No. 171 Abril - Junio DOI: 10.29236/sistemas ISSN 0120-5919

SISTEMAS

Computación confidencial:

El reto de la seguridad y control en la nube

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS
Calle 93 No. 13 - 32 of. 102
Bogotá, D.C.
www.acis.org.co

‹SHIELDING DIGITAL ASSETS GLOBALLY›

a3Sec

CIBER SEGURIDAD

Con nuestra metodología
fortaleces tu entorno digital.

En A3Sec nos hacemos responsables de la
Operación Unificada de Ciberseguridad
de las organizaciones.

< A3Sec España />
< A3Sec México />
< A3Sec Colombia />
< A3Sec Ecuador />

www.a3sec.com

En esta edición

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

Abril - Junio 2024
Calle 93 No.13 - 32 Of. 102
Teléfonos 616 1407 - 616 1409
A.A. 94334
Bogotá D.C.
www.acis.org.co

GAMMA INGENIEROS

40 años de experiencia respaldan nuestra labor

La innovación **acompaña su** primera línea de **defensa**

Ofrecemos soluciones y servicios en tecnología de última generación e impulsadas por IA, las cuales, sumadas a nuestra experiencia, tienen como foco la protección de datos de las empresas.

¿Cómo lo logramos?

Contamos con un CSOC propio que actúa 24/7, permitiéndonos responder de manera rápida y efectiva ante eventos de seguridad.

Nombrados como uno de los mejores 250MSSP's a nivel mundial por MSSP Alert A CRA Resource

Escanea este código para conocer nuestros portafolios de ciberseguridad

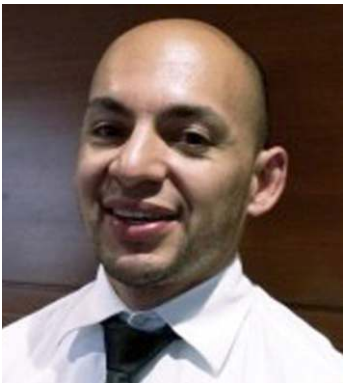
GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Computación confidencial

DOI: 10.29236/sistemas.n171a1

El reto de la seguridad y el control de los datos "en uso".



Jeimy J. Cano M.

Andrés R. Almanza J.

La dinámica de los datos tanto a nivel empresarial como global, implica reconocer los retos, los tratamientos y los flujos de información que determinan las diferentes ventajas competitivas de las naciones y los negocios. En este sentido, la protección de los datos en sus tres estados actuales: *en reposo* (almacenados en servidores y equipos de usuario final), *en movimiento* (a través de redes y conectores entre aplicaciones) y *en uso* (en la ejecución y procesamiento de las aplicaciones) se convierte en un escenario de acción conjunta entre organi-

zaciones y terceros de confianza para lograr un mayor aseguramiento de sus operaciones y por tanto, concretar la promesa de valor para sus clientes.

Una reciente encuesta latinoamericana realizada por la consultora internacional EY (2024) indica que los ejecutivos de las empresas de esta región consideran al menos las siguientes tecnologías como claves para su desarrollo en los próximos tres años: grandes datos & analítica, computación en la nube, inteligencia artificial y conectividad 5G.

En este escenario, el tratamiento de los datos a nivel de las aplicaciones se vuelve más sensible habida cuenta que, es en su explotación (la de los datos), donde se concreta el nuevo valor para los clientes, lo que implica un mayor procesamiento y uso por parte de las aplicaciones representadas en las nuevas iniciativas digitales generalmente desplegadas en la nube.

La computación confidencial tiene como objetivo "cifrar los datos en uso en la memoria principal del sistema sin comprometer el rendimiento. Lo anterior implica que los datos en memoria tienen dos aspectos claves:

- Cifrado de toda la memoria del sistema, y
- Cifrar la memoria individual de la máquina virtual (MV) y aislar la memoria de la MV del hipervisor (el hipervisor es un tipo de software informático, firmware o hardware que crea y ejecuta máquinas virtuales)" (Felk, 2023).

El reconocer que los datos "en uso" son el nuevo reto de las organizaciones modernas, ahora motivadas por una acelerada transformación digital y el desarrollo de nuevos ecosistemas digitales de negocio, implica actualizar el paradigma de seguridad y control vigente de las empresas que ha puesto el énfasis en los datos "en reposo" y en los datos "en tránsito". En este sentido, se advierten una serie de desafíos tanto para las organizaciones como para sus terceros de confianza para concretar y asegurar la confianza digital que los clientes demandan en un entorno cada vez más interconectado y dinámico como el actual. Algunos de los retos son: (CCC, 2021)

- Establecer un inventario de aplicaciones que requiere la implementación urgente de las características de la computación confidencial.
- Invertir en la formación de talento especializado que permita apalancar las nuevas iniciativas alrededor de la computación confidencial y cerrar la brecha que esto supone.
- Identificar los socios estratégicos en sus terceros de confianza para apalancar el aseguramiento de los datos extremo a extremo con el fin de aumentar la confiabilidad de la operación y el

aseguramiento de las exigencias normativas alrededor de los datos.
- Crear casos de negocio con los socios estratégicos para invertir de forma proactiva en el desarrollo de pruebas de concepto que muestren las oportunidades de la computación confidencial sobre sus aplicaciones críticas.
- Cuidar los elementos claves de la transición hacia un entorno de computación confidencial, lo que implica mantener entornos híbridos y mixtos en la operación, con una hoja de ruta clara y validada tanto por los objetivos de negocio como por los socios estratégicos.

En una organización centrada en la protección y defensa de los datos y la información, tanto de su dinámica empresarial como la de sus clientes, la computación confidencial se transforma en el estándar base de seguridad y control que asegura un adecuado procesamiento de los datos, cuidando no sólo la sensibilidad de la información que produce la compañía, sino el cumplimiento de la responsabilidad que implica el cuidado de la información que entregan los clientes al utilizar cada una de sus aplicaciones o iniciativas digitales.

Es por esto 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 la computación confidencial, con el fin de traer al escenario actual diferentes posturas sobre el tema, como insumo para plantear alternativas y opciones en un entorno de disrupción tecnológica acelerada. 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 en esta temática, capitalizando lecciones aprendidas, casos de estudio, repensando las dinámicas de los negocios y retos actuales, así mismo explorar el futuro que se avizora en el horizonte.

La ingeniera Sandra Rueda, profesora asociada del Departamento de Ingeniería de Sistemas y Computación de la Universidad de los Andes, columnista invitada, aborda algunas reflexiones sobre las tendencias y retos de la computación confidencial en la actualidad.

La entrevista efectuada al ingeniero Javier Evans, Director General Global firma A3SEC, revela aspectos prácticos de los retos de la computación confidencial y establece algunas orientaciones tanto para los profesionales en seguridad/ciberseguridad sobre este nuevo paradigma de protección datos en la nube que demanda repensar la vista de los diferentes estados de los datos y la infraestructura de hardware que se requiere para dar cuenta de las promesas de este nuevo avance en seguridad y control.

La investigación a cargo del ingeniero Andrés Almanza Junco, es el resultado del ejercicio continuado de la Asociación Colombiana de Ingenieros de Sistemas para tomarle el pulso a la evolución y transformación de las prácticas de seguridad/ciberseguridad en Colombia. Los resultados muestran entre otros aspectos como la confianza digital y la ciberresiliencia se convierten generadores de nuevos negocios, como elementos claves para cultivar las relaciones entre consumidores y quienes ofrecen los servicios, como una oportunidad para manejar y maniobrar en los ecosistemas digitales actuales.

El artículo desarrollado por el ingeniero Jeimy J. Cano M., se centrada en la conceptualización de la computación confidencial como nuevo paradigma de seguridad y control para la información “en uso”. Este hace una revisión básica de la temática, plantea algunas realidades (y una mentira) sobre la implementación de este nuevo paradigma y establece algunas conclusiones prácticas sobre sus retos e implicaciones tanto para las empresas como para los proveedores de servicios en la nube.

El foro de esta revista fue un espacio para compartir visiones desde diferentes ángulos la computación confidencial. Los ingenieros Diego Bueno de Oracle y Alonso Verdugo de Microsoft, desarrollaron un diálogo abierto y nutrido para contrastar y complementar sus posturas alrededor de los retos que implica la computación confidencial para las organizaciones modernas.

Ellos advierten sobre la necesidad de aumentar la visibilidad y conocimiento de esta nueva apuesta de transformación de la seguridad y control en la nube, el reto de establecer una seguridad extremo a extremo de las iniciativas digitales que actualmente despliegan las organizaciones y sobremanera, establecer planes de transición para concretar la promesa de valor de esta tecnología.

En resumen, se trata de un panorama renovado y provocador de nuevas transformaciones, retos y propuestas alrededor de la computación confidencial, que tensionan las certezas de los saberes y prácticas existentes de la seguridad en la nube y las realidades de las empresas en el tratamiento de sus datos con sus terceros de confianza. Su contenido invita a todos los profesionales, en las diferentes áreas del conocimiento, a explorar los nuevos retos y oportunidades en el uso y procesamiento de los datos y la información en un mundo digital y tecnológicamente modificado, sin perjuicio de las amenazas, fallas y vulnerabilidades propias de esta nueva propuesta de seguridad y control, donde tanto el negocio, la infraestructura, las aplicaciones y los datos plantean, revelan y reescriben nuevas incertidumbres y potencian el desarrollo de capacidades cibernéticas antes inexisten-

tes, de cara a los riesgos que permanecen ocultos en los retos de la transformación digital que avanza actualmente en las empresas.

Referencias

EY (2024). Desafíos y tendencias 2024 para las empresas de Latinoamérica. https://www.ey.com/es_co/insights/desafios-tendencias-2024-empresas-latinoamerica

Felk, Y. (2023). Confidential computing. En Mulder, V., Mermoud, A., Lenders, V. & Tellenbach, B. (editors). (2023). *Trends in Data Protection and Encryption Technologies*. Cham, Switzerland: Springer Nature Switzerland AG. 103-107.

Confidential Consulting Consortium – CCC (2021). Confidential Computing – The Next Frontier in Data Security. https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/Everest_Group_-_Confidential_Computing_-_The_Next_Frontier_in_Data_Security_-_2021-10-19.pdf

***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–.*

***Andrés 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.*

PAS
Palo Alto Solutions

¡DALE CONTINUIDAD A TU CARRERA PROFESIONAL EN LOS EEUU!

¿Eres INGENIERO O TIENES UN TÍTULO PROFESIONAL y más de 5 años de experiencia?

A través de la visa EB-2 NIW puedes lograrlo. En **Palo Alto Solutions PAS** te asesoramos y acompañamos a alcanzar este objetivo.

¡Contáctanos!

+1 689 (318) 5465 info@paloaltopas.us

Palo Alto Solutions @paloalto_solutions Palo Alto Solutions

Trabajando en "Las Nubes"

DOI: 10.29236/sistemas.n171a2

Sandra Rueda

Por sus beneficios, el uso de la tecnología de nube ha aumentado de forma consistente en los últimos años, sin embargo, esta tecnología también ha creado nuevos retos de ciberseguridad. Este artículo ofrece recomendaciones para facilitar el aseguramiento de servicios en "las nubes".

