su evolución y puesta en operación: (Bambara & Allen, 2018)

---

<sup>1</sup> Concepto desarrollado por Szabo, 1996.

- *Los contratos a menudo incluyen conceptos de juicio subjetivo, razonabilidad y buena fe, conceptos no pueden traducirse fácilmente en afirmaciones lógicas.*
- *Si algo sale mal en la ejecución del contrato y alguien sufre una pérdida, ¿a dónde se recurre?*
- *¿Cómo se deshacen las transacciones que no deberían haber ocurrido o si se trata de un contrato que por alguna razón (o en algún lugar) es ilegal o infringe los requisitos normativos?*
- *¿Qué pasa si las partes no quieren que se divulguen los detalles?*
- *No hay una autoridad administrativa central para resolver una disputa.*

La oferta inicial de moneda (ICO – *Initial Coin Offering*) es el ofrecimiento de “fichas” o “testigos” o tokens digitales, en los que se acumula valor, que son ofrecidas a inversionistas que los adquieren pagando con criptoactivos, siendo los más utilizados los bitcoins o los etherums (Blanco, 2022, p.520).

Esta oferta de acuerdo con Blanco (2022, p.521) puede tener dos objetivos:

- Ofrecer la moneda como activo por sí mismo, de manera que se usaría como medio de pago, con valor propio intrínseco, o
- Ofrecer tokens, que les dan a los tenedores participaciones sobre el emisor, sin valor directo, pero

con derechos de cobro sobre dicho emisor, o un derecho para adquirir bienes o servicios producidos por la respectiva empresa.

El uso más frecuente de esta alternativa en la actualidad se hace a través del *crowdfunding*, que se define como un “mecanismo de recaudo de recursos para la financiación de un proyecto a través de una plataforma de internet que se encarga de publicar el proyecto, así como del recaudo y pago de los recursos que aporten los inversionistas” (Padilla, 2022, p.151). Este tipo de iniciativas tiene beneficios y riesgos que se mencionan a continuación: (Padilla, 2022, pp.156-160)

- Beneficios:
  - A la economía – promueve la competencia dentro de los mercados financieros: motiva la innovación y prestación de servicios financieros más eficientes y menos costosos.
  - A los receptores – acceso a recursos financieros a menor costo respecto de la banca tradicional o el mercado público de valores.
  - A los aportantes – diversificación de portafolios de inversiones al ofrecer gran multiplicidad de proyectos en los cuales invertir su dinero.
- Riesgos
  - Conlleva riesgo sistémico consistente en un colapso genera-

lizado de un sistema o de un mercado.

- La inhabilidad o dificultad que tiene un inversionista de obtener liquidez de una inversión una vez hace parte de ella.
- La contingencia de pérdida por el incumplimiento de las obligaciones de los receptores, esto es, los receptores pueden llegar a un estado de insolvencia.
- La pérdida de cartera de los inversionistas derivada de problemas técnicos que se puedan presentar en las plataformas electrónicas, que pueden llevar a cierres temporales o permanentes de las mismas.

Los *tokens digitales respaldados por activos*, son criptoactivos que están asociados con criptomonedas estables, las cuales son una apuesta en medio de la volatilidad de las criptomonedas como el bitcoin, que trata de resolverse con emisores limitados y un valor referenciado al dinero fiduciario de curso legal, esto es, una moneda tradicional como puede ser el euro, el dólar, el yen, entre otras, mediante una reserva que le sirva de respaldo. Lo que en últimas se busca con esta estrategia es reducir las oscilaciones de su cotización, para generar mayor confianza en sus potenciales usuarios (Sanz, 2021).

Estos tokens particularmente aquellos colateralizados (con respaldo externo, y los no colateralizados, es decir basados en algoritmos para evitar las fluctuaciones

de precio) no cuentan con una red de seguridad frente a movimientos drásticos que pueden obligar a las divisas estables a vender a cualquier precio sus colaterales (bonos, pagarés, metales preciosos, entre otros). Lo anterior puede generar un riesgo de contagio que varía según el tamaño, la liquidez y el riesgo de sus tenencias de activos, así como la transparencia y la gobernanza del operador, entre otras cosas (Nieves, 2021).

Frente a esta tendencia los bancos centrales han venido avanzando en el desarrollo de sus monedas digitales (*Central Bank Digital Currencies – CBDC*) con el fin de movilizar sus esfuerzos para contar con emisiones de dinero digital estable, el cual estaría sujeto a la política monetaria del banco emisor, que fue lo que precisamente motivó la desconfianza y, por ende, el surgimiento de las criptomonedas.

A continuación, se presenta una vista de la taxonomía del dinero desarrollada por el Banco de Pagos Internacionales (*Bank of International Settlements – BIS*) (BIS, 2018), que ubica al CBDC frente a las cuatro propiedades básicas del dinero: emisor (BC-Banco Central u otro), forma (digital o física), accesibilidad (universal o restringida) y tecnología (basada en cuentas o tokens).

Los retos claves que tiene la banca central frente a sus CBDC son: (Elliot & De Lima, 2021)

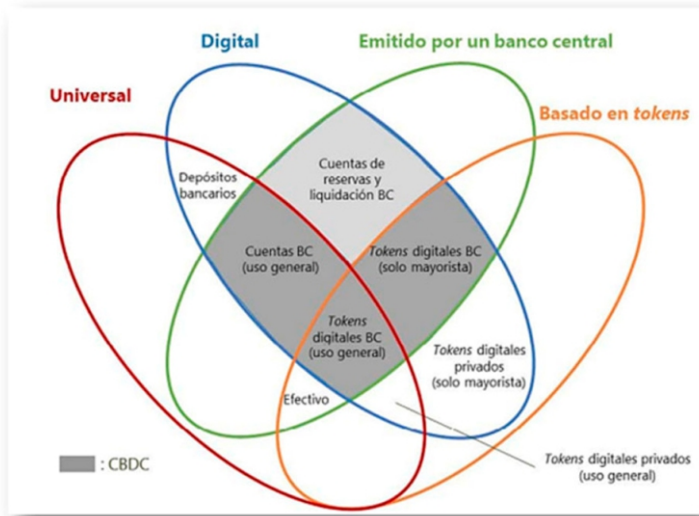


Figura 1. Taxonomía del dinero (Tomado de: BIS, 2018, p.6)

- Disminución del uso del efectivo.
- Pagos más rápidos, sostenibles y resistentes.
- Aumentar inclusión financiera.
- Aumento de monedas digitales del sector privado.
- Mejorar proceso de pagos transfronterizos.
- Reducción del fraude y actividades ilícitas.
- Facilitar innovación y competencia abierta.

