Seguridad A.H.I (Asimétrica, Híbrida e Interconectada)

DOI: 10.29236/sistemas.n167a6

El reto de una seguridad convergente y multidominio.

Resumen
La dinámica del mundo actual establece retos y exigencias para las organizaciones y sus planes estratégicos, así como para los Estados. Desde una perspectiva disciplinar, la comprensión de este escenario no permite reconocer y abordar la creciente y desbordada complejidad que implica desarrollar nuevas apuestas de negocios e iniciativas estatales para motivar transformaciones y crear experiencias novedosas.

En este sentido, es necesario transformar el paradigma de seguridad lineal y conocido, propio de los estándares y buenas prácticas vigente, por uno de seguridad asimétrica, híbrida e interconectada, detallado en este artículo, en la búsqueda de una mirada más holística de la realidad, para desde allí explorar el reto de seguridad y control de forma convergente y multidominio, como una respuesta natural a un entorno en donde abundan los inciertos y escasean las certezas, y en donde las policrisis son el nuevo anormal que deben atender y superar las organizaciones y Estados para habilitar su viabilidad en el largo plazo.

Palabras claves
Asimétrico, Híbrido, Interconectado, Convergencia, Multidominio

Introducción

El mundo asiste a un cambio estructural y dinámico en la medida que múltiples dominios (políticos, económicos, sociales, tecnológicos, legales y ambientales) interactúan entre sí, reforzándose mutuamente unos a otros en ciclos de causa-efecto no lineales, creando escenarios inéditos y desconocidos que las organizaciones y las naciones deben comenzar a identificar, comoquiera que no hacerlo los expone a condiciones y resultados que posiblemente no podrán manejar o tratar de cara a la defensa de los intereses estratégicos y de sus grupos de interés (WEF, 2023).

Este nuevo escenario de "policrisis" resultado de una interrelación de momentos, contextos y situaciones que se materializan a nivel internacional, motivan inestabilidad, incierto y algunas veces caos, que llevan a las empresas y países a movilizar diferentes alternativas que les permita navegar con el menor impacto sobre los riesgos emergentes que se generan y las expectativas propias de sus clientes y ciudadanos (Colomina et al., 2022). En línea con lo anterior, saben que no podrán asegurar ningún resultado en sí mismo, por la fragilidad inherente de las relaciones internacionales y la cadena de suministro, las vulnerabilidades tecnológicas, sociales y cognitivas que revisten la sociedad actual y los mercados globales, obligando a un cambio de postura en su relación con su entorno y las prácticas de negocios.

Así las cosas, las organizaciones y las naciones deberán motivar acciones que preparen a sus colectivos para concretar condiciones de resiliencia empresarial y nacional respectivamente, sabiendo que el "nuevo anormal" es la nueva base de las capacidades que se requieren para enfrentar las debilidades de los gobiernos, las tensiones geopolíticas, la mayor superficie de ataque, la especialización e innovación de los adversarios, los estallidos sociales y la crisis climática (Renn, 2018). Esta nueva realidad, rompe con los paradigmas actuales de la gestión de riesgos que por lo general tratan de ubicar certezas desde perspectivas disciplinares para desde allí movilizar acciones que estimulen iniciativas en las organizaciones o Estados.

En este sentido, se requiere una revisión y desarrollo de nuevas propuestas para el análisis, comprensión y anticipación de los riesgos a nivel corporativo y nacional sabiendo que es necesario estar vigilantes para actuar y continuar operando aun cuando se materialice la inevitabilidad de la falla (visible o invisible). Esto es, reconocer un escenario interconectado con efectos cascada, donde la volatilidad multidominio crece de manera paralela

con efectos inesperados, y se erosionan cada vez más las capacidades resilientes de personas, empresas y Estados por cuenta de riesgos profundamente conectados con resultados no esperados y efectos de borde que exceden los mejores pronósticos de los analistas (Sheffi, 2020).

En consecuencia, este artículo introduce un modelo de seguridad asimétrica, híbrida e interconectada (Modelo A.H.I) que busca situar tanto a empresas como naciones en un ejercicio de comprensión y tratamiento de riesgos en un contexto multidominio. Lo anterior, implica la interdependencia y el acoplamiento de los diferentes actores, los flujos asimétricos de mercancías, tecnologías, personas, dinero e imaginarios sociales, para habilitar un diálogo interdisciplinar que tenga como insumos las inestabilidades y los inciertos con el fin de acelerar el aprendizaje/desaprendizaje colectivo, y así abrir nuevas fronteras para responder a la interconexión global y la necesidad de una seguridad convergente y multidominio.