La organización NIST (*National Institute of Standards and Technology*) define Cómputo en la Nube como "*un modelo para habilitar acceso ubicuo, conveniente y por demanda a un conjunto compartido de recursos configurables de cómputo que pueden ser rápidamente aprovisionados y liberados con un esfuerzo de administración mínimo"* (Mell & Grance, 2011). Entre las ventajas de esta tecnología podemos mencionar, reducir el costo de la infraestructura tecnológica y

su mantenimiento, mejorar la capacidad de responder a cambios en la demanda de recursos y ampliar la posibilidad de conexión a servicios vía internet.

Considerando estas ventajas, no sorprende que el uso de servicios en la nube haya crecido de forma consistente en los últimos años. La Figura 1 muestra la inversión realizada por diferentes empresas, desde 2017, en tecnología de nube y se puede observar un crecimiento consistente en el valor de la inversión. Los valores estimados para la inversión en 2024 y 2025 son US$675430 millones de dólares ($675,43 *US billions*) y US$824760 millones de dólares ($824,76 *US billions*) respectivamente (Statista, 2024).

Gartner por su parte pronostica un crecimiento del 22,1% en el valor de las inversiones para 2025 (Gartner, 2024). Con base en estos datos podemos afirmar que el valor de la inversión y el número de empresas consumidoras de tecnología de nube seguirá creciendo en los próximos años.

Principales Retos para Asegurar un Servicio en la Nube

El amplio uso de tecnología de nube justifica el trabajo de los expertos para garantizar la seguridad y privacidad de datos y servicios en ese contexto. Entre los principales retos que las empresas deben enfrentar cuando deciden migrar un servicio a la nube podemos identificar: asumir el modelo de responsabilidad compartida, manejar el aumento de la superficie de ataque y la pérdida de visibilidad y responder a los requerimientos de privacidad y cumplimiento.

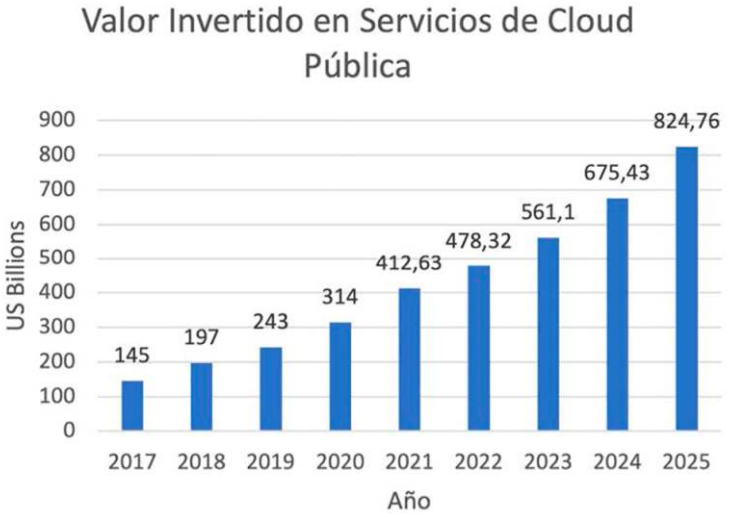


Figura 1. Inversión en Servicios de Cloud Pública (datos de Statista).

Asumir el modelo de responsabilidad compartida. Las empresas medianas y pequeñas, y algunas grandes, creen que migrando sus servicios a la nube transfieren al proveedor la responsabilidad de resolver los problemas de seguridad, pero, esta creencia es errónea. Al migrar los servicios a la nube la responsabilidad no se transfiere completamente, se distribuye, dando lugar a un modelo de responsabilidad compartida. Esto ocurre porque la migración no cambia los requerimientos de seguridad de un servicio o un conjunto de datos, los requerimientos de confidencialidad, integridad, disponibilidad y privacidad se conservan, pero las soluciones deben ser implementadas de forma compartida por el proveedor y la empresa que compra el servicio de nube.

La distribución de responsabilidades varía dependiendo del modelo de servicio; Infraestructura como Servicio, Plataforma como Servicio y Software como Servicio implican variaciones en las responsabilidades de proveedores y clientes. Google Cloud (Google Cloud, s.f.), Microsoft Azure (Microsoft, 2023) y otros proveedores de nube tienen sus propias versiones del modelo de responsabilidad compartida, los nombres de las capas usadas varían un poco, pero todos comparten el concepto fundamental: tanto el proveedor como el cliente son responsables del despliegue seguro de un servicio en la nube. Como consecuencia, la empresa que despliega un servicio en la nube debe identificar sus responsabilidades, entre las cuales podemos mencionar dos tareas que el cliente siempre debe asumir: (i) la identificación de los requerimientos de seguridad de sus datos y servicios, y (ii) hacer (o contratar) un análisis de riesgos para verificar que los requerimientos de seguridad están siendo gestionados de forma apropiada.

Manejar el aumento en la exposición de los datos y servicios. Un servicio de nube da mayor conexión a los usuarios gracias al uso de protocolos de comunicación estándar que facilitan la conexión vía internet con dispositivos como servidores, computadores de escritorio, laptops, tabletas y teléfonos celulares inteligentes. Por otro lado, los atacantes pueden usar está misma capacidad de acceso para desplegar ataques vía internet. La empresa que despliega un servicio en la nube es responsable de evaluar el riesgo asociado, decidir cómo manejarlo y definir las políticas de seguridad correspondientes. Además, dependiendo del modelo de servicio, debe implementar controles en las capas que estén bajo su responsabilidad.

Manejar la pérdida de visibilidad. El control de una empresa sobre su infraestructura y mecanismos en una instalación local (*on-premise*) es completo, pero cuando migra un servicio a la nube mueve sus recursos fuera del alcance de su red y transfiere parte del control al pro-

veedor. Además, un servicio en la nube permite a los empleados conectarse desde cualquier parte, a cualquier hora y con diferentes dispositivos. Con el auge de trabajo remoto desde la pandemia de COVID-19, estas características son ideales, sin embargo, las empresas pueden perder visibilidad sobre cómo y cuándo se usa su información y, como los recursos en la nube están fuera del alcance de una red corporativa, las herramientas tradicionales no sirven para monitorear los recursos protegidos.

Manejar los requerimientos de privacidad y cumplimiento. La privacidad se define como el derecho de todos los individuos a controlar lo que se sabe y se almacena sobre ellos mismos. Las regulaciones sobre protección de datos personales son consecuencia de este derecho y su cumplimiento debe ser una de las prioridades de cualquier empresa que recopile, almacene y procese los datos de sus usuarios, tanto por el aspecto legal como por principios éticos dado que las regulaciones protegen aspectos sensibles de las personas (International Telecommunication Union-ITU, 2012). Adicionalmente, al mover datos a la nube, hay que considerar que serán almacenados en centros de datos distribuidos en diferentes sitios geográficos y, por otro lado, algunos países tienen regulaciones que establecen restricciones sobre los sitios de procesamiento y almacenamiento de datos sensibles y datos personales de sus ciudadanos, como en el caso de la limitación geográfica de GDPR (*General Data Protection Regulation*) de la Unión Europea (Intersoft Consulting, s.f.).

Aunque los proveedores de nube ofrecen herramientas que permiten satisfacer estándares de cumplimiento, es responsabilidad de los clientes identificar la regulación que deben cumplir, como PCI DSS (P*ayment Card Industry Data Security Standard*) o GDPR (*General Data Protection Regulation*), y definir e implementar políticas y controles que protejan sus datos de fugas y usos no autorizados y permitan cumplir con la regulación.

Incidentes Recientes

El reporte de seguridad en nube para 2024 de Cybersecurity Insiders y Check Point indica que 61% de las empresas con servicios de nube reportan haber sufrido incidentes de seguridad durante los últimos 12 meses, lo cual representa un incremento de 24% con respecto al año anterior. 23% de los encuestados no están seguros o no pueden reportar los incidentes y solo 16% dicen que no hubo incidentes (Check Point y Cybersecurity Insiders, 2024).

Entre los principales problemas de seguridad que conducen a incidentes están:

- Errores de configuración. Estos errores son una de las principales causas de problemas de se-

guridad y fugas de datos. Ocurren por desconocer las características de una infraestructura de nube, no comprender el alcance/limitaciones de los controles de seguridad, y por la heterogeneidad de despliegues multinube (Check Point, s.f.). Estos errores incluyen fallas en: la gestión de vulnerabilidades, en el uso de autenticación multifactor, en la configuración del control acceso y en la configuración de las interfaces de conexión a los servicios de nube (Check Point, s.f.) (THALES, 2024).

- Secuestro de cuentas. Algunos usuarios tienen contraseñas débiles y las usan en varios servicios. Esto facilita que un atacante logre acceso no autorizado a una cuenta legítima y la use para robar datos, sin que los administradores del servicio lo noten. (Check Point, s.f.)
- Mecanismos no controlados para compartir datos. La tecnología de nube está diseñada para facilitar la tarea de compartir datos e incluye la posibilidad de crear un enlace que se envía por correo electrónico para dar acceso a un recurso, sin necesidad de autenticación. Este mecanismo permite que el enlace sea reenviado múltiples veces y dificulta controlar quién tiene acceso a un recurso (Check Point, s.f.)
- Ciberataques. Los servicios en nube son un objetivo atractivo para un atacante porque la infraestructura subyacente ofrece un alto nivel de conectividad vía internet, lo cual facilita el intento de acceso con un costo muy bajo. Además, tienen una alta probabilidad de presentar errores de configuración y almacenan gran cantidad de datos que pueden ser valiosos (Check Point, s.f.) (THALES, 2024). Adicionalmente, como la configuración de la infraestructura es estándar es posible que una técnica de ataque pueda repetirse con una alta probabilidad de éxito, de hecho, en 2023 Mandiant y VMware remediaron una vulnerabilidad de día cero; esta situación probó que los atacantes tienen los ambientes de nube entre sus objetivos (Google Cloud, 2024)

Factores Adicionales

Además de los retos mencionados, hay tres factores que amplifican la problemática de seguridad que se debe enfrentar al migrar servicios a la nube: herramientas específicas, falta de expertos y complejidad del ambiente.

Herramientas Específicas. Las herramientas que ofrecen los proveedores de nube para implementar políticas de seguridad son diferentes de las herramientas usadas en infraestructuras locales. Esto significa que el equipo de seguridad debe familiarizarse con herramientas nuevas, y a menudo complejas por la gran cantidad de opciones de configuración, identificando el alcance de estas y cómo gestionarlas.

Falta de Expertos. Asegurar servicios en la nube es diferente de asegurarlos en una instalación local (*on-premise*) y los equipos de seguridad deben ser conscientes.