De otra parte, se encuentran los *tokens no fungible* o NFT. Para comprender este concepto es importante saber qué es un bien fungible y uno no fungible. Un bien fungible es aquel que es intercambiable teniendo un valor en función de su número, medida o peso. Y los bienes no fungibles son los que no

son sustituibles. Un bien fungible es el dinero. Si tienes un billete de \$10000 pesos colombianos lo puedes intercambiar por otro de \$10000 o dos de \$5000, no pierde valor y es exactamente igual.

Adicionalmente, el billete o billetes se consumen una vez se usan. Un bien no fungible es una obra de arte, el cual no se consume al utilizarse y tampoco puede sustituirse por otro cuadro. No existe equivalencia entre una obra de arte y otra, son de carácter único (Fernández, 2022).

Así las cosas, un NFT, es un activo único que no se puede modificar ni intercambiar por otro que tenga el mismo valor, ya que no hay dos NFT que sean equivalentes. A los

NFT, se les asigna una especie de certificado digital de autenticidad, una serie de metadatos que no se van a poder modificar. En estos metadatos se garantiza su autenticidad, se registra el valor de partida y todas las adquisiciones o transacciones que se hayan hecho, y también a su autor, todo en un registro contable digital distribuido (Fernández, 2022).

A la fecha si bien han adquirido gran relevancia y movilidad dado que se cotizan dependiendo de lo que las personas quieren pagar por ellos, lo que puede generar una gran rentabilidad al igual que una gran volatilidad, la seguridad propia de los monederos electrónicos que se utilizan suelen ser la parte más vulnerable para que agentes agresores concreten robos que terminen con la dinámica de compra-venta que implica el uso de estos tokens.

Finalmente, las finanzas descentralizadas (*Decentralized Finance* DEFI). De acuerdo con el Foro Económico Mundial las DEFI tienen como objetivo transformar las formas tradicionales de financiación mediante la reconstrucción y reinención de los servicios. En este sentido son contratos financieros (préstamo e inversión) basados en DLT y, por tanto, anotados en una cadena de bloques inmutable. Una compañía de finanzas descentralizada es un conjunto de sistemas que permite intercambiar valor ('tokens') de un punto A un punto B (en-

tre monederos) sin intermediarios (WEF, 2021).

Los defensores de las DEFI dicen que puede resolver los problemas del sistema financiero tradicional. La tecnología de código abierto, las recompensas económicas, los contratos inteligentes programables y la gobernanza descentralizada podrían ofrecer una mayor eficiencia, oportunidades de inclusión, una rápida innovación y acuerdos de servicios financieros totalmente nuevos, que abren posibilidades para propuestas innovadoras que cambien la dinámica financiera actual.

Por otro lado, existen voces de advertencia sobre el uso de las finanzas descentralizadas que plantean consideraciones relacionadas con la protección del consumidor, la pérdida de fondos, las complejidades de la gobernanza, el riesgo técnico y el riesgo sistémico, donde a la fecha ya se han registrado incidentes relevantes relacionados con fallos técnicos y ataques a los servicios DEFI.

### **Reflexiones finales**

La emergente industria de los criptoactivos es fuente permanente de innovación, de oportunidades y riesgos potenciales entre las distintas iniciativas como las mencionadas en esta reflexión. Estas distintas iniciativas generalmente responden a un ecosistema experimental de servicios financieros que están sustentados en la tecnología de libro contable digital distribuido



(DLT), la cual implica el reconocimiento de diferentes participantes, la creación de confianza entre ellos, el consenso, la transferencia de valor y el aseguramiento de las transacciones.

De acuerdo con Feyen et al. (2022) el volumen total de criptoactivos en los últimos dos años aumentó hasta un total de 2,8 billones de dólares solo en la primera mitad de 2021. En esta línea los volúmenes en ether (40%) y stablecoins (24%) han ganado más cuota con el tiempo en comparación con el bitcoin (24%). DEFI y otros criptoactivos representan el 12%. Al observar la actividad de las criptomonedas por el tamaño de las transacciones, encontramos que las transferencias de gran valor (2,68 billones de dólares) resultan de menor tamaño (128.000 millones de dólares), lo que sugiere un papel desproporcionadamente grande de la actividad institucional.

Este escenario creciente de innovación financiera demanda de los reguladores estrategias concretas para habilitar nuevas propuestas y espacios de experimentación que permitan desarrollar este mercado.

Los areneros de experimentación o *sandbox* regulatorios establecen espacios de innovación regulatoria donde se puede diseñar, expedir, probar y analizar regulación experimental, de tal manera que se pueda determinar el impacto de la iniciativa en un entorno controlado, lo

que permite estudiar en detalle la dinámica de la innovación y, luego de cumplir con los trámites y autorizaciones requeridas, concretar las normas que regirán para el desarrollo de las propuestas novedosas (Castaño & Ocampo, 2021).

Todos estas iniciativas revisadas en este documento, adicionalmente a las consideraciones regulatorias necesarias para su despliegue, deberán mantener en foco que toda propuesta que se articule con la tecnología DLT deberán ser diseñadas desde la ética, la seguridad y la privacidad desde el diseño y por defecto, pues el uso de estos sistemas se expone a retos de transparencia, responsabilidad, control y explicabilidad de las interacciones de sus diferentes componentes que pueden llegar a vulnerar los derechos humanos y desafiar la intervención del Estado en la economía (Castaño & Ocampo, 2021).

Los avances recientes reportados alrededor del concepto del Metaverso representan una combinación de múltiples tecnologías y tendencias requeridas para su funcionamiento. Entre las capacidades tecnológicas que contribuyen en esta dirección se encuentran la realidad aumentada (RA), los estilos de trabajo flexibles, gafas de visualización, una nube de RA, el Internet de las cosas (IoT), el 5G, la inteligencia artificial (IA) y las tecnologías espaciales. El Metaverso se puede considerar como la siguiente versión de internet, un espacio vir-

tual compartido, donde es viable desarrollar una vida donde es posible: (Gutpa, 2022)

- Compra de trajes y accesorios para avatares en línea
- Compra de terrenos digitales y construcción de casas virtuales
- Participar en una experiencia social virtual
- Comprar en centros comerciales virtuales a través del comercio inmersivo
- Utilizar aulas virtuales para experimentar un aprendizaje inmersivo
- Comprar arte digital, objetos de colección y activos (NFT)
- Interactuar con seres humanos digitales para la incorporación de empleados, el servicio al cliente, las ventas y otras interacciones comerciales

Entre otras actividades, donde los criptoactivos serán parte natural de la dinámica económica que se desarrollará en un escenario digital que apenas se inicia a reconocer y experimentar.