Fundamentos conceptuales: Contexto asimétrico, híbrido e interconectado

Para concretar el reto de una seguridad A.H.I (Asimétrica, Híbrida, Interconectada) es necesario entrar en profundidad de estos tres conceptos con el fin de entender cómo se crea este nuevo escenario emergente y disruptivo para los especialistas en gestión de riesgos, en su tarea de proveer una postura razonable, balanceada y costo efectivo para las empresas en el contexto de sus estrategias de negocio, y las exigencias de confianza digital de los ciudadanos en los Estados.

En primer lugar, es necesario indicar que tanto organizaciones como gobiernos saben que no podrán asegurar ni riesgo cero, ni seguridad cien por cien en el logro de sus propósitos, por tanto deberán definir su **apetito de riesgo** (*riesgo con el cual se siente cómodo y sabe que tiene los mecanismos para responder frente a su materialización y de aquellos residuales*), su **nivel de tolerancia** (*nivel de desviación permitido del apetito de riesgo definido*, que genera las alertas claves) y su **capacidad** (*el máximo nivel de riesgo que puede soportar*) para establecer los márgenes de operación y estrategias de acción que le permitan balancear su operación y mantener la integridad de sus planes y retos empresariales y nacionales (IIA, s.f.).

Las definiciones anteriores son necesarias y constituyen el primer insumo de los fundamentos de una seguridad A.H.I, pues en un contexto donde abundan las incertidumbres y escasean las certezas, se debe tener claridad el margen de acción y movilidad cuando las cosas no salen como estaban previstas, o cuando las sorpresas (previsibles o inesperadas) aparecen en

medio de la dinámica de las organizaciones y las naciones.

La *asimetría* como primer elemento del contexto que hace referencia a un desbalance natural que existe en la dinámica de las sociedades, donde la información, las tecnologías, las personas, el dinero y los imaginarios sociales mantienen posiciones inestables que por cuenta de las relaciones entre los diferentes agentes de la sociedad que tratan de movilizar con sus labores algunos de estos elementos siguiendo intereses particulares y generales, de tal forma que los resultados de sus acciones favorecen alguna lectura particular del entorno, desde donde las organizaciones y las naciones deberán concretar un equilibrio dinámico que les permita situarse en posiciones privilegiadas y estratégicas para el logro de su agenda específica.

Por otro lado, el concepto de *híbrido*, generalmente utilizado y entendido en el contexto militar como un cambio de dominio de combate, es una distinción mucho más elaborada y desafiante. Lo híbrido, siguiendo las definiciones de la Real Academia de la Lengua, supone un objeto o cosa diferente que es producto de elementos de distinta naturaleza. Esto es, un resultado novedoso y distinto a las fuentes que lo crearon, es la manifestación de un proceso de transformación y trasmutación que da vida a un evento completamente inédito, que genera mayor inestabilidad e incertidumbre y, por tanto, es necesario volver a reconocer, entender, analizar y descubrir para situarlo en el escenario donde hasta el momento no es conocido.

Finalmente lo *interconectado*, se refiere al uso de tecnologías de información y comunicaciones, que habilita, potencia y refuerza los dos elementos anteriores, creando realidades complemente distintas con flujos de información conocidos e inesperados, realidades aumentadas e inmersivas, y dinámicas abiertas y globales (productos/servicios) que implica reconocer en la densidad digital, la manera como los objetos físicos se transforman en “artefactos digitales” que ahora cuentan con capacidades inteligentes que informan, controlan y asisten la dinámica de los humanos en medio de un escenario como el ciberespacio.

Lo digital, implica la experiencia de estar conectados (aprovechando las oportunidades de una mayor densidad digital) y al mismo tiempo expuestos (proclives a engaños, fallas y vulnerabilidades de los ecosistemas digitales) sabiendo que al final la diferencia estará en el comportamiento de los seres humanos frente al fenómeno tecnológico.