Estas diferencias incluyen el conjunto de riesgos, dado que hay mayor exposición de los recursos, un participante adicional que puede tener privilegios (el proveedor de servicios) y un conjunto diferente de herramientas. El reporte de seguridad en nube para 2024 de Cybersecurity Insiders y Check Point menciona que 76% de los encuestados han enfrentado la falta de profesionales expertos en seguridad en contextos de nube (Check Point y Cybersecurity Insiders, 2024). The Cloud Security Alliance (CSA) también incluyó la falta de conocimientos y experiencia como uno de los principales retos para 2023. (Cloud Security Alliance, 2023)

Complejidad del Ambiente. Es común que un cliente decida construir un ambiente híbrido o multinube, el primero combina una nube pública y una privada, o una nube pública y una instalación local, mientras el segundo ambiente combina dos o más proveedores de nube. Estas combinaciones ofrecen la posibilidad de distribuir cargas de trabajo de forma flexible con base en las necesidades de la organización y en las ventajas del proveedor, como precio, capacidad de procesamiento y distribución geográfica. Sin embargo, los equipos de seguridad deben enfrentar un nivel de complejidad mayor al que se enfrenta en una instalación local en todas las combinaciones. Esta complejidad es resultado de las diferencias de funcionalidad, interfaces y herramientas en cada plataforma, agrava la pérdida de visibilidad y hace más difícil la tarea de asegurar los servicios y datos en la nube. (Check Point y Cybersecurity Insiders, 2024) (THALES, 2024)

Recomendaciones

El Centro Nacional para la Ciberseguridad del Reino Unido hace las siguientes recomendaciones tradicionales para escoger, configurar y usar servicios de nube de forma segura: proteger los datos en tránsito, proteger los activos en almacenamiento y en procesamiento, identificar las técnicas de aislamiento de clientes, usar un framework para gobernanza de la seguridad, implementar técnicas para operar y manejar los servicios de forma segura, considerar el acceso del personal del proveedor, diseñar, desarrollar y desplegar los servicios de forma segura, considerar la seguridad de la cadena de suministros, administrar usuarios, manejar identidad y autenticación, proteger las interfaces externas, asegurar los sistemas de administración, auditar y alertar, y usar seguridad por defecto. (National Cyber Security Centre, s.f.)

Además de estos principios tradicionales, con base en las amenazas y retos identificados más re-

cientemente, es recomendable tener en cuenta (ISC2 y Cybersecurity Insiders, 2024) (Google Cloud, 2024):

- Automatizar. Usar herramientas automatizadas para evaluar configuración y comportamiento y monitorear en tiempo real para detectar amenazas y responder rápidamente.
- Incorporar IA (Inteligencia Artificial). La rápida evolución de la IA generativa ofrece a los atacantes una nueva herramienta para mejorar sus técnicas. Los expertos en seguridad deberían usar esta misma tecnología para mejorar su capacidad de prevención, detección y respuesta.
- Mejorar la protección de datos. Usar cifrado, control de acceso y técnicas de prevención de fuga de datos para proteger información sensible.
- Invertir en entrenamiento y certificación. Ofrecer entrenamiento que permita a los equipos de seguridad entender los retos de seguridad en la nube y diseñar y construir arquitecturas apropiadas para las necesidades de la organización.
- Adoptar un modelo de confianza cero. El modelo busca proteger los recursos, suponiendo que la confianza nunca debe asignarse implícitamente y debe evaluarse continuamente.
- Construir un plan de respuesta a incidentes. Este plan debe adaptarse a las características de un servicio en nube para responder eficazmente a un incidente de seguridad.

Desplegar un servicio seguro en nube puede ser una tarea compleja que debe abordarse de forma organizada; entendiendo las responsabilidades asociadas, capacitándose y aprendiendo sobre las características de la infraestructura de nube, las herramientas disponibles y los retos presentes, y apoyándose en recomendaciones de centros reconocidos y expertos.

Referencias

Statista. (2024). *Public cloud services end-user spending worldwide from 2017 to 2024*. Retrieved from Estadísticas: https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/)

Mell, P., & Grance, T. (2011, September). The NIST Definition of Cloud Computing (Special Publication 800-145).

Intersoft Consulting. (n.d.). Retrieved Junio 2024, from GDPR: https://gdpr-info.eu/art-3-gdpr/

ISC2 y Cybersecurity Insiders. (2024). *2024 Cloud Security Report*.

International Telecommunication Union-ITU. (2012). *Privacy in Cloud Computing*.

Check Point y Cybersecurity Insiders. (2024). *2024 Cloud Security Report*.

Check Point. (n.d.). *Top 15 Cloud Security Issues, Threats and Concerns*. Retrieved Junio 2024, from Check Point Cyber Hub: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/

THALES. (2024). *2024 Cloud Security Study*.

Cloud Security Alliance. (2023, Abril). *Top Cloud Security Challenges in 2023*. Retrieved Junio 2024, from Cloud Security Alliance: https://cloudsecurityalliance.org/blog/2023/04/14/top-cloud-security-challenges-in-2023

Google Cloud. (2024). *Insights for Future Planning. Google Cloud*. (n.d.). Shared responsibilities and shared fate on Google Cloud. Retrieved Junio 2024, from Cloud Architecture Center: https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate

Microsoft. (2023). *Responsabilidad compartida en la nube*. Retrieved Junio 2024, from Documentación de los aspectos básicos de la seguridad en Azure: https://learn.microsoft.com/es-es/azure/security/fundamentals/shared-responsibility

National Cyber Security Centre. (n.d.). *The Cloud Security Principles*. Retrieved Junio 2024, from Cloud Security Guidance: https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

Gartner. (2024, Mayo). *Gartner Forecasts Worldwide Public Cloud End-User Spending to Surpass $675 Billion in 2024*. Retrieved Junio 2024, from Gartnet Newsroom: https://www.gartner.com/en/newsroom/press-releases/2024-05-20-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-surpass-675-billion-in-2024

Sandra Rueda: *Profesora asociada en el Departamento de Ingeniería de Sistemas y Computación de la Universidad de los Andes, Colombia. Ph.D. Computer Science and Engineering, The Pennsylvania State University, Estados Unidos. Sus áreas de investigación son seguridad de sistemas de software, análisis y generación automática de políticas de control de acceso y ciberseguridad en plataformas emergentes como IoT y móviles.*

Seguridad en la nube y el futuro

DOI: 10.29236/sistemas.n171a3

Javier Díaz Evans experto en ciberseguridad y líder en dirección aceptó la convocatoria para entrevistarlo alrededor de la seguridad en la nube y el futuro en este número de la revista.

"Existen personas muy importantes en mi desarrollo profesional, entre ellos César Tarazona, mi gran mentor, quien aportó en mi carrera el conocimiento técnico y la experiencia para evolucionar y desarrollarme en el frente de ciberseguridad y Julio Leonzo Álvarez quien me apoyó en el desarrollo de mis capacidades de liderazgo y dirección", señaló Javier Díaz Evans.

El entrevistado es ingeniero electrónico, especialista en Telemática de la Universidad de los Andes y eMBA de Inalde Business School. Cuenta con más de 20 años de experiencia en el campo de la ciberseguridad, ha desempeñado un papel clave en la evolución y expansión de A3SEC desde su fundación en 2012, como un spin-off de AlienVault y Teldat; A3SEC ha cre-

cido bajo su liderazgo para convertirse en una empresa líder en soluciones de ciberseguridad, operando en España, Colombia, Ecuador y México, con planes de expansión hacia Europa y Estados Unidos, agregó.

Javier Díaz Evans ha sido pionero en la adopción de una estrategia basada en la inteligencia de datos, la hiperautomatización y el uso de IA/ML, transformando la forma en que las organizaciones protegen sus activos digitales.

Antes de A3SEC, acumuló una vasta experiencia como proveedor y consultor de seguridad, así como CISO (Chief Information Security Officer) de un conglomerado financiero, lo que le ha permitido tener una visión integral y práctica de las necesidades del sector.

Revista Sistemas: *¿Es la computación confidencial el futuro de la seguridad en la computación en la nube?*

Javier Díaz Evans: Tradicionalmente, la protección de datos se ha centrado en el resguardo y la transmisión, pero la confidencialidad del procesamiento de datos solo se había abordado para elementos muy sensibles utilizando soluciones como los HSM (Módulos de Seguridad en Hardware) y los EPP (Pin Pad Cifrados). La computación confidencial promete extender esta protección al procesamiento de datos en entornos de nube, pero enfrenta varios retos significativos:

- Estándares y Regulaciones: La falta de normas unificadas y regulaciones claras puede dificultar la adopción generalizada.
- Rendimiento: Mantener un alto nivel de rendimiento mientras se garantiza la seguridad es un desafío técnico.

- Interoperabilidad: Es crucial asegurar que las soluciones de computación confidencial funcionen eficientemente en diferentes plataformas y con otros sistemas de seguridad.
- Adopción del Mercado: Convencer a las organizaciones del valor y la necesidad de invertir en estas tecnologías es un reto.
- Complejidad Técnica: Implementar y gestionar entornos de ejecución confiables (TEE) requiere conocimientos avanzados y recursos significativos.
- Ataques Sofisticados: Es necesario desarrollar métodos para protegerse contra ataques cada vez más sofisticados que buscan explotar vulnerabilidades en los TEE.

Aunque la computación confidencial tiene un gran potencial, el futuro podría ver la aparición de otras tecnologías emergentes que transformen este paradigma de la seguridad en la nube. La evolución constante en el ámbito de la seguridad cibernética significa que debemos estar preparados para adaptarnos a nuevas soluciones que puedan ofrecer aún más protección y eficiencia.

RS: *Si una organización quiere incorporar la computación confidencial en sus prácticas y despliegues actuales, ¿cuál sería la hoja de ruta a seguir?*

JDE: Para incorporar la tecnología de computación confidencial en una organización y garantizar que nos preparemos para enfrentar los desafíos y maximizar los beneficios es necesario seguir una hoja de ruta detallada, comparto algunas ideas:

1. Desarrollar Conocimientos y Capacidades:
- Fortalecer las competencias internas sobre el paradigma de la computación confidencial.
2. Evaluación Inicial:
- Realizar un análisis de las necesidades de negocio, inventario, flujos y clasificación de datos, así como de los riesgos actuales de ciberseguridad y privacidad.
3. Diseño de Arquitectura:
- Seleccionar los estándares y tecnologías más adecuadas, planificando la integración con las soluciones existentes y definiendo políticas y estándares específicos.
4. Prueba Piloto:
- Implementar una prueba piloto para evaluar la seguridad y el rendimiento, permitiendo realizar ajustes y optimizaciones necesarias antes del despliegue a gran escala.
5. Plan de Despliegue:
- Establecer un plan de migración gradual de la tecnología, con monitoreo constante y soporte continuo para asegurar una transición fluida.
6. Estrategia de Gobernanza:
- Desarrollar una estrategia de gobernanza que incluya evaluaciones periódicas de ciberseguridad, actualizaciones tecnoló-

gicas y la integración en procesos de gestión de fallos e incidentes.

7. Evaluación de Impacto:

- Medir y evaluar los resultados obtenidos con la nueva tecnología, generando retroalimentación continua para mejorar y ajustar la implementación según sea necesario.

RS: *¿Cuáles podrían ser los retos más importantes a tener en cuenta para una organización si quiere incorporar la computación confidencial en su infraestructura y aplicaciones?*

JDE: La respuesta fue planteada en la primera pregunta para validar si es el futuro de la computación en la nube, pero si analizamos los más importantes diría que son:

- Rendimiento.
- Interoperabilidad.
- Ataques Sofisticados.

RS: *¿Cómo encaja la computación confidencial con las actuales medidas de seguridad desplegadas en la nube como son XDR, SOAR, entre otras?*

JDE: La computación confidencial, al centrarse en el cifrado integral de los datos, plantea retos y oportunidades para los sistemas de seguridad en la nube.

Desafíos en Detección y Respuesta:

- Cifrado de Datos en Tránsito: Los sistemas de detección de intrusos (IDS) y su evolución NDR (Network Detection & Response) que analizan el tráfico de red pueden encontrar limitaciones al analizar datos cifrados, afectando su visibilidad y capacidad de detección de amenazas.
- Sistemas EDR: Podrían enfrentar dificultades para identificar ciertas tácticas y técnicas que implican acceso y procesamiento de datos cifrados, requiriendo una evolución en sus capacidades de detección.
- Integración y Evolución de Controles:

- XDR y SOAR: Estas soluciones, que combinan múltiples fuentes de datos y capacidades de respuesta automatizada, necesitarán adaptarse para gestionar y analizar datos en entornos de computación confidencial. Esto implica actualizar metodologías y procesos de ingeniería de detección para mantener y mejorar la eficacia en la identificación de amenazas, incluso con datos cifrados.