Así las cosas, los criptoactivos se convierten en la nueva frontera de investigación, análisis, experimentación y uso que deberá ser parte de las agendas académicas, ejecutivas y gubernamentales, cualquiera que se convierten en un habilitador de una nueva realidad digital donde emerge una dinámica social distinta, se transforman las prácticas económicas y la conceptualización del valor, así como la

reinención del concepto de propiedad que ya no estará atado a un concepto físico, sino a un conjunto de algoritmos y estructuras de datos que representan a una figura humana con nombre, vida y relacionamiento social denominado avatar.

## Referencias

- Arkhyphenko, I. (2020). Theoretical and legal perspective of civil liability in cryptocurrency relations. *Master Thesis*. Taras shevchenko National University of Kyiv. Faculty of law. Civil Law Department. <https://doi.org/10.13140/RG.2.2.20658.02247>
- Athanassiou, P. (2017). Impact of digital innovation on the processing of electronic payments and contracting: an overview of legal risks. European Central Bank. *Legal Working Paper Series*. <https://www.ecb.europa.eu/pub/pdf/scplps/ecb.lwp16.en.pdf>
- Bambara, J. & Allen, P. (2018). *Blockchain. A Practical Guide to Developing Business, Law, and Technology Solutions*. New York, USA: McGraw Hill
- Banco de la República (2019). Criptoactivos: análisis y revisión de literatura. *Ensayos sobre política económica*. No.92. 1-37. <https://repositorio.banrep.gov.co/handle/20.500.12134/9766>
- Bank of England (2020). What are cryptocurrencies. <https://www.bankofengland.co.uk/knowledgebank/what-are-cryptocurrencies>
- BCG (2021). Seven trends at the frontier of blockchain banking. *Report*. <https://www.bcg.com/publications/202>

- 1/trends-at-the-frontier-of-blockchain-banking
- assets-evolution-and-macro-financial-drivers
- BIS (2018). Monedas digitales emitidas por bancos centrales. Comité de Pagos e Infraestructuras de Mercado. Comité de Mercados.  
[https://www.bis.org/cpmi/publ/d174\\_es.pdf](https://www.bis.org/cpmi/publ/d174_es.pdf)
- Blanco, C. (2021). Ofertas públicas iniciales de moneda (OPM). Entre la innovación tecnológica y la innovación. En López, L., Baquero, M. & Corredor, J. (eds.) (2021). *Los mercados financieros ante la disrupción de las nuevas tecnologías digitales*. Bogotá, Colombia: Universidad Externado de Colombia. 519-550
- Castaño, D. & Ocampo, S. (2021). Innovación Fintech & Start-ups. En López, L., Baquero, M. & Corredor, J. (eds.) (2021). *Los mercados financieros ante la disrupción de las nuevas tecnologías digitales*. Bogotá, Colombia: Universidad Externado de Colombia. 33-93
- Chen, L., Gao, Z. & Shi, W. (2018) Tyranny of the Majority: On the (Im)possibility of Correctness of Smart Contracts. *IEEE Security & Privacy*. 16. 30-37. DOI: 10.1109/MSP.2018.3111240
- Elliot, D. & De Lima, L. (2021). Central bank digital currencies. Six policy mistake to avoid. *Oliver Wyman Report*.  
<https://www.oliverwyman.com/our-expertise/insights/2021/jun/central-bank-digital-currency-and-the-policy-mistakes-to-avoid.html>
- Fernández, Y. (2022). *Que son los NFT y cómo funcionan*.  
<https://www.xataka.com/basics/que-nft-como-funcionan>
- Feyen, E., Kawashima, Y. & Mittal, R. (2022). The ascent of crypto assets: Evolution and macro-financial drivers. *Voxeu CEPR*.  
<https://voxeu.org/article/ascent-crypto>
- Gupta, A. (2022). What is a metaverse. *Gartner Insights*.  
<https://www.gartner.com/en/articles/what-is-a-metaverse>
- Nieves, V. (2021). ¿Qué hay detrás de las stablecoins? Los riesgos que oculta el boom de tether y otras divisas estables. *El Economista*.  
<https://www.eleconomista.es/mercados-cotizaciones/noticias/11422199/10/21/Que-hay-detras-de-las-stablecoins-Los-riesgos-que-oculta-el-boom-de-las-divisas-estables.html>
- Padilla, J. (2021). Regulación del Crowdfunding en Colombia: crítica y propuestas. En López, L., Baquero, M. & Corredor, J. (eds.) (2021). *Los mercados financieros ante la disrupción de las nuevas tecnologías digitales*. Bogotá, Colombia: Universidad Externado de Colombia. 147-184
- Sanz, P. (2021). Criptomonedas: naturaleza jurídica y regulación europea de los proveedores de servicios de cambio y de custodia de monederos electrónicos. En López, L., Baquero, M. & Corredor, J. (eds.) (2021). *Los mercados financieros ante la disrupción de las nuevas tecnologías digitales*. Bogotá, Colombia: Universidad Externado de Colombia. 331-390
- Szabo, N. (1996). Smart Contracts: Building Blocks for Digital Markets. *EXTROPY: The Journal of Transhumanist Thought*. 16.  
[https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart\\_contracts\\_2.html](https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html)
- WEF (2021). Decentralized Finance (DeFi) Policy-Maker Toolkit. *White Paper*.  
[https://www3.weforum.org/docs/WEF\\_DeFi\\_Policy\\_Maker\\_Toolkit\\_2021.pdf](https://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf)

**Jeimy J. Cano M., Ph.D, CFE, CICA.** Ingeniero y Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Especialista en Derecho Disciplinario, Universidad Externado de Colombia; Ph.D en Business Administration, Newport University, CA. USA. y Ph.D en Educación, Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.

# Monedas digitales

DOI: 10.29236/sistemas.n163a7

*Protocolos de consenso y consumo de energía: Impacto y retos medioambientales de las criptomonedas.*

## Resumen

A pesar de su naturaleza totalmente digital, el mercado de criptomonedas está suscitando amplio debate por su impacto medioambiental, dada el altísimo consumo de energía requerido para su funcionamiento y la resultante huella de carbono. No obstante, el volumen de demanda energética no es una característica propia de las criptomonedas, sino principalmente un resultado de los más difundidos protocolos de consenso deliberadamente seleccionados, como el *Proof-of Work (PoW)*. En el presente artículo se presentan cifras que sustentan el impacto medioambiental de las monedas digitales, al tiempo que se genera una reflexión alrededor de protocolos alternativos de consenso, como el *Proof of Stake (PoS)* o el *Proof-of-Authority (PoA)*, que llevan a la distinción entre criptomonedas “sucias” y “limpias”, concluyendo que la efectividad técnica del *blockchain* debe ser complementada por el fomento de la sostenibilidad medioambiental.