La relación entre estos tres elementos establece un sistema complejo, socio-técnico y multidimensional que los modelos tradicionales de riesgo no logran manejar. En este sentido, una seguridad A.H.I

busca sensibilizar a todos los participantes y actores del escenario para analizar contradicciones, rarezas e incompatibilidades (Charan, 2015), y aprender no solo a tolerar la ambigüedad, sino a celebrarla, esto es, crear una perspectiva de relaciones posibles y no establecidas, en una zona psicológicamente segura para construir desde la sabiduría del error y los inciertos.

Evolución de la seguridad en un escenario convergente y multidominio

La seguridad en general se ha configurado como una percepción humana que busca establecer un estado de certeza concreto que le permita a una persona, actuar y movilizarse con un marco de consecuencias conocidos y validados para avanzar en sus propios objetivos. Si se parte del principio que no existen negocios o ganancias sin asumir riesgos (apetito de riesgo) es natural que tanto las organizaciones como las naciones asuman riesgos calculados para concretar sus objetivos estratégicos (O'Hare, 2022).

En este ejercicio continuado que se hace a nivel Estado como empresarial, se han generado diferentes posturas que persiguen todo el tiempo disminuir los inciertos, pues resultan incómodos y poco confiables para el logro de sus propósitos. Esta situación ha llevado a que muchos de los modelos de seguridad y control, así como las metodologías de gestión de riesgos tradicionales, se ocupen todo el tiempo de buscar formas de encontrar certezas y en este proceso, las encuentran en los eventos que ya han ocurrido. Esto es, basan sus indicadores en resultados de eventos pasados, tratando de extrapolar el conocimiento adquirido para sugerir una propuesta de acción en el futuro (Hopkin, 2010).

En este proceso las organizaciones buscan *gestionar y medir* la capacidad de la empresa o Estado para tratar los riesgos y establecer mecanismos de prevención y control que le permitan saber qué tanto debe avanzar o detenerse frente a una situación fuera de lo previsto, y desde allí concretar la mejor posición posible con el máximo de beneficio. Desafortunadamente los estándares y buenas prácticas disponibles sólo se refieren a aquellos riesgos conocidos, donde aplican sus "recetas" particulares para encontrar las certezas que necesita la organización, particularmente los equipos ejecutivos en la toma de decisiones donde lo que está en juego no sólo son los activos empresariales (o nacionales), sino su promesa de valor para con sus diferentes grupos de interés.

Una organización o nación que ha superado el ejercicio de gestión y medición, por lo general situado en el pasado, se moviliza al presente donde se exige el *sensar y responder*, un ejercicio de reconocimiento y análisis de datos e información en tiempo real, para saber qué, cómo y

dónde ocurre, y desde allí, responder para atender la situación, y no esperar a los efectos adversos que se puedan concretar, y si algo inesperado ocurre, es viable tener información para aprender tan rápido como sea posible para actuar y no dejar margen a los efectos colaterales que terminen impactando la dinámica de la entidad (Benjamins, 2022).

Sensar y responder es una evolución natural en un ejercicio de seguridad convergente donde diferentes vistas se conjugan para darle sentido a la nueva realidad enriquecida que transforma un incierto particular situado en un dominio, en una lectura enriquecida y aumentada del contexto que permite observar patrones de actividad por fuera de los marcos generales y formales establecidos para habilitar reflexiones y posturas proactivas que dan cuenta de las inestabilidades no para controlarlas, sino para comprenderlas y encontrar oportunidades que permitan situar la agenda estratégica de la organización, bien sea empresa o Estado.

La conexión entre el pasado y el presente implica una transición de un paradigma mecanicista y repetible, a uno marcado por el uso de los datos y la identificación de patrones en tiempo real, que retan el conocimiento hasta el momento adquirido por la organización. En este contexto, pensar ahora en el futuro (que no es posible predecir o conocer) se hace más retador el ejercicio de gestión de riesgos y de seguridad, comoquiera que mirar y caminar hacia adelante sin saber el comportamiento o situación que se puede presentar, implica navegar y asumir el incierto como la materia prima de la estrategia de seguridad y control. Esto es, pensar y advertir diferentes futuros, para establecer estrategias y acciones que lleven a la materialización de aquel que ofrezca las mejores condiciones y los menores impactos para la organización o Estado (Medina, 2023).