- Complementariedad:

- Analítica de Ciberseguridad: Herramientas de analítica avanzadas pueden complementar las capacidades de detección y respuesta de XDR y SOAR, asegurando que no se pierdan capacidades críticas para reducir el tiempo de exposición ante ataques.

En resumen, la computación confidencial exige una evolución en las herramientas de seguridad actua-

les para integrarse eficazmente, manteniendo y potenciando las capacidades de detección y respuesta.

RS: *¿Qué nuevos desarrollos se ven a futuro para la computación confidencial?*

JDE: La computación confidencial está avanzando con el desarrollo de procesadores que incorporan tecnologías para proteger la ejecución de código y datos. Estos procesadores permiten aislar la ejecución del sistema operativo y las aplicaciones, mejorando así la privacidad de datos.

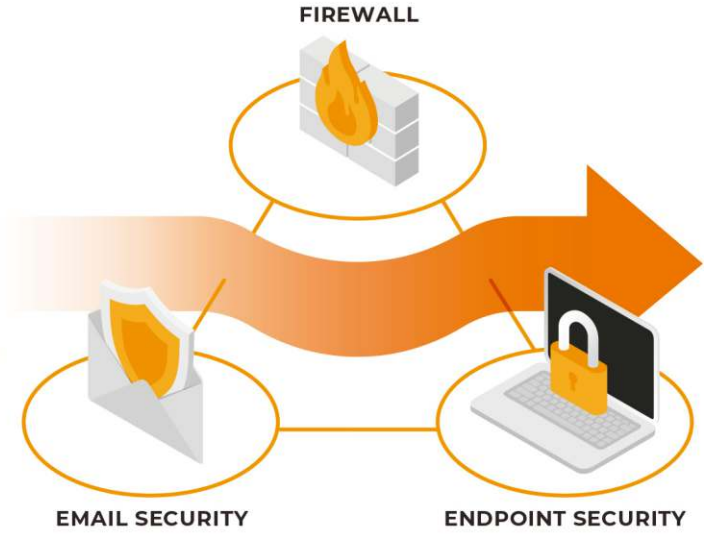
Además, están surgiendo nuevos modelos criptográficos que facilitan realizar cálculos con datos cifrados sin necesidad de descifrarlos previamente. Esto no solo fortalece la privacidad, sino que también puede mejorar el rendimiento de las aplicaciones.

Otro avance importante es la computación distribuida confidencial, que permite a múltiples entidades colaborar en el cálculo de funciones sin revelar sus datos de entrada individuales. Este enfoque preserva la privacidad y la integridad de los datos entre los participantes.

Finalmente, se esperan desarrollos significativos en normativas y estándares, que jugarán un papel crucial en la regulación y adopción de estas tecnologías seguras a nivel global.

LUMU

El **100%** de
los ataques
sobrepasan
estas defensas



Lumu completa su **stack de ciberseguridad**

- **Ofrece visibilidad** de la red de 360°
- **Responde a las amenazas** en segundos
- **Maneja el 100%** de las alertas
- **Reduce el costo de SecOps** hasta en un 80%

Prueba **Lumu gratis**

Reserva una **demostración**

www.lumu.io

XXIV Encuesta Nacional de Seguridad Informática

DOI: 10.29236/sistemas.n171a4

De la seguridad a la confianza.

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 2024, contó con la participación de 203 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 que colaboraron también con el diligenciamiento del instrumento. 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 en el corto, mediano y largo plazo, así como ayudar a formular mejoras en la postura de seguridad control y resiliencia 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 el desarrollo de la seguridad y ciberseguridad de las organizaciones y como los diferentes sectores de la industria empiezan a comprender a la seguridad digital y ciberseguridad como herramientas que ayudan a incrementar el valor de estas.

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.

Hallazgos principales

Demografía

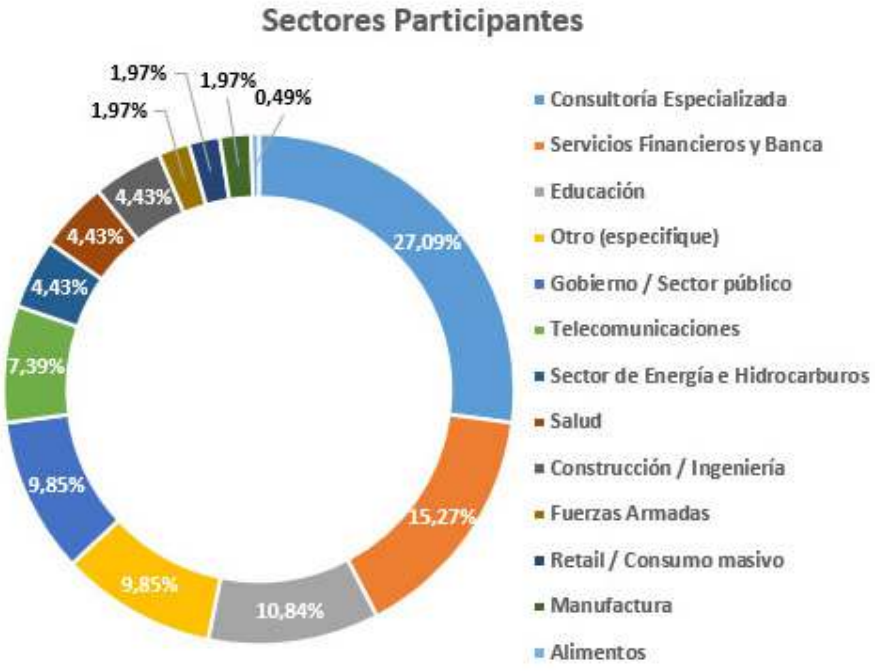
Sectores participantes

La gráfica 1 refleja la participación de algunos de los sectores de la economía colombiana. Los tres segmentos con mayor participación de la encuesta para este año fueron Consultoría especializada, Financieros, Educación y Otros, el cual representa a aquellos que no se identifican con los sectores definidos (Servicios legales, aseguradores, sociedad civil, y otros).

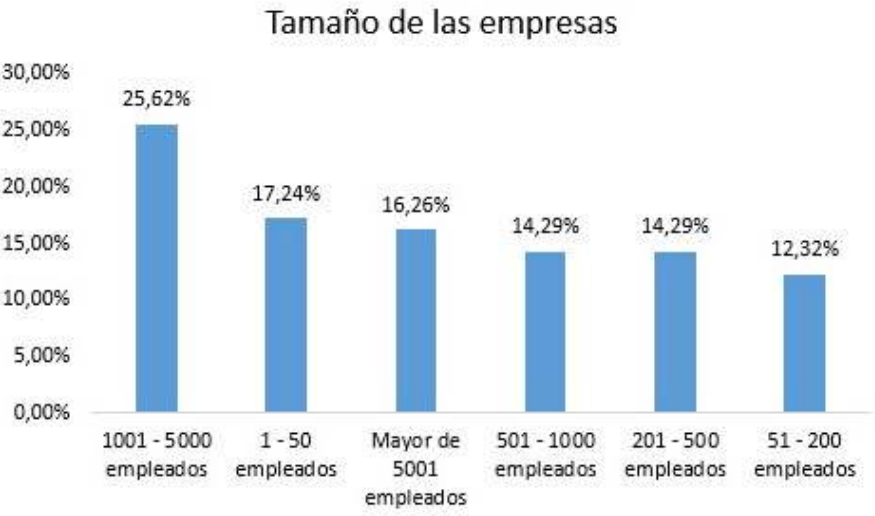
La grafica 2 muestra el tamaño de las empresas en Colombia, de acuerdo con el número de empleados y se puede observar la participación de empresas de todos los tamaños y cómo la ciberseguridad ha impactado sus operaciones.

La gráfica 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.

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-



Gráfica 1: Sectores participantes



Gráfica 2: Tamaño de las empresas participantes.

Gráfica 3: Cargos de los encuestados

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 acerca de lo que representa la ciberseguridad en sus organizaciones.

En la gráfica 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, seguido de establecer e implementar un modelo de políticas y en tercer lugar Definir, implementar y asegurar la estrategia de ciberseguridad de la empresa.

La gráfica 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 35%, seguido por la Vicepresidencia/Director Departamento de Tecnologías de la Información 17% y en tercer lugar del Director/Jefe de Seguridad Informática 15%.

En la gráfica 6 se observan los roles dentro de una organización en materia de seguridad digital. El rol de analista de seguridad de la información es el número 1, seguido de la posición CISO u Oficial de Seguridad de la Información y analista de seguridad informática.

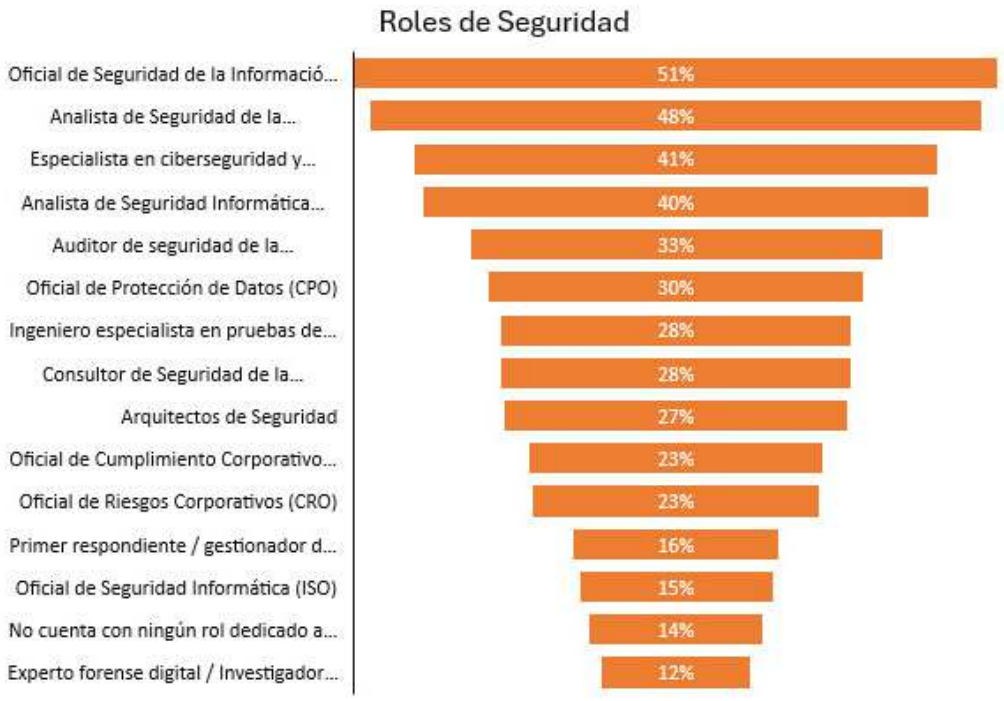
Consideraciones de los datos

Participación de la industria

Después de 24 años de este ejercicio, se ha mantenido la participación de los diferentes profesionales de seguridad, tecnologías y afines, que ven en este instrumento una oportunidad para seguir apren-

Gráfica 4: Funciones del responsable de seguridad

Gráfica 5: Dependencia del área de Seguridad



Gráfica 6: Roles de Seguridad

diendo sobre la ciberseguridad en la región y el país.