## Palabras clave

Criptomonedas, Bitcoin, protocolo de consenso, consumo de energía, impacto ambiental, sostenibilidad.

## 1. Introducción

Uno de los tantos aspectos que suscita debate en el contexto de las criptomonedas es su impacto medioambiental, ya que, a pesar de que su naturaleza es totalmente digital, es necesario el uso de importantes cantidades de energía para su producción, intercambio y control (Giudici et al., 2020). Si bien es cierto que en su primera la atención se centró en la eficiencia técnica, una de las grandes preocupaciones actuales es la que tiene que ver con el impacto sobre el entorno, llevando a que la sostenibilidad sea uno de los aspectos centrales que se desea conseguir en el mercado de criptoactivos y, en general, en la industria *blockchain* (Quang et al., 2022). Este hecho lleva a que hoy en día sea necesario evaluar su sostenibilidad medioambiental, principalmente mediante su eficiencia energética, para lo cual es un requisito medir el consumo que implica su creación, transacción, vigilancia y mantenimiento de bloques de información (Iberdrola, 20-21).

Ahora bien, el alto consumo de energía realizado por los sistemas de criptomonedas no es una característica obligatoria de los mismos, sino que es el resultado del mecanismo más tradicional de producción y administración, que en el caso de activos como el Bitcoin corresponde con un esquema de competencia entre algoritmos en

un entorno de complejos acertijos criptográficos. No obstante, como se analiza en el presente artículo, es posible utilizar otros mecanismos, también robustos en lo técnico y, principalmente, muy eficientes en cuanto al consumo de energía. Tales mecanismos reciben el nombre genérico de “protocolos de consenso”, los cuales, según Hyland-Wood y Johnson (2022) son procesos por los cuales una cadena de bloques forma un acuerdo entre sus nodos y reconoce que ese consenso ha sido logrado.

El objetivo de este documento es aportar al debate actual sobre el impacto en términos de uso de energía que generan las criptomonedas, para lo cual ha sido dividido en cuatro secciones, a saber: en la primera se hace una introducción general, en la segunda se describe la historia reciente y el estado actual del mercado de criptomonedas, con énfasis en su consumo de energía y la huella de carbono que genera, en la tercera se diferencia entre criptomonedas “sucias” y “limpias”, al tiempo que se exponen las ventajas de protocolos de consenso alternativos, para finalizar en la cuarta sección con reflexiones a manera de conclusión.

## 2. Las criptomonedas: consumo de energía e impacto medioambiental

En 2018 apareció en el mercado Bitcoin, la primera moneda digital

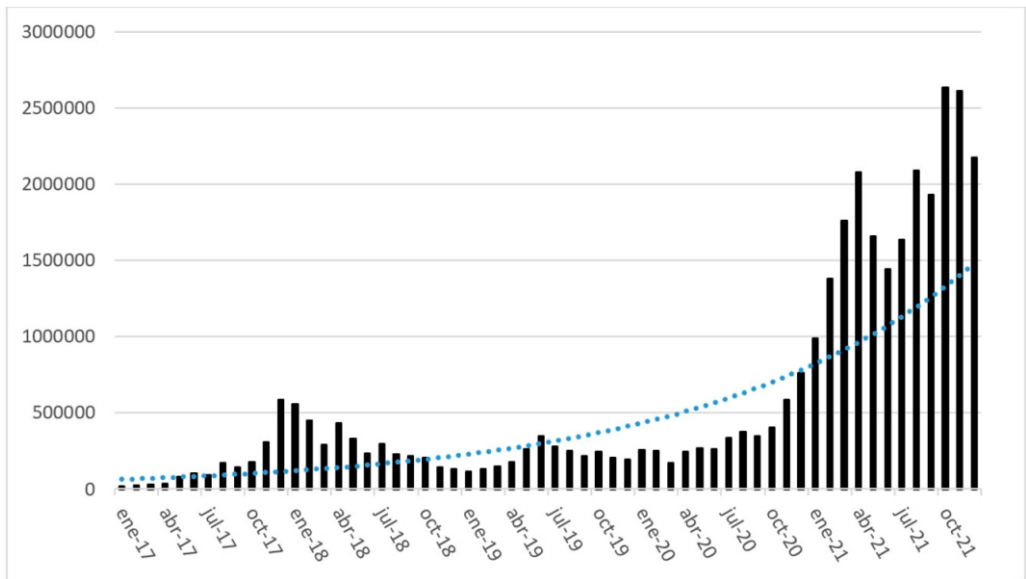
descentralizada de la historia, una “*versión electrónica del efectivo que permitiría enviar pagos online de una parte a otra sin ir a través de una institución financiera*” (Nakamoto, 2008, p. 1). Solamente 13 años después, a cierre de 2021, había más de 1000 diferentes criptomonedas en circulación y cerca de 7000 criptoactivos, incluyendo *tokens* y *stablecoins*, con un valor superior a los 2.2 millones de millones de dólares estadounidenses (CoinMarketCap, 2022), como se puede observar en la Gráfica 1.

En un primer momento, la atención se centró en los aspectos técnicos de las criptomonedas, principal-

mente para llegar a mecanismos que permitieran una mayor eficiencia y seguridad de su producción, su intercambio y su administración. Sin embargo, con el paso del tiempo y la masificación de tales actividades, se empezó a generar preocupación en el público a nivel global al conocerse las cifras relacionadas con el consumo de energía realizado por el mercado de criptoactivos y su correspondiente impacto medioambiental.

En general, el control de cada criptomoneda se realiza gracias a una base descentralizada, en la que una cadena de bloques actúa como libro mayor abierto al público, con

**Gráfica 1.** Capitalización de mercado del mercado de criptodivisas, 2017-2021, total global en millones de dólares (barras) y línea de tendencia (puntos).



Fuente: realización propia a partir de Digiconomist (2022).