Defender y *anticipar* se configuran como los nuevos verbos de acción que se conectan con una seguridad convergente y multidominio pues demanda que los participantes exploren y se muevan en la zona de los riesgos emergentes, donde la dinámica de los inciertos es la norma y la resiliencia organizacional el objetivo fundamental. En este escenario los analistas de seguridad y control deben abandonar las certezas, cuestionar sus saberes previos y abrirse a las posibilidades más que a las probabilidades, con el fin de encontrar nuevos lugares comunes de riesgos sistémicos que puedan involucrar a su organización en efectos dominó que terminen comprometiendo su viabilidad en el mediano y largo plazo.

En este ejercicio de defender y anticipar, tanto las organizaciones como los Estados deberán mantener estrategias asociadas con disuadir, demorar, confundir y engañar para ganar espacios de acción y tiempo

de análisis, con el fin de contar con una tribuna de observación privilegiada, y desde allí, con la capacidad analítica de datos disponible, no sólo descubrir los patrones actuales, sino las tendencias consolidadas que permitan situar a la organización y los Estados en diferente futuros posibles donde pueden iniciar desde el hoy a construir las capacidades requeridas y los protocolos necesarios para actuar y avanzar cuando las señales del entorno muestren algunas características de ese futuro posible (Day & Schoemaker, 2019).

Al observar la transformación de la seguridad en un escenario convergente y multidominio, es clave entender que los conceptos vigentes de seguridad y control se quedan cortos y ubicados en una perspectiva que fragmenta la realidad dada su alta especialidad, análisis particular y disciplinar. Por tanto, habilitar una seguridad A.H.I implica combinar de forma simultánea el análisis y la síntesis de los diferentes dominios, observando en particular sus relaciones para revelar tanto los patrones como las tendencias con el fin de traducir el ejercicio de comprensión de esta dinámica en distinciones novedosas y prospectivas que le permitan a los involucrados no sólo tomar las decisiones del caso, sino aprender rápidamente de los acontecimientos y escenarios inéditos que ocurren o van a ocurrir en el mediano y largo plazo, así como sus posibles impactos.

Modelo de seguridad asimétrica, híbrida e interconectada

Desarrollar un modelo de seguridad que reconozca la dinámica y convergencia de diferentes dominios de operación, así como la capacidad de aprendizaje y resiliencia, implica no sólo navegar en el tiempo presente, sino influenciar igualmente el futuro. En este sentido, la propuesta que se presenta a continuación demanda una formación interdisciplinar, desinstalación intelectual, mentalidad de principiante y conciencia de la temporalidad de las cosas (Spitz, R., 2022), como base para movilizar esfuerzos, decisiones, acciones y retos que transformen los inciertos y ambigüedades en oportunidades y patrones de comportamiento que transformando el presente exploren nuevas ideas que reten el futuro.

El modelo propuesto cuenta con seis (6) pasos básicos, los cuales hacen parte de la definición de una seguridad A.H.I:
Es una percepción de confianza, confiabilidad e integridad multidominio basada en la capacidad de percibir, adaptar, disuadir, demorar, amortiguar y avanzar en medio de la incertidumbre, la inestabilidad y el caos que un evento adverso puede producir en el modelo de seguridad y control de una organización o nación.

1 Dominios: Social, Tecnológico, Económico, Político, Ambiental y Legal

El primer paso es *percibir*. Esto es, la observación de tendencias, definición y seguimiento de las incertidumbres críticas, y definición de escenarios para evaluar. El resultado de la percepción establece la vista panorámica de la situación, así como las diferentes alternativas de acción que se pueden concretar frente a diferentes escenarios posibles y probables.

El segundo momento es *adaptar*. La adaptación implica antifragilidad, configuración y reconfiguración de defensas en función de tendencias y analítica de comportamientos. Es un espacio para capitalizar el incierto sobre la dinámica actual de los eventos que tienen potencial de afectación para la organización. El resultado es una postura de objetivo móvil que deteriora la inteligencia del adversario (Cho et al., 2019).

El tercer paso es *disuadir*. La disuasión como la desmotivación del adversario o la pérdida de interés por parte del atacante para concretar su acción contraria en un objetivo específico, a través de la incorporación de tecnologías de engaño y de blanco móvil siguiendo los resultados del *adaptar* (Jasper, 2017).

El cuarto elemento es *demorar*. Demorar al agente agresor es diseñar espacios o zonas de distracción y contención de sus ataques en los diferentes dominios de operación creando confusión en sus acciones, que lleven a la variación de su plan y estrategia de desestabilización previamente definida. El resultado mayor distracción del agresor y aumento de su exposición y visibilización por parte de los controles organizacionales.