El informe del Foro Económico Mundial en Davos del 2024, una vez más muestra qué importante es la ciberseguridad para el ecosistema empresarial y como está viene evolucionando de hablar de solo proteger a ser un generador de confianza (WEFc, 2024), así mismo el informe de la misma institución titulado Global Cybersecurity Outlook 2024, resalta la importancia que menciona aspectos claves de la seguridad en la sociedad y la importancia para las empresas, y como las tecnologías emergentes son y serán piezas claves del desarrollo económico de los estados y las empresas en procura de una resiliencia que haga sostenible a los mismos (WEFa, 2024)

Roles, responsabilidades y funciones

Las áreas de seguridad siguen desempeñando un rol importante en las empresas colombianas, este año al hacer análisis por tamaños de empresas hemos encontrado en los diferentes sectores de industrias datos interesantes.

Se siguen manteniendo las funciones básicas de las áreas de seguridad como unas áreas tácticas u operacionales en las empresas de Colombia, donde la *Definición de*

controles de TI en materia de seguridad de la información con un 67%, Creación de programas de entrenamiento en materia de seguridad de la información con un 63%, y Establecer e implementar un modelo de políticas en materia de seguridad de la información con un 61%, son las principales funciones del área de seguridad. Sin embargo, si existen algunas interesantes variaciones al revisar por tamaño de las empresas en la realidad colombiana.

1. Las empresas de 1 a 50 empleados, el área de seguridad cumple con un propósito muy técnico y táctico, al estar enfocadas en velar por la protección de información personal en un 21%, aseguramiento de los procesos de la organización 18% y seguimiento de prácticas en materia de protección de la privacidad con igual %
2. Las empresas de 51 a 200 empleados centran sus esfuerzos en el 15% en el seguimiento a las prácticas en materia de protección de la privacidad, la Implementación de controles de TI en materia de seguridad de la información con el mismo porcentaje y como su tercera acción está Definir, diseñar y velar por el programa de privacidad de la información de la organización, todos con el mismo porcentaje.
3. Las empresas de 201 a 500 empleados enfocan sus acciones en, Definición de controles de TI en materia de seguridad de la información el 18%, Definir, implementar y asegurar el programa de protección de datos personales de la empresa 17% y Definir programas de resiliencia digital el 17%.
4. De 501 a 1000, Creación de programas de entrenamiento en materia de seguridad de la información 19%, Evaluar la eficiencia y efectividad del modelo de seguridad de la información 19%, Definir o diseñar escenarios/simulaciones/Playbooks en relación con ciberriesgos 18%.
5. De 1001 a 5000, Supervisar procesos de cumplimiento regulatorio en tecnología de información 35%, Supervisar y gestionar los procesos de investigaciones forenses digitales 33%, Establecer y revisar la arquitectura de seguridad de la información 32%.
6. Mayores a 5001, Dirigir y supervisar los programas de riesgos de seguridad de la información de la organización 22%, Gestionar el programa de gestión de incidentes de seguridad de la información 21%, Definir programas de resiliencia digital 20%.

La confianza y la resiliencia son dos pilares fundamentales de las economías actuales que hacen por tanto que los datos se conviertan en la herramienta, junto a sus procesos de protección en una estrategia para brindar a las partes interesadas la confianza para crear entornos digitales confiables (Edelman, 2024), los datos de la realidad

de Colombia, a la luz de informes como el de ISACA muestran que la protección de la confianza se está volviendo cada vez más relevante y de mayor importancia (ISACA, 2024).

Igualmente se puede decir que mientras las empresas pequeñas entienden al dato como un activo de vital importancia (Connectwise, 2024), maduran a un ritmo no uniforme y se presentan desconexiones en las organizaciones que hacen que ese ritmo no sea más eficiente frente a la cantidad de ataques informáticos exitosos que existen en la actualidad (Latpass, 2024).

Al revisar por sectores, hay notorias diferencias que muestran un poco la realidad de las empresas, y que basado en los datos inclusive por tamaños de empresas se comportan de manera distinta, acá para efectos de la investigación dejamos el general de algunos sectores de la industria y sus esfuerzos número uno tabla 1.

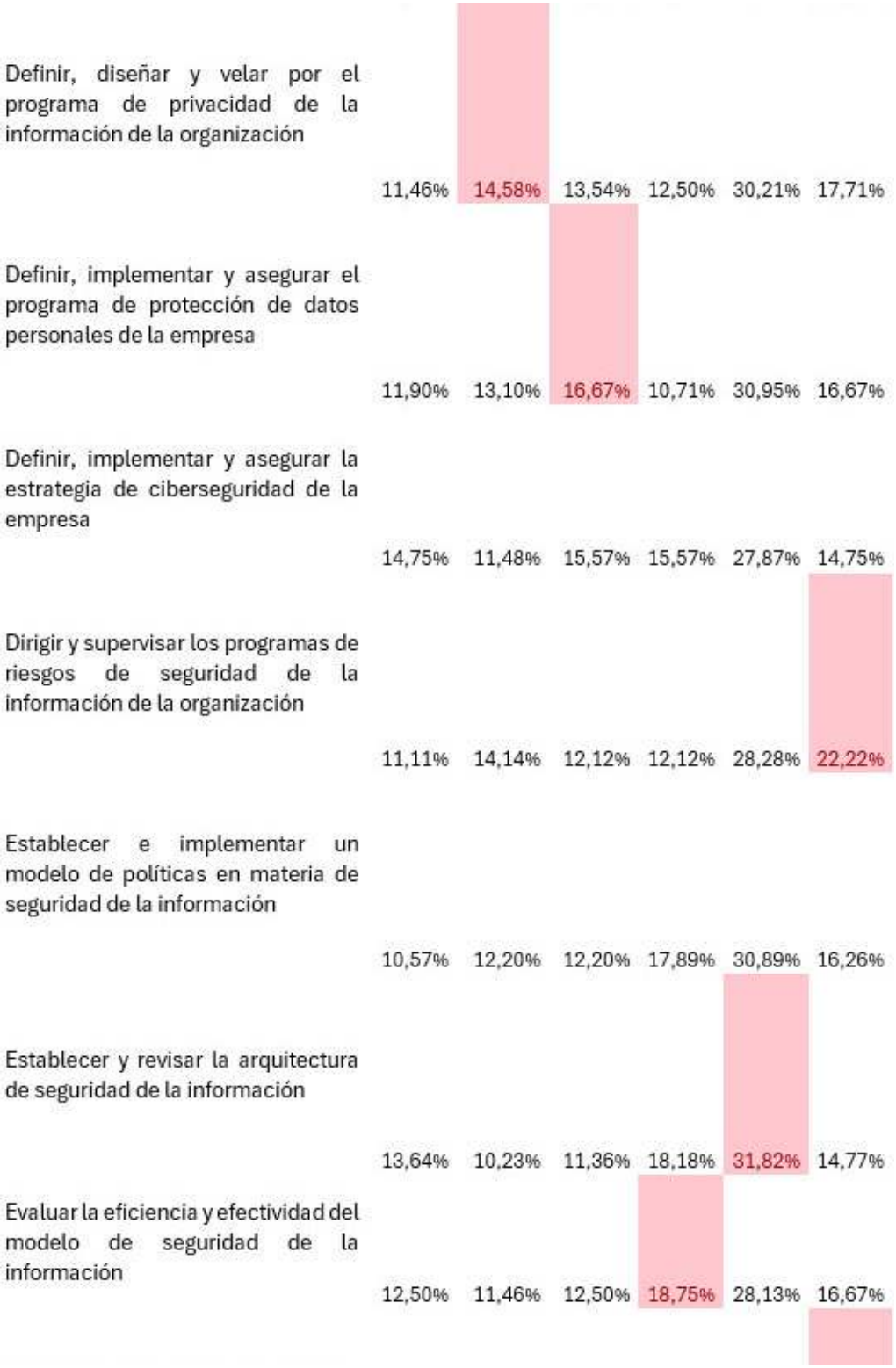
La tabla 2, describe y resalta el top tres de funciones en (rojo) que suceden en las empresas basados en sus tamaños, en ellas se pueden representar la madurez de las empresas en el desarrollo de sus prácticas, las pequeñas hasta 200 empleados parece que entienden que el dato y más los personales son fuentes y motor del negocio que necesita ser protegidos, las medianas mayor de 200 hasta 999, educar, gestionar riesgos, generar controles, crear resiliencia y proteger los datos son piezas claves de sus fun-

Sectores	Función principal.
Construcción / Ingeniería	Velar por la protección de la información personal
Consultoría Especializada – Manufactura - Salud	Aseguramiento de procesos de la organización
Educación	Establecer y revisar la arquitectura de seguridad de la información
Fuerzas Armadas - Gobierno / Sector público	Definir, diseñar y velar por el programa de privacidad de la información de la organización
Otro (especifique)	Creación de programas de entrenamiento en materia de seguridad de la información
Sector de Energía e Hidrocarburos	Definir programas de resiliencia digital
Servicios Financieros y Banca	Definir o diseñar escenarios/simulaciones/Playbooks en relación con ciberriesgos
Telecomunicaciones	Seguimiento de prácticas en materia de protección de la privacidad de la información personal

Tabla 1: Sectores x función de seguridad (Elaboración propia)

Tabla 2: Distribución de responsabilidades por tamaños de empresas

Valores	1 - 50 empleados	51 - 200 empleados	201 - 500 empleados	501 - 1000 empleados	1001 - 5000 empleados	Mayor de 5001 empleados
Aseguramiento de procesos de la organización	18,09%	11,70%	13,83%	14,89%	29,79%	11,70%
Creación de programas de entrenamiento en materia de seguridad de la información	10,16%	11,72%	14,84%	18,75%	25,78%	18,75%
Creación de programas de gobierno y gestión en materia de seguridad de la información	9,80%	12,75%	11,76%	17,65%	28,43%	19,61%
Definición de controles de TI en materia de seguridad de la información	10,22%	11,68%	18,25%	16,79%	28,47%	14,60%
Definir o diseñar escenarios/simulaciones/Playbooks en relación con ciberriesgos	6,67%	10,00%	15,00%	18,33%	30,00%	20,00%
Definir programas de resiliencia digital	12,50%	12,50%	16,67%	8,33%	29,17%	20,83%


Definir, diseñar y velar por el programa de privacidad de la información de la organización
11,46% 14,58% 13,54% 12,50% 30,21% 17,71%
Definir, implementar y asegurar el programa de protección de datos personales de la empresa
11,90% 13,10% 16,67% 10,71% 30,95% 16,67%
Definir, implementar y asegurar la estrategia de ciberseguridad de la empresa
14,75% 11,48% 15,57% 15,57% 27,87% 14,75%
Dirigir y supervisar los programas de riesgos de seguridad de la información de la organización
11,11% 14,14% 12,12% 12,12% 28,28% 22,22%
Establecer e implementar un modelo de políticas en materia de seguridad de la información
10,57% 12,20% 12,20% 17,89% 30,89% 16,26%
Establecer y revisar la arquitectura de seguridad de la información
13,64% 10,23% 11,36% 18,18% 31,82% 14,77%
Evaluar la eficiencia y efectividad del modelo de seguridad de la información
12,50% 11,46% 12,50% 18,75% 28,13% 16,67%