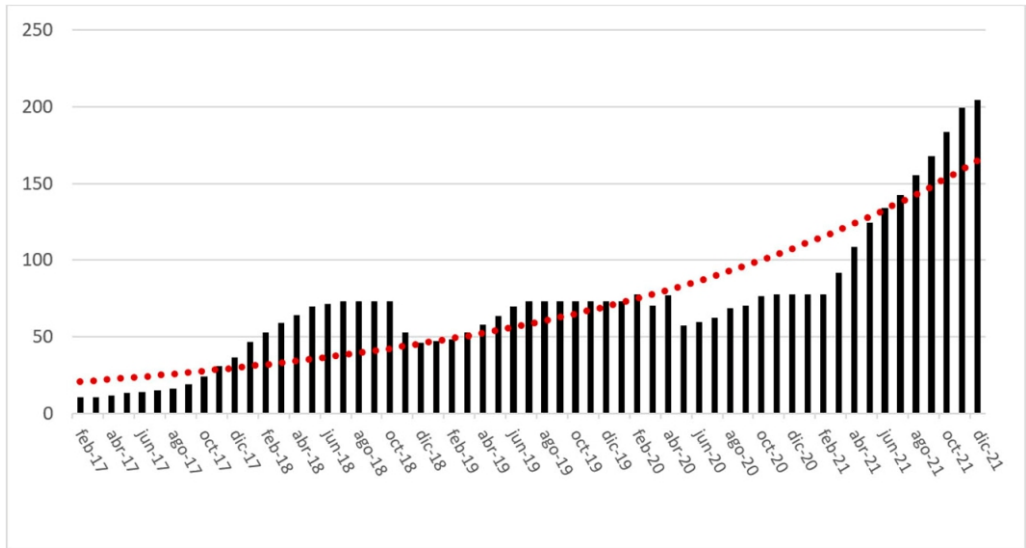
información que se almacena en múltiples terminales conectadas en tiempo real, en una red electrónica en la que poderosos computadores llevan a cabo un complejo protocolo de validación denominado *data mining* o “minería de datos” (Chan et al., 2020; Claeys & Demertzis, 2021). De manera particular, el proceso de validación o minería de Bitcoin, realizado en dispositivos altamente especializados que trabajan con el algoritmo SHA-256, consume una inmensa cantidad de energía.

Al ser una moneda descentralizada, no es posible contar con estadísticas únicas o consolidadas sobre el consumo de energía realizado por el mercado de criptoactivos

(de Vries, 2020), por lo cual diversas fuentes como Digiconomist y Cambridge Bitcoin Electricity Consumption Index, CBECI llevan a cabo sus propias estimaciones (Li et al., 2018).

Entre los datos disponibles, el portal Statista (2022) muestra que el consumo de energía para realizar una transacción de una unidad de Bitcoin es de 2.188,59 kilovatios/hora, misma cantidad de energía que requiere la realización de 1'472.509 transacciones con tarjeta de crédito, monto que a su vez es equivalente al consumo total de energía de una familia estadounidense promedio durante 74 días. En su punto máximo registrado hasta 2021, el consumo de energía

**Gráfica 2.** Consumo de energía relacionado con transacciones de Bitcoin, 2017-2021, en terawatts por hora (barras) y línea de tendencia (puntos).



Fuente: realización propia a partir de Digiconomist (2022).



de Bitcoin es equivalente al realizado por Tailandia, alcanzando un total de 204,50 teravatios/año (ver Gráfica 2).

En el caso particular de Bitcoin, la oferta total definida desde su creación es de 21 millones de unidades, de los cuales el 90% ya fue minado a corte de junio de 2021. Sin embargo, el diseño del sistema implica que la dificultad de minar la criptomoneda va aumentando exponencialmente, al tiempo que hay mayor complejidad de la red dada la participación de una mayor cantidad de mineros, llevando simultáneamente a que se incremente el poder de cómputo requerido y los requerimientos de energía.

Por su parte, se estima que cada transacción con la criptomoneda Ethereum requiere en promedio de 210,16 kilovatios/hora de electricidad, llevando a un consumo total de alrededor de 87,29 teravatios de energía eléctrica anualmente, lo que es comparable con el consumo de energía de un país como Finlandia (Reiff, 2022).

Ahora bien, el impacto medioambiental de la actividad del mercado de criptodivisas ha mostrado una relación directa con el consumo de energía mencionado. Para 2021, se estimó una huella de carbono de 114,06 millones de toneladas de CO<sub>2</sub> (MtCO<sub>2</sub>), comparable a la generada por la República Checa (Digiconomist, 2022). La minería de Ethereum implica a 2022 un esti-

mado de 48,69 MtCO<sub>2</sub> en emisiones, equivalente a las generadas por Bulgaria (Reiff, 2022).

En términos geográficos, Estados Unidos concentró a cierre de 2021 la mayor proporción de la minería de Bitcoin, con un 37,84% del total global, seguido por China con 21,11% y Kazajistán con 13,22% (University of Cambridge, 2022). No obstante, este dato debe ser analizado con cuidado, pues es claro que mineros de todas partes del mundo buscan realizar sus actividades en sitios que resulten más convenientes tanto en términos económicos como en aspectos técnicos y legales, lo que significa entre otras, que muchos de ellos centran sus operaciones en Estados Unidos, dada las condiciones de libertad de mercado y la confiabilidad tecnológica, o en otros como Kazajistán, que se ha vuelto atractivo para los mineros chinos sujetos a estrictas regulaciones e incluso prohibiciones, dada su cercanía geográfica de China y su conveniente relación costo/eficiencia.

Un impacto medioambiental adicional se relaciona con los desechos electrónicos, pues el *hardware* para la minería tiende a volverse obsoleto en periodos más bien cortos de tiempo, especialmente en la minería que emplea equipos ASIC (Application-Specific Integrated Circuit). Tal situación lleva a que, según Digiconomist (2022), la operación de Bitcoin sea responsable de generar desechos e-

lectrónicos por 36,31 miles de toneladas al año, similar a todos los pequeños equipos tecnológicos de Holanda.

Es previsible que a futuro la actividad del mercado de criptomonedas aumente, mientras su uso y la confianza en el sistema crezcan alrededor del planeta, pero también porque el minado tradicional de los activos digitales es un proceso competitivo en el que, en la medida en que el valor de la recompensa por bloque se incrementa, habrá un mayor incentivo hacia la minería de los mismos. Este hecho lleva a plantear, en principio, un panorama pesimista, ya que el mayor desarrollo que con seguridad tendrá el mercado de criptomonedas implicará una mayor demanda de energía y, como consecuencia, un impacto medioambiental creciente. Pero, como se explica a continuación, esto no tiene que ser así.

En este punto es necesario, entonces, preguntarse el porqué de tan elevado consumo de energía para el funcionamiento del mercado de criptoactivos: la respuesta es que no corresponde con una característica propia del sistema, sino que es una consecuencia del más extendido protocolo de consenso, deliberadamente seleccionada. Uno de los principios sobre los cuales funcionan los sistemas más importantes de criptomonedas es que no deben permitir que un solo agente tome control de los mismos, o que se genere una posición dominante

a partir de la cual se manipule el mercado a favor de uno o pocos agentes con mayor poder que otros. Es por esto precisamente que el alto consumo de recursos electrónicos y de energía es una característica de la creación de criptomonedas, incorporada desde su concepción. Así, este puede ser definido como un sistema de minería ineficiente, en el que una serie de computadores descentralizados se dedica a resolver acertijos matemáticos cada vez más complejos, compitiendo unos con otros para ver cuál es el primero en certificar una transacción y recibir a cambio criptomonedas, sistema conocido como *Proof-of-Work (PoW)*.