El quinto paso es *amortiguar*. La amortiguación es un ejercicio de capacidad de aguante y soporte de un evento adverso, esto es una declaración de umbrales de operación, apetito, tolerancia y capacidad de riesgo frente a un ataque exitoso. Este ejercicio de resistencia exige de todos los participantes un nivel de coordinación y comunicación definido, practicado y fluido que permite una actuación organizacional conjunta frente a la inevitabilidad de la falla (Fiksel, 2015).

Finalmente, y no menos importante, el paso seis que es *avanzar*. Esto significa capacidad de aprendizaje ágil, cuestionamiento del saber previo y reconocimiento del error como parte del proceso y no como resultado. Lo anterior implica, aprovechar las nuevas estrategias y tecnologías de defensa y anticipación para proteger la promesa de valor de la empresa o nación, y así habilitar la percepción de confianza, confiabilidad e integridad multidominio objetivo, que no es otra cosa que encontrar el balance real y concreto del apetito de riesgo y las apuestas por la implementación de experiencias innovadoras que transformen y superen las expectativas de los diferentes grupos de interés (Saydjari, 2018).

Si bien la propuesta conceptual se alinea con las necesidades actuales de seguridad y control tanto de negocios como de naciones, requiere un cambio de mentalidad y desacoplamiento de los modelos de riesgos tradicionales, para repensar la seguridad ahora desde los inciertos, no como una manera de evitar daños o impactos negativos, sino como la oportunidad de crear nuevas opciones y transformaciones que cambien el statu quo de las empresas y movilicen alternativas que acompañen y den sentido a los inciertos y eventos inesperados.

Reflexiones finales

Con un mundo cada vez más inestable, donde escasean las certezas y abundan los inciertos, los modelos de seguridad y control entran en crisis existencial, pues la base de su operación (las certezas) se deteriora y no permite mayor capacidad de acción y/o asesoría. En este sentido, se hace necesario superar el paradigma de la prevención basado en un conjunto de actividades sugeridas y probadas para disminuir el nivel de exposición, para transformarlo en una postura vigilante de defensa y anticipación que si bien, no garantiza un resultado específico, si habilita una acción coordinada y resiliente que permite actuar y sobrevivir aún en los escenarios más adversos e inesperados (Hepfer & Powell, 2020).

Las condiciones actuales de los escenarios asimétricos, híbridos e interconectados expanden y superan las capacidades actuales de las organizaciones y naciones por cuenta de una explosión de complejidad que escapa a los mejores análisis y pronósticos de los analistas. En este sentido, los Estados y las compañías se deben preparar para mantener sus operaciones y acompañar a sus grupos de interés en medio de un creciente ambiente hostil donde las tensiones en los diferentes dominios de acción: político, económico, social, tecnológico, ecológico y legal, se refuerzan entre sí, creando un entorno donde cualquier evento puede ocurrir y la capacidad de respuesta y resiliencia deberá ser la marca e impronta natural de la organización para ajustar su plan de navegación para alcanzar sus objetivos estratégicos (Medina, 2023).

El modelo A.H.I establece una propuesta conceptual que más allá de entender y visualizar los cambios del entorno, introduce una forma de incorporar los inciertos, la complejidad y los cambios como parte fundamental del reconocimiento de la gestión y gobierno del riesgo, ahora con perspectiva sistémica, con apertura frente la inevitabilidad de la falla y foco en la resiliencia organizacional. Esta apuesta conceptual busca mover a las organizaciones y los Estados fuera de la zona cómoda de las certezas y buenas prácticas, para avanzar y alcanzar sus objetivos en medio de la inestabilidad y los eventos inesperados propios del entorno actual.

Así las cosas, en mundo cada vez más desconocido, volátil, interconectado, complejo y exponencial, se hace necesario mantener una postura relevante y vigilante para lo cual es importante entender la seguridad y el control como una distinción multidominio donde todo el tiempo pueda dar respuesta a preguntas como: (Spitz, 2022)

- ¿Cuándo y cómo identifica los cambios?
- ¿Cada cuánto y cómo define su apetito de riesgo?
- ¿Cuándo y cómo aprende de aquello que no salió como estaba planeado?
- ¿Cuándo y cómo toma decisiones audaces?
- ¿Cómo reconcilia el corto y el largo plazo?
- ¿Cuándo y cómo identifica tendencias y patrones relevantes?
- ¿Cuándo y cómo reta sus propios saberes previos?