Gestionar el programa de gestión de incidentes de seguridad de la información	9,47%	11,58%	14,74%	14,74%	28,42%	21,05%
Implementación de controles de TI en materia de seguridad de la información	12,75%	14,71%	13,73%	14,71%	28,43%	15,69%
Informar a la alta gerencia sobre el avance del programa de seguridad de la información	11,21%	13,08%	13,08%	16,82%	26,17%	19,63%
Interacción con las diferentes áreas de negocio	13,98%	13,98%	11,83%	17,20%	26,88%	16,13%
Seguimiento de prácticas en materia de protección de la privacidad de la información personal	18,03%	14,75%	14,75%	11,48%	29,51%	11,48%
Seguimiento de prácticas en materia de seguridad de la información	13,46%	13,46%	10,58%	14,42%	30,77%	17,31%
Supervisar procesos de cumplimiento regulatorio en tecnología de información	12,33%	13,70%	12,33%	13,70%	35,62%	12,33%
Supervisar y gestionar los procesos de investigaciones forenses digitales	12,73%	9,09%	14,55%	12,73%	32,73%	18,18%
Velar por la protección de la información personal	21,43%	14,29%	9,52%	11,90%	28,57%	14,29%

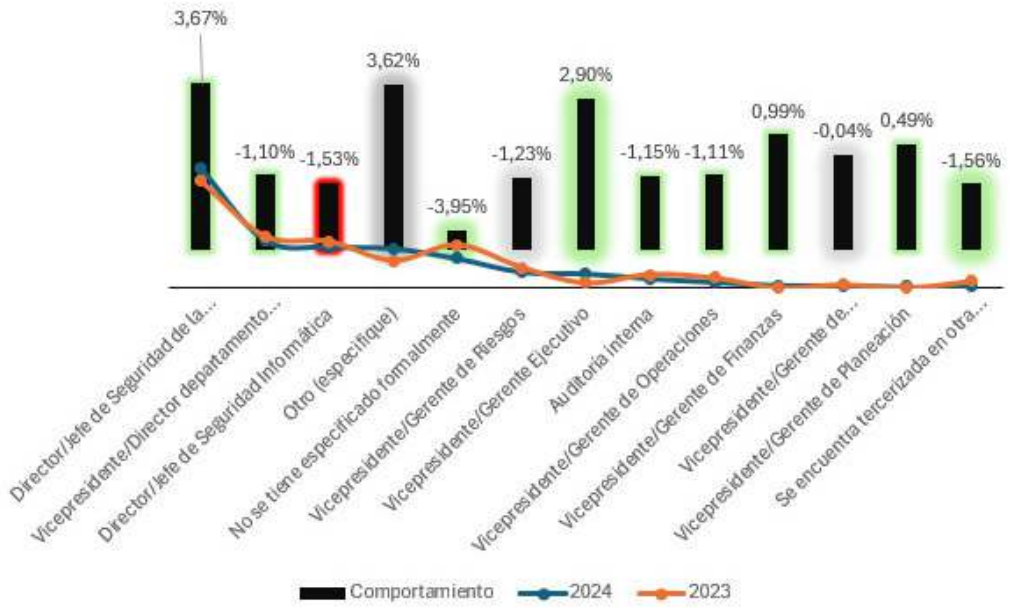
ciones y por último las mayores de 1000, velar por sus riesgos, desarrollar resiliencia, gestionar incidentes y saber que ocurre son las acciones que muestran mejor su madurez.

Seguimos en un proceso de cambios y transformaciones que ha afianzado al trabajo remoto, los ambientes híbridos como realidades que se han plasmado en la vida de las personas y de las organizaciones, que han hecho que el profesional de seguridad tenga que repensar la forma en como desarrolla su función y que reta la práctica, en donde se hace necesario que nuevos aprendizajes y nuevas formas de visualizar el futuro sean posibles. No es posible aprender del futuro, si este no se visualiza en el presente y la realidad existente (Martínez, J., 2021).

Dependencia de la seguridad

Con el pasar de los años se ve a un área de seguridad mucho más empoderada y posicionada, los datos ratifican que hay mejoras en la dependencia de seguridad, que soportan la idea de un área que sigue su proceso de consolidación en las empresas.

Este año se ven cambios importantes frente al año inmediatamente anterior, por ejemplo, el sector salud a diferencia del año anterior muestra avances en la creación de áreas de seguridad y tener un director de esta para guiar todas las iniciativas de seguridad. La gráfica



Gráfica 7: Crecimiento de la dependencia del área de seguridad.

7 muestra la dependencia de la seguridad en la organización y en este caso una comparación con el año inmediatamente anterior.

Cabe resaltar que, la función de seguridad en todos los sectores de la industria se sigue posesionando, un crecimiento del año 2023 a 2024 en 3,67% muestra que se vuelve más importante y se evidencia como necesidad, tendencia que se puede evidenciar en múltiples informes de industria como (Cyber XM 2024; PwC 2024b). Otro de los aspectos relevantes es el crecimiento en 2,90% de la dependencia del área de seguridad de la dirección general, esto se puede explicar como contexto de los fenómenos recientes de ciberataques muy sonados como caso Solarwinds, MGM y otros ataques que han puesto en evidencia la importancia de la ciberseguridad y su relación con la dirección, así como, el incremento sostenido de las regulaciones, como el caso de las consideraciones de seguridad de la Security Exchange Comission (SEC) (Auditboard, 2024), quien ha creado reglas de cumplimiento para los cuerpos directivos y ejecutivos en los Estados Unidos, de la misma manera ha pasado en Europa con la regulación DORA (Digital Operational Resilience Act) que ha determinado reglas de juego en el escenario de la ciberseguridad que hace más demandante el trabajo para los equipos de seguridad y su relación con los cuerpos ejecutivos y directivos de la misma (PwC, 2024a; Deloitte, 2024a; Digital Institute, 2024; EY, 2024).

Dos de los resultados que llaman la atención, por un lado, un crecimiento del 3,62% que menciona que el área de seguridad depende de otras áreas, sin embargo, más por sintaxis que por nombre están asociados áreas de seguridad y riesgos que áreas diferentes a las que existen. El segundo resultado que es muy alentador es que hay una diminución cercana al 4% de los que no lo tienen formalmente definidos, eso es un gran avance y demasiado alentador, pues se ratifica la tendencia relacionada con la presencia del área de seguridad y ciberseguridad necesita su espacio en relación con la dinámica de los negocios digitales (ISACA, 2024).

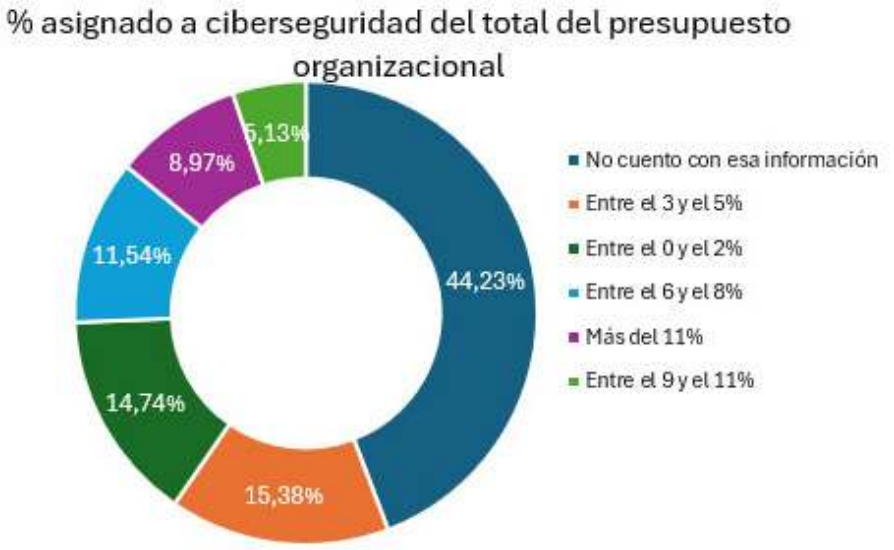
Mientras se siga avanzando en el desarrollo de la función de la seguridad en las organizaciones de Colombia como se viene dando, se seguirá mostrando unos aprendizajes que muy seguramente dejaran lecciones para optimizar y mejorar como igual se manifiesta en la tendencia mundial.

Presupuestos

Continúa la asignación de presupuestos para la ciberseguridad; en esta oportunidad el 82%, frente a un 18% que dice no tenerlo. Gráfica 8.

La gráfica 9 muestra el porcentaje que representa el presupuesto pa-

Gráfica 8: Presupuesto de Seguridad



Gráfica 9: Porcentaje del presupuesto Global

ra la ciberseguridad del total del presupuesto de la organización.

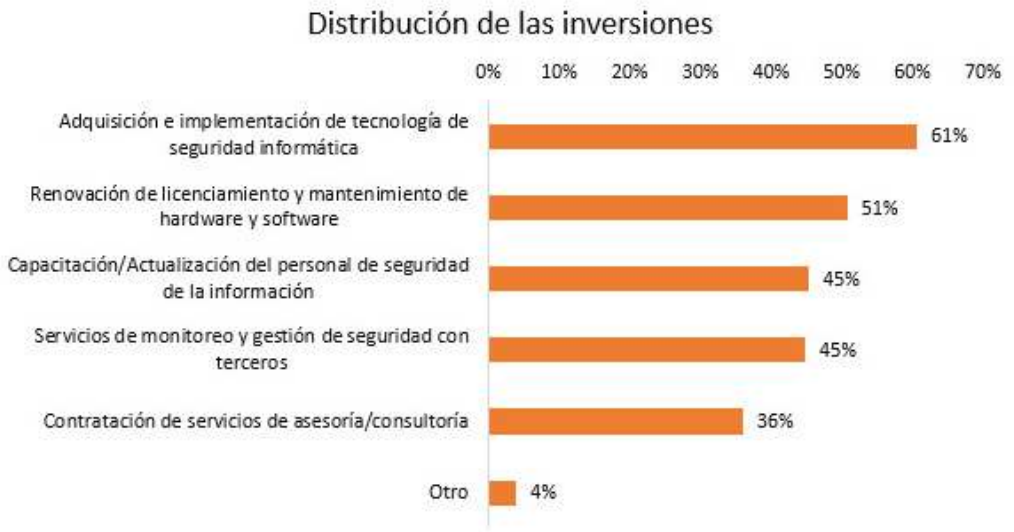
Cerca del 56% de los encuestados lo conoce, mientras que el otro 44% dice no conocer o no tener la información. De quienes conocen los montos asignados se puede observar que los montos inferiores al 5% del presupuesto global de la compañía representan el 30%, mientras que el 26% están para los montos superiores al 5%. Entre el 0 y 2% representa un 15%, entre 3 y el

Gráfica 10: Presupuesto de Seguridad

5% representa el 15%, 9% es más del 11%, y entre el 9 y 11% es el 5%, mientras que entre el 6 y el 8% representa el 12%.

La gráfica 10 refleja los montos asignados en las organizaciones para la ciber-seguridad. Para este año cerca del 50% tiene un monto asignado para la seguridad; que disminuye comparado con el año pasado cerca de un 9%, por su parte el 50% dice no conocer cuánto es el presupuesto asignado para la ciber-seguridad. Para este año cerca de un 10% dice que asigna menos de $US20.000 dólares americanos en sus presupuestos, seguido 6% que corresponde a la franja entre $US20.000 y $US50.000; siguiente es el 17% que corresponde a los presupuestos por encima de $US-130.000, el 3% asigna entre $US-90.000 y $US110.000, el 6% asigna entre $US50.000 a $US70.000, 3% asigna entre $US70.000 a $US90.000 y 5% entre $US-110.000 a $US130.000 dólares americanos.