El protocolo *PoW* no es el único posible, sino que existe un conjunto creciente de alternativas que pueden ser igualmente robustas y con impacto medioambiental mucho menor, que se explican en la siguiente sección.

### 3. Protocolos alternativos de consenso: de criptomonedas sucias a limpias

Cuando se comparan los requerimientos energéticos para el funcionamiento de cada moneda digital, se encuentran dos grupos principales de las mismas:

- i) **Criptomonedas “sucias”**: son aquellas que hacen uso intensivo de energía, principalmente con fines de comprobación del tipo *PoW* (Corbet & Yarovaya, 2020), caracterizadas por una

alta relación consumo por número de transacciones (Sedlmeir et al., 2020) o que requieren el uso de *hardware* de alta demanda energética. Se considera que hacen parte de este conjunto criptomonedas como Bitcoin, Ethereum, Bitcoin Cash, Ethereum Classic, Litecoin y Monera.

ii) **Criptomonedas “limpias”:** también llamadas “verdes” o “ecoeficientes”. Al funcionar con base en protocolos de consenso no competitivos, reducen significativamente las operaciones requeridas y, por lo tanto, el uso de energía y la huella de carbono (Ren & Lucey, 2022). Ejemplos de este tipo de monedas digitales son SolarCoin, Powerledger, Cardano, Stella, Nano, Ripple, Polygon, Algorand, VeChain, TRON, Cosmos, Hedera, Tezos, EOS e IOTA (Leafscore, 2022).

El cambio de protocolo de consenso permite reducir el consumo de energía en cerca de 2000 veces, gracias a lo cual sería posible fomentar la sostenibilidad del mercado de criptomonedas, como es la meta de Ethereum 2.0 (Lee & Wu, 2022). Para que eso sea posible, se está reemplazando en la actualidad el protocolo *PoW* principalmente por otros como *PoS* y *PoA*, que se explican a continuación.

El protocolo *Proof of Stake (PoS)* es un sistema en el que el propietario del computador ofrece sus criptomonedas como garantía o co-

lateral a cambio de la oportunidad de ser elegido aleatoriamente para minar o verificar bloques en la cadena, cambiando el sistema de competencia con otros mineros por uno de selección automática al azar y, como resultado, reduciendo la cantidad de procesos realizados y de energía consumida (Frankenfield, 2021; Nguyen et al., 2019; Saleh, 2021). Lo anterior implica que se incentiva a que los participantes no sean solo validadores externos, sino que al poner como garantía sus propios recursos económicos, sean también inversionistas, dada la necesidad de disponer continuamente de una determinada cantidad de criptodivisas en el sistema (Bit2Me, 2021), en un entorno en el que mayores montos de reservas significan mayor probabilidad de ser elegidos para validar transacciones o minar nuevas unidades de la moneda digital.

Por su parte, en el protocolo *Proof-of-Authority (PoA)* los algoritmos son sometidos a estrictos procesos automatizados de examen para verificar *a priori* su calidad, en cadenas públicas donde quien desea participar abre una cuenta usando su identidad personal real. Una vez se verifica la calidad técnica del algoritmo y, especialmente, la buena reputación personal de su administrador, se le da a nombre propio la calidad de “validador”, una persona confiable que protege la cadena de bloques. Los validadores que son preaprobados organizan las transacciones en bloques y van

ganando mayor reputación, la que han de conservar cuidadosamente, debiendo estar dispuestos a invertir su propio dinero y a poner su buen nombre como garantía (Manolache et al., 2022; Yang et al., 2022). Al ser un mecanismo de consenso, más que de competencia, se requiere apenas un mínimo de poder de cómputo y, por lo tanto, el consumo de energía es mínimo.

Además, al requerir de una cantidad limitada de participantes para su funcionamiento, la red puede actualizar la cadena de bloques con mayor frecuencia, reduciendo procesos, tiempos, costos y consumo de energía (Coinhouse, 2021).

En la actualidad se están validando otros protocolos de consenso, dentro de los que se pueden mencionar *Proof-of-History (PoH)*, *Proof-of-elapsed-time (PoET)*, *Proof-of-Burn (PoB)* y *Proof-of-Capacity (PoC)*, los cuales pueden ofrecer nuevas alternativas para el minado, la transacción y la administración de criptoactivos más amigables con el medioambiente (Reiff, 2022).

Como comentario final, es importante reconocer que el impacto ambiental del mercado de criptomonedas es aún más incierto de lo que se ha mencionado, pues no solamente es compleja la contabilidad sobre su consumo total de energía, sino que además es necesario tener en cuenta cuál es la fuente de la que ella proviene, aspecto sobre el

que no hay estadísticas precisas (Gallersdörfer et al., 2020). Por ejemplo, si la fuente de la electricidad es una energía limpia, como la solar o la eólica, el perjuicio medioambiental es menor que de provenir de gas natural o combustibles fósiles (Stoll, 2019). En este orden de ideas, se requiere diferenciar la energía que un sistema consume de la cantidad de carbón que el mismo emite, es decir, que no se puede extrapolar el impacto ambiental si no se conoce la combinación de fuentes de energía. En el caso de Bitcoin, se estima en un rango muy amplio que entre el 39% y el 73% de su consumo de energía es carbón-neutral, porque ha sido obtenido o transado en zonas del planeta que cuentan con abundante energía hidroeléctrica, como es el caso de Escandinavia (Carter, 2021).

#### 4. Conclusiones

La preocupación por el impacto medioambiental de las actividades productivas, asociada en el pasado principalmente con industrias generadoras de bienes físicos, se convierte hoy en un punto central de atención de los procesos digitales, particularmente del mercado de criptoactivos, dado el altísimo consumo de energía necesario para su minado y posterior funcionamiento.

Se proyecta para los próximos años un crecimiento aún mayor del mercado de criptomonedas a escala global, lo que genera la pers-

pectiva de que él demandará cantidades crecientes de energía y que, como consecuencia, generará una huella de carbono cada vez mayor, lo cual es cierto solamente si se mantienen las características actuales de las criptomonedas más difundidas, principalmente Bitcoin y Ethereum. Tales monedas digitales fueron diseñadas con base en protocolos de consenso en los que diversos participantes compiten por minar nuevos bloques y validar transacciones, en un ambiente en el que la complejidad de los acertijos criptográficos crece exponencialmente y con ella, el volumen de procesos requeridos y la demanda energética correspondiente.