En resumen, cuando la seguridad no se concibe desde una perspectiva disciplinar particular, ni se asocia con la protección frente a daños, ni se ajusta con las inversiones que se hacen para lograr mayor tranquilidad (Proctor, 2023), se advierte una transformación de la distinción seguridad hacia un concepto de confiabilidad y balance dinámico, que responde, aprende y se adapta frente a las inestabilidades del entorno como una respuesta natural que entiende la disrupción y los inciertos como el fundamento de la toma de decisiones y del apetito de riesgo de las organizaciones en un contexto más asimétrico, híbrido e interconectado.

Referencias

Benjamins, R. (2022). *A data-driven company. 21 claves para crear valor a través de los datos y la inteligencia artificial*. España: LID Editorial

Charan, R. (2015). *The attacker's advantage. Turning uncertainty into breakthrough opportunities*. New York, USA: Perseus Books Groups

Cho, J., Sharma, D., Alavizadeh, H., Yoon, S., Ben-Asher, N., Moore, T., Kim, D. S., Lim, H. & Nelson, F. (2019) Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense. *IEEE Communications Surveys & Tutorials*. 1-39. Doi 10.1109/COMST.2019.2963791

Colomina et al. (2022). El mundo en 2023: diez temas que marcarán la agenda internacional. *CIDOB Notes Internationals*. No. 238. https://bit.ly/3YHt7uK

Day, G. & Schoemaker, P. (2019). *See soon, act faster. How vigilant leader thrive in an era of digital turbulence*. Cambridge, MA. USA: MIT Press.

Fiksel, J. (2015). *Resilient by Design. Creating Businesses That Adapt and Flourish in a Changing World*. Washington, DC. USA: Island Press.

Hepfer, M. & Powell, T. (2020). Make Cybersecurity a Strategic Asset. *Sloan Management Review*. 62(1). 40-45. https://sloanreview.mit.edu/article/make-cybersecurity-a-strategic-asset/

Hopkin, P. (2010). *Fundamentals of Risk Management. Understanding, evaluating and implementing effective risk management*. London, UK. Kogan

Page Limited - The Institute of Risk Management.

IIA (s.f.) Definición e implantación de apetito al riesgo. *Fábrica de Pensamiento*. Instituto de Auditores Internos de España. De: https://auditoresinternos.es/uploads/media_items/apetito-de-riesgo-original.original.pdf

Jasper, S. (2017). *Strategic cyber deterrence. The active cyber defense option*. Lanham, Maryland. USA: Rowman & Littlefield.

Medina, J. (2023). *Prospectiva para un mundo interdependiente*. Bogotá, Colombia: Editorial Aurora – Academia Colombiana de Ciencias Económicas.

O'Hare, D. (2022). *Introduction to Safety Science. People, Organisations, and Systems*. Boca Raton, Fl. USA: CRC Press.

Proctor, P. (2023). Cybersecurity Spending Does Not Equal Protection. *Gartner Blog*. https://blogs.gartner.com/paul-proctor/2023/02/12/cybersecurity-spending-does-not-equal-protection/

Renn, O. (2018). *Risk Governance. Coping with Uncertainty in a Complex World*. London, UK.: Earthscan.

Saydjari, O. (2018). *Engineering trustworthy systems: get cybersecurity design right the first time*. New York, USA.: McGraw Hill.

Sheffi, Y. (2020). *The new (ab)normal. Reshaping business and supply chain strategy beyond Covid-19*. Cambridge, MA. USA: MIT CTL Media

Spitz, R. (2022). *The definitive guide to thriving on disruption. Essential frameworks for disruption and uncertainty*. Vol II. USA: Disruptive Future Institute LLC.

WEF (2023). The Global Risks Report 2023. 18th Edition. *Insight Report*. https://www.weforum.org/reports/global-risks-report-2023/digest

***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–.*

NOS RENOVAMOS

LA ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

ACIS

ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

Queremos expandirnos. Es por esto, que hemos decidido ampliar nuestro nombre, para poder tener mayor alcance a todas las personas e instituciones que van de la mano con la tecnología.

Más información en:
www.ACIS.org.co
o escríbenos a:
301 5530540
Suscripciones@acis.org.co
Cursos@acis.org.co

CONECTA CON NOSOTROS

@Comunidadacis

ACIS

ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

WWW.ACIS.ORG.CO