La gráfica 11 muestra la forma cómo se está invirtiendo el dinero en materia de ciberseguridad. El 61% invierte en la adquisición e implementación de tecnología de seguridad, el 51% invierte en renovación de licenciamiento, el 45% invierte en capacitación del personal de seguridad, así como en los servicios de monitoreo y gestión, el 36% invierte en y contratación de servicios de consultoría.



Gráfica 11: Inversión de Seguridad

Consideraciones de los datos

Inversiones en ciberseguridad

Este año hay varias consideraciones importantes, al analizar el tamaño de las empresas, los sectores de industria y los montos asociados se encuentran algunos datos muy interesantes.

1. El sector salud, es el sector que menos conoce cuanto se invierte en la ciberseguridad y particularmente en las empresas del tamaño de los 1000 a 5000 empleados.
2. El sector financiero en las empresas de más de 5000 empleados es la que invierte más en la franja de los $US 130.000 dólares, que puede estar explicado por todo el marco regulatorio tanto nacional como internacional que existe y que es una de las tendencias claves del año 2024 (WEF, 2024c; WEF 2024a; CyberXM, 2024)
3. En la franja de los $US 0 hasta los $US 70.000 dólares la consultoría especializada de 1 a 50 empleados, son las empresas que hacen más inversiones, en dichas franjas los otros sectores de empresas hasta de 500 empleados invierten de la misma manera. Tendencia que nos aleja de la realidad de otras latitudes como Estados Unidos (Connectwise, 2024).
4. En la banda de los $US70.000 hasta $US90.000 dólares, los sectores de telecomunicaciones, financiero, consultoría especializada en las franjas desde 200 hasta 1000 empleados son los más representativos en esas inversiones.
5. Las empresas del sector financiero medianas (entre 200 y 500

empleados) son las que invierten en la banda de los $US 110.000 a $US130.000 dólares.

6. En la banda de inversiones de los $US90.000 a $US110.000 las empresas del sector público, financiero y consultoría resaltan por sus inversiones entre las empresas de 200 a 1000 empleados.

La tabla 3, se deja para el lector y pueda revisar más valores los cuales están disgregados todos los criterios anteriormente analizados.

Tabla 3: Distribución de Inversión por Tamaño de empresa y sector

Etiquetas de fila	No cuento con esa información	Más de USD$130.001	Menor de USD$20.000	Entre USD$20.001 y USD$50.000	Entre USD$50.001 y USD$70.000	Entre USD$110.001 y USD$130.000	Entre USD$70.001 y USD$90.000	Entre USD$90.001 y USD$110.000	Total general
1001 - 5000 empleados									
Educación	4,61%	0,66%							5,26%
Otro (especifique)	1,97%	1,32%				1,32%			4,61%
Servicios Financieros y Banca	1,97%	1,32%				0,66%	0,66%		4,61%
Gobierno / Sector público	3,29%	0,66%						0,66%	4,61%
Consultoría Especializada	3,29%								3,29%
Telecomunicaciones	1,32%	0,66%					0,66%		2,63%
Construcción / Ingeniería	1,32%								1,32%
Salud	1,32%								1,32%
501 - 1000 empleados									
Otro (especifique)	1,97%	1,32%	0,66%	0,66%	1,32%	0,66%			6,58%
Servicios Financieros y Banca	2,63%	0,66%				0,66%	0,66%	0,66%	5,26%
Educación	1,97%	0,66%	0,66%						3,29%
Gobierno / Sector público	1,97%								1,97%
Consultoría Especializada	0,66%						0,66%		1,32%
Sector de Energía e Hidrocarburos				0,66%					0,66%
Mayor de 5001 empleados									
Otro (especifique)	1,32%	1,97%			1,32%				4,61%
Servicios Financieros y Banca	1,32%	2,63%							3,95%
Consultoría Especializada	1,97%	1,32%							3,29%
Sector de Energía e Hidrocarburos		0,66%			0,66%				1,32%
Salud	0,66%	0,66%							1,32%
Gobierno / Sector público	0,66%								0,66%
Telecomunicaciones				0,66%					0,66%
Educación	0,66%								0,66%
201 - 500 empleados									

Otro (especifique)	2,63%		1,32%						3,95%
Servicios Financieros y Banca						1,32%		0,66%	1,97%
Consultoría Especializada	0,66%				0,66%			0,66%	1,97%
Educación	0,66%		0,66%	0,66%					1,97%
Telecomunicaciones	1,32%								1,32%
Construcción / Ingeniería			0,66%			0,66%			1,32%
Sector de Energía e Hidrocarburos		0,66%							0,66%
Salud	0,66%								0,66%
1 - 50 empleados									
Consultoría Especializada	1,97%		1,32%	1,97%	1,32%				6,58%
Otro (especifique)	1,32%		0,66%						1,97%
Telecomunicaciones	0,66%		0,66%						1,32%
Sector de Energía e Hidrocarburos				0,66%					0,66%
Construcción / Ingeniería			0,66%						0,66%
Gobierno / Sector público	0,66%								0,66%
51 - 200 empleados									
Otro (especifique)	1,32%	0,66%	1,32%	0,66%					3,95%
Telecomunicaciones	1,32%			0,66%					1,97%
Consultoría Especializada	1,32%				0,66%				1,97%
Gobierno / Sector público		0,66%	0,66%						1,32%
Servicios Financieros y Banca							0,66%		0,66%
Salud	0,66%								0,66%
Construcción / Ingeniería	0,66%								0,66%
Total general	**50,66%**	**16,45%**	**9,21%**	**6,58%**	**5,92%**	**5,26%**	**3,29%**	**2,63%**	**100,00%**

La tabla 4, relaciona las inversiones de seguridad por sectores de las empresas colombianas, teniendo que el valor mayor de todos los sectores se da en el rubro de entrenamiento de las personas de seguridad "Capacitación/Actualización del personal de seguridad de la información" que además lo hace el sector de la consultoría especializada con un 28%, este mismo rubro es el valor mayor valor para el sector de las telecomunicaciones con un 14%, tendencia interesante y que se conecta con la realidad del mantenimiento del talento de seguridad (ISC2, 2024; Kaspersky 2024b; ISC, 2024b, ISC, 2024c), que se ha convertido en un reto para las empresas, por tanto una estrategia clara es fortalecer al talento existente razón por la cual estrategias como el upskilling o fortalecimiento del talento y el reskilling desarrollo de talento nuevo dentro de las empresas toman fuerza en el mundo de la ciberseguridad (WEF, 2024b).

Al revisar en profundidad como se distribuye esas inversiones en los sectores de industria y el tamaño de las empresas, encontramos que, el sector de la consultoría especializada en las empresas de 1 a 50 empleados es donde más se in-

Tabla 4: Distribución de tipos de inversiones por sectores

Inversiones / Sectores	Consultoría Especializada	Educación	Gobierno / Sector público	Salud	Sector de Energía e Hidrocarburos	Servicios Financieros y Banca	Telecomunicaciones
Servicios de monitoreo y gestión de seguridad con terceros	25,00%	9,38%	15,63%	7,81%	6,25%	26,56%	9,38%
Adquisición e implementación de tecnología de seguridad informática	25,00%	15,00%	8,75%	5,00%	6,25%	26,25%	13,75%
Renovación de licenciamiento y mantenimiento de hardware y software	25,71%	15,71%	14,29%	8,57%	2,86%	22,86%	10,00%
Contratación de servicios de asesoría/consultoría	26,92%	11,54%	13,46%	7,69%	7,69%	25,00%	7,69%
Capacitación/Actualización del personal de seguridad de la información	27,69%	12,31%	6,15%	7,69%	6,15%	26,15%	13,85%

vierte para capacitar al personal de seguridad. Para el sector financiero la contratación de servicios de consultoría en las empresas de hasta 5000 empleados es el valor más alto, la adquisición de soluciones de seguridad en las empresas de hasta 1000 empleados es el valor mayor, y los servicios de monitoreo y gestión de seguridad con terceros en las empresas de más de 5000 empleados, son las inversiones más representativas. El sector de la consultoría especializada de empresas entre 200 y 500 empleados se invierte en el monitoreo como inversión más representativa, mientras que el sector de las telecomunicaciones en las empresas de 50 a 200 empleados, la adquisición de

soluciones de seguridad informática es lo más representativo, estos datos y más pueden ser vistos en la tabla 5.

Tabla 5

Etiquetas de fila	1 - 50 empleados	1001 - 5000 empleados	201 - 500 empleados	501 - 1000 empleados	51 - 200 empleados	Mayor de 5001 empleados	Total general
Consultoría Especializada							
Servicios de monitoreo y gestión de seguridad con terceros	6,25%	3,13%	4,69%	3,13%	3,13%	4,69%	25,00%
Adquisición e implementación de tecnología de seguridad informática	8,75%	2,50%	3,75%	2,50%	2,50%	5,00%	25,00%
Renovación de licenciamiento y mantenimiento de hardware y software	10,00 %	4,29%		1,43%	2,86%	7,14%	25,71%
Contratación de servicios de asesoría/consultoría	7,69%	7,69%	1,92%	3,85%	1,92%	3,85%	26,92%
Capacitación/Actualización del personal de seguridad de la información	10,77 %	4,62%	1,54%	1,54%	1,54%	7,69%	27,69%
Educación							
Servicios de monitoreo y gestión de seguridad con terceros		4,69%	1,56%	3,13%			9,38%
Adquisición e implementación de tecnología de seguridad informática		6,25%	3,75%	5,00%			15,00%
Renovación de licenciamiento y mantenimiento de hardware y software		5,71%	4,29%	4,29%		1,43%	15,71%
Contratación de servicios de asesoría/consultoría		5,77%	1,92%	3,85%			11,54%
Capacitación/Actualización del personal de seguridad de la información		4,62%	1,54%	4,62%		1,54%	12,31%
Gobierno / Sector público							
Servicios de monitoreo y gestión de seguridad con terceros		7,81%		3,13%	3,13%	1,56%	15,63%
Adquisición e implementación de tecnología de seguridad informática		5,00%		1,25%	1,25%	1,25%	8,75%
Renovación de licenciamiento y mantenimiento de hardware y software	1,43%	4,29%		4,29%	2,86%	1,43%	14,29%
Contratación de servicios de asesoría/consultoría		5,77%		5,77%		1,92%	13,46%
Capacitación/Actualización del personal de seguridad de la información	1,54%	1,54%		1,54%		1,54%	6,15%
Salud							
Servicios de monitoreo y gestión de seguridad con terceros		3,13%	1,56%			3,13%	7,81%
Adquisición e implementación de tecnología de seguridad informática		1,25%	1,25%			2,50%	5,00%
Renovación de licenciamiento y mantenimiento de hardware y software		2,86%	1,43%		1,43%	2,86%	8,57%
Contratación de servicios de asesoría/consultoría		1,92%	1,92%		1,92%	1,92%	7,69%
Capacitación/Actualización del personal de seguridad de la información		3,08%	1,54%		1,54%	1,54%	7,69%
Sector de Energía e Hidrocarburos							
Servicios de monitoreo y gestión de seguridad con terceros			1,56%	1,56%		3,13%	6,25%