Pero el alto consumo de energía no es una característica propia de las criptomonedas, sino, de manera destacada, un resultado deliberado de protocolos competitivos como el *Proof-of-Work (PoW)*. Es así que el desarrollo y la implementación de protocolos alternativos, como el *Proof of Stake (PoS)* o el *Proof-of-Authority (PoA)*, se convierte en una necesidad para reducir la huella de carbono generada por la actividad de los mercados de monedas digitales, que con seguridad seguirán expandiéndose a futuro.

La efectividad técnica del *blockchain* ha de ser acompañada ahora por el logro de su sostenibilidad medioambiental, lo cual redundará en beneficio para el mercado de criptoactivos y en bienestar para toda la sociedad.

## Referencias

- Bit2Me (2021). ¿Qué es Prueba de participación / Proof of Stake (PoS)? Recuperado de: <https://academy.bit2me.com/que-es-proof-of-stake-pos/>
- Carter, N. (2021). How Much Energy Does Bitcoin Actually Consume? *Harvard Business Review*, May. Recuperado de: <https://hbr.org/2021/05/how-much-energy-does-bitcoin-actually-consume>
- Chan, S., Chu, J., Zhang, Y. & Nadarajah, S. (2020). Blockchain and Cryptocurrencies. *Journal of Risk and Financial Management* 13(10), 227. <https://doi.org/10.3390/jrfm13100227>
- Claeys, G. & Demertzis, M. (2021). Digital currencies: what role in our financial system? En: K.T. Liaw (ed.), *The Routledge Handbook of FinTech*, p. 51-66. Routledge / Taylor & Francis Group.
- Coinhouse (2021). What is Proof of Authority? Recuperado de: <https://www.coinhouse.com/what-is-proof-of-authority/>
- CoinMarketCap (2022). Global Cryptocurrency Charts - Total Cryptocurrency Market Cap. Recuperado de: <https://coinmarketcap.com/charts/>
- Corbet, S. & Yarovaya, L. (2020). The environmental effects of cryptocurrencies. En: S. Corbet, A. Urquhart & L. Yarovaya (Eds.), *Cryptocurrency and Blockchain Technology*, pp. 149-184. De Gruyter.
- de Vries, A. (2020). Bitcoin's energy consumption is underestimated: A market dynamics approach. *Energy Research & Social Science* 70, 1-6. <https://doi.org/10.1016/j.erss.2020.101721>

- Digiconomist (2022). Bitcoin Energy Consumption Index. Recuperado de: <https://digiconomist.net/bitcoin-energy-consumption/>
- Frankenfield, J. (2021). Proof-of-Stake (PoS), What Investors Need to Know About Altcoins. Recuperado de: [https://www.investopedia.com/terms/p/proof-stake-pos.asp#:~:text=expert%20and%20educator.,What%20is%20Proof%20of%20Stake%20\(PoS\)%3F,and%20keeping%20the%20database%20secure.](https://www.investopedia.com/terms/p/proof-stake-pos.asp#:~:text=expert%20and%20educator.,What%20is%20Proof%20of%20Stake%20(PoS)%3F,and%20keeping%20the%20database%20secure.)
- Gallersdörfer, U., Klaaßen, L. & Stoll, C. (2020). Energy Consumption of Cryptocurrencies Beyond Bitcoin. *Joule* 4, 1839–1851.
- Giudici, G., Milne, A. & Vinogradov, D. (2020). Cryptocurrencies: market analysis and perspectives. *Journal of Industrial and Business Economics* 47, 1-18. <https://doi.org/10.1007/s40812-019-00138-6>
- Hyland-Wood, D. & Johnson, S. (2022). Guest editorial: Blockchain consensus protocols. *Computer Networks* 207, 1-2. <https://doi.org/10.1016/j.comnet.2022.108861>
- Iberdrola (2021). What are green cryptocurrencies and why are they important? Recuperado de: <https://www.iberdrola.com/sustainability/green-cryptocurrencies>
- Krause, M.J. & Tolaymat, T. (2018). Quantification of energy and carbon costs for mining cryptocurrencies. *Nature Sustainability* 1, 711-718. <https://doi.org/10.1038/s41893-018-0152-7>
- Leafscore (2022). The 28 Most Sustainable Cryptocurrencies for 2022. Recuperado de: <https://www.leafscore.com/blog/the-9-most-sustainable-cryptocurrencies-for-2021/>
- Lee, A. & Wu, W. (2022). Energy Consumption in Crypto: an Overview. Report. Recuperado de: [https://content-hub-static.crypto.com/wp-content/uploads/2022/04/20220331\\_cryptodotcom\\_1\\_Public\\_Energy-consumption-in-Crypto\\_-an-Overview.pdf](https://content-hub-static.crypto.com/wp-content/uploads/2022/04/20220331_cryptodotcom_1_Public_Energy-consumption-in-Crypto_-an-Overview.pdf)
- Li, J., Li, N., Peng, J., Cui, H. & Wu, Z. (2018). Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies. *Energy* 168, 160–168. DOI: 10.1016/j.energy.2018.11.046.
- Manolache, M.A., Manolache, S. & Tapus, N. (2022). Decision Making using the Blockchain Proof of Authority Consensus. *Procedia Computer Science* 199, 580-588. DOI: 10.1016/j.procs.2022.01.071
- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Recuperado de: <https://bitcoin.org/bitcoin.pdf>
- Nguyen, C.T., Hoang, D.T., Nguyen, D.N., Niyato, D., Nguyen, H.T. & Dutkiewicz, E. (2019). Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities. *IEEE Access* 7, 85727-85745. DOI: 10.1109/ACCESS.2019.2925010.
- Quang, H.A.N., Duy, D., Burggraf, T., Thu, L.H.T. & Bui, N.H. (2022). Energy Consumption and Bitcoin Market. *Asia - Pacific Financial Markets* 29(1), 79-93. <https://doi.org/10.1007/s10690-021-09338-4>
- Reiff, N. (2022). What's the Environmental Impact of Cryptocurrency? Report.

Recuperado de:  
<https://www.investopedia.com/tech/whats-environmental-impact-cryptocurrency/>

Ren, B. & Lucey, B. (2022). A clean, green haven? - Examining the relationship between clean energy, clean and dirty cryptocurrencies. *Energy Economics* 109, 1-29.  
<https://doi.org/10.1016/j.eneco.2022.105951>

Saleh, F. (2021). Blockchain without waste: Proof-of-Stake. *The Review of Financial Studies* 34, 1156-1190.  
DOI:10.1093/rfs/hhaa075

Sedlmeir, J., Buhl, H.U., Fridgen, G. & Keller, R. (2020). The Energy Consumption of Blockchain Technology: Beyond Myth. *Business & Information Systems Engineering* 62(6): 599–608u7.  
<https://doi.org/10.1007/s12599-020-00656-x>


Statista (2022). Bitcoin average energy consumption per transaction compared of that to VISA as April 25, 2022.

Recuperado de:  
<https://www.statista.com/statistics/881541/bitcoin-energy-consumption-transaction-comparison-visa/>

Stoll, C., Klaufen, L., & Gellersdörfer, U. (2019). The Carbon Footprint of Bitcoin. *Joule* 3, 1647–1661.

University of Cambridge (2022). Bitcoin Mining Map - Cambridge Bitcoin Electricity Consumption Index.

Recuperado de:  
[https://ccaf.io/cbeci/mining\\_map](https://ccaf.io/cbeci/mining_map)

Yang, J., Dai, J., Gooi, H.B., Nguyen, H. & Paudel, A. (2022). A Proof-of-Authority Blockchain Based Distributed Control System for Islanded Microgrids. *IEEE Transactions on Industrial Informatics*, forthcoming.  
DOI: 10.1109/TII.2022.3142755. 

**Alejandro J. Useche.** Economista, Universidad del Rosario. Especialista en Finanzas, Universidad de los Andes. Doctor of Business Administration, Swiss Management Center University (Zug, Suiza). Profesor Asociado de la Escuela de Administración, Director Académico Maestría en Administración MBA, Universidad del Rosario (Bogotá, Colombia). Presidente del Comité Académico del Autorregulador del Mercado de Valores AMV.



# EXPERTOS EN CIBERSEGURIDAD

Somos una compañía de ciberseguridad con más de 20 años de experiencia dedicada a enfrentar las amenazas, proteger los activos y sistemas de organizaciones. Nos actualizamos constantemente en tecnologías y procesos para estar a la altura de las nuevas amenazas, basados en la innovación y el saber de seguridad. Siempre a la vanguardia de Latinoamérica en el desarrollo de la ciberseguridad.

Seguridad  
Corporativa

SGS

Identidad  
Digital

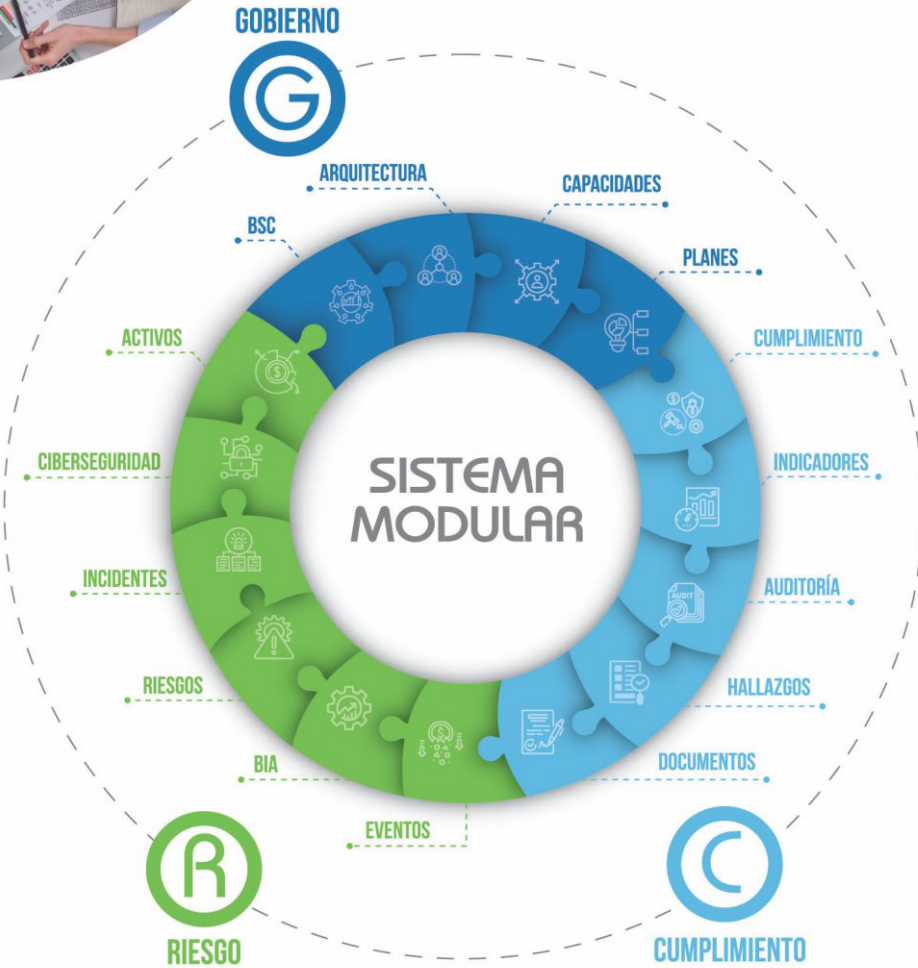
Seguridad OT

Consultoría





Fácil de usar, se adapta rápido a las necesidades de nuestros clientes, solo invierten en lo que requieren y siempre tienen asesoría especializada y soporte personalizado



## CONTÁCTANOS

WWW.NOVASEC.CO

57 301 241 07 76

571 344 14 03

INFO@NOVASEC.CO

@NOVASECSAS

@NOVASECSAS

@NOVASECSAS

13 AÑOS PROTEGIENDO LOS  
NEGOCIOS DE NUESTROS CLIENTES



# XXII

Del 25 al 28 de Julio



## Jornada Internacional de seguridad Informática

El Riesgo Geopolítico y la Ciberseguridad



**Dr. Mariano Bartolomé**

Operaciones en el  
cibersespacio, en el conflicto



**David Pereira**

Evolución del Kill Chain en  
Ciber Operaciones.



**Dr. Alexander Crowther**

Un análisis de los impactos  
para América Latina del  
conflicto cibernético entre  
Rusia y Ucrania



**Andrés Almanza**

Resultados encuesta  
Nacional de Seguridad



**Dr. Rafael Mota**

Armas Autónomas Letales y  
su impacto en la  
geopolítica actual y futura



**Gabriela Saucedo**

Resultados encuesta  
Latinoamericana de  
Seguridad



**Belisario Contreras**

Un compromiso por la Ciber  
Resiliencia



**Jeimy Cano**

El ransomware: una  
estrategia de  
desestabilización geopolítica.



**Emmanuel Ortíz**

Lazarus vs Lapsus: ¿actores  
maliciosos o agentes de  
amenaza ?



**Germán Realpe Delgado**

La Ciberinteligencia como  
herramienta para identificar  
Ciberriesgos en la Geopolítica



[www.acis.org.co/JornadaSeguridad2022](http://www.acis.org.co/JornadaSeguridad2022)  
+57 301 5530540 +57 304 3463413  
[www.acis.org.co](http://www.acis.org.co)