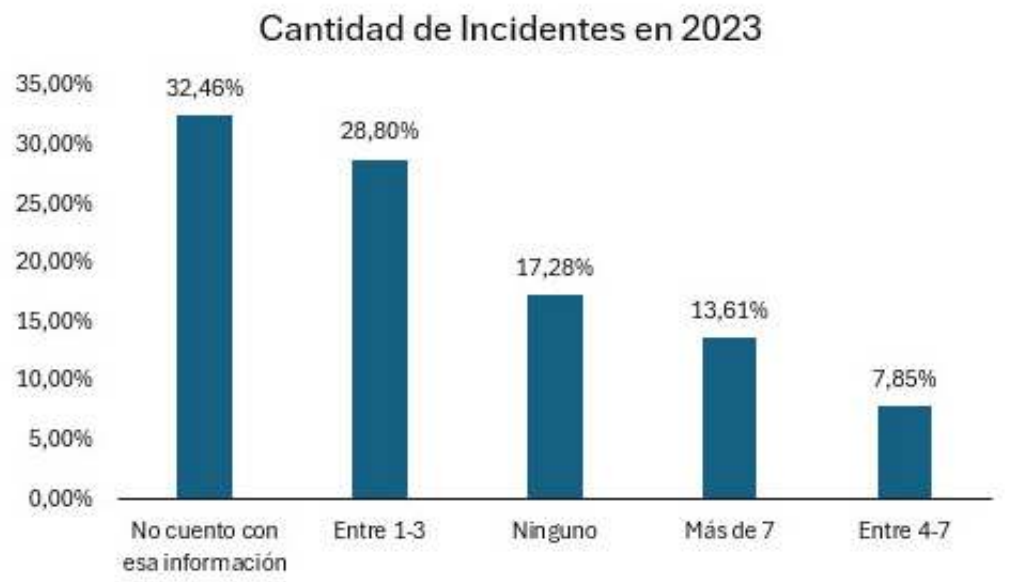
Adquisición e implementación de tecnología de seguridad informática	1,25%		1,25%	1,25%		2,50%	6,25%
Renovación de licenciamiento y mantenimiento de hardware y software			1,43%			1,43%	2,86%
Contratación de servicios de asesoría/consultoría			1,92%	1,92%		3,85%	7,69%
Capacitación/Actualización del personal de seguridad de la información			1,54%	1,54%		3,08%	6,15%
Servicios Financieros y Banca							
Servicios de monitoreo y gestión de seguridad con terceros		7,81%	3,13%	6,25%	1,56%	7,81%	26,56%
Adquisición e implementación de tecnología de seguridad informática		6,25%	3,75%	8,75%	1,25%	6,25%	26,25%
Renovación de licenciamiento y mantenimiento de hardware y software		7,14%	1,43%	7,14%		7,14%	22,86%
Contratación de servicios de asesoría/consultoría		9,62%	1,92%	5,77%		7,69%	25,00%
Capacitación/Actualización del personal de seguridad de la información		7,69%	1,54%	7,69%	1,54%	7,69%	26,15%
Telecomunicaciones							
Servicios de monitoreo y gestión de seguridad con terceros		4,69%	1,56%		3,13%		9,38%
Adquisición e implementación de tecnología de seguridad informática	2,50%	5,00%	1,25%		3,75%	1,25%	13,75%
Renovación de licenciamiento y mantenimiento de hardware y software	1,43%	2,86%	1,43%		2,86%	1,43%	10,00%
Contratación de servicios de asesoría/consultoría		5,77%	1,92%				7,69%
Capacitación/Actualización del personal de seguridad de la información	3,08%	6,15%	1,54%		1,54%	1,54%	13,85%

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, 2024).

Hoy por hoy en Colombia se confirma que las organizaciones están asignando presupuesto, aun así, sigue siendo algo para observar porqué 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 encuesta no tenga acceso a dicha información.

Incidentes

La gráfica 12 representa la cantidad de incidentes que para este año los encuestados manifestaron que se presentaron. Para este año cerca del 50% de los encuestados manifiesta que ha estado en contacto con algún incidente de seguridad en su empresa con un crecimiento del 2% general frente al año inmediatamente anterior. El 33% manifiesta no tener información al



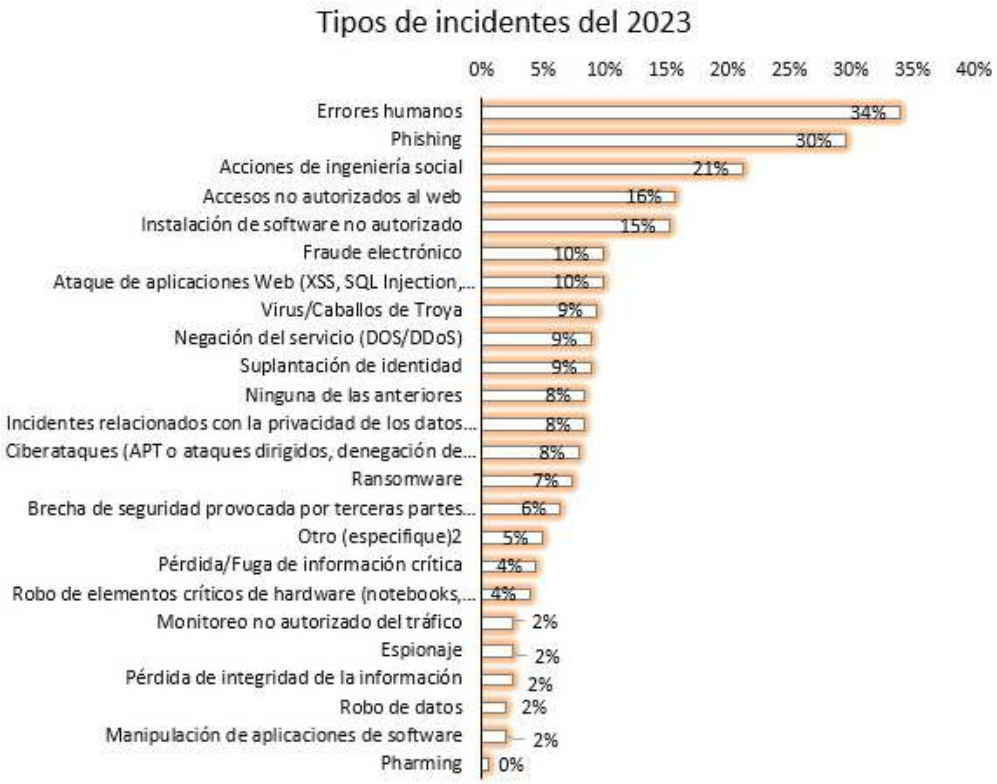
Gráfica 12: Cantidad de Incidentes.

respecto de los incidentes en sus organizaciones, al revisar los detalles se encuentra que el 29% manifiesta haber experimentado entre 1 y 3 incidentes, 14% más de 7 incidentes y 8% entre 4 y 7 incidentes, así mismo, el 17% manifiesta que no ha tenido incidentes.

La gráfica 13 relaciona los tipos de incidentes que se presentaron en las organizaciones, Errores humanos (34%), Phishing (30%) y acciones de ingeniería social (21%) son los tres primeros que han sido identificados en este año. Si bien comparados con el año pasado disminuyen un poco todos los valores los cambios no son significativos para decir que hay un cambio de tendencia.

La gráfica 14 representa el costo promedio de los incidentes cibernéticos en las empresas colombianas, el 87% manifiesta que los costos estimados totales luego de sufrir un incidente están por debajo de los $US50.000 dólares americanos, entre $US50.000 y $US100.000 solo el 9%, más de $US150.000 el 3% y entre $US100.000 y $US150.000 dólares americanos el 1%

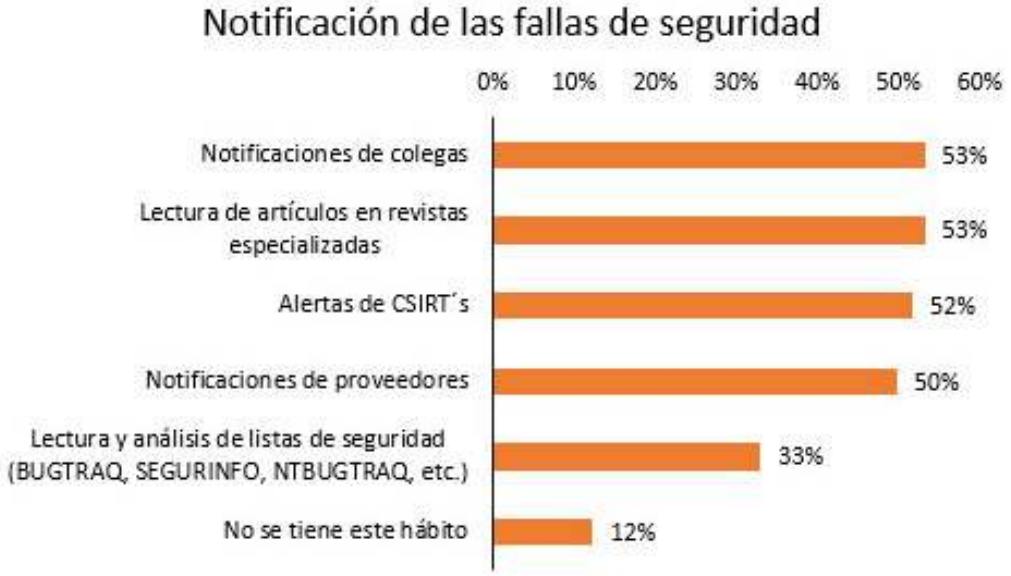
La gráfica 15, muestra ante quién se reportan los incidentes de seguridad. El 67% lo reporta directamente a los directivos de la organización, el 44% lo reporta al equipo de atención de incidentes (CSIRT), el 32% a las autoridades nacionales, el 26% a los asesores legales, el 20% a autoridades locales o regionales y solo el 5% manifiesta que no se denuncian. Para este año hubo más reporte hacia los directivos un aumento del 4% y una



Gráfica 13: Tipos de Incidentes de Seguridad

Gráfica 14 Costos de los Incidentes

Gráfica 15: A quien se reportan los incidentes



Gráfica 16: Notificación de las fallas de seguridad

disminución del 3% de reportes ante los CSIRT, otro dato interesante que se mantiene en el 5% igual aquellos que no dicen nada o no notifican nada de sus incidentes.

La gráfica 16, muestra como los profesionales de ciberseguridad se mantienen informados sobre las vulnerabilidades y fallas de los sistemas. El 53% de los profesionales

Contacto con autoridades	Porcentaje
No	39%
Si	61%

Tabla 6: Contacto con autoridades

de seguridad se enteran a través de colegas en primera medida, seguido de la lectura de artículos especializados o revistas 53%, la notificación de un CSIRT ocupa el tercer lugar con el 52%, el cuarto lugar las notificaciones de los proveedores 50%, lectura de listas de seguridad 33% y 12% no tiene el hábito.

Comparado con el año pasado hay un drástico cambio, primera vez que se ve que los profesionales estrechan sus relaciones de confianza con sus pares, la cooperación entre pares se está convirtiendo en una fortaleza, la creación de comunidades se fortalece como lo sugieren distintos informes de industria.

La tabla 6 se resalta que el 61% de las personas encuestadas si tienen contacto con las autoridades, mientras que el 39% no lo posee.

En cuanto la evidencia digital, los datos muestran que, 77% de los encuestados si es consciente del manejo de la evidencia digital y que es requerida como parte del proceso de la gestión de incidentes, el 18% no sabe del tema y solo el 4% no es consciente, frente al año anterior hay cambios importantes incremento de un 6% de la conciencia, y disminución en un 10% de aquellos que no son conscientes de la misma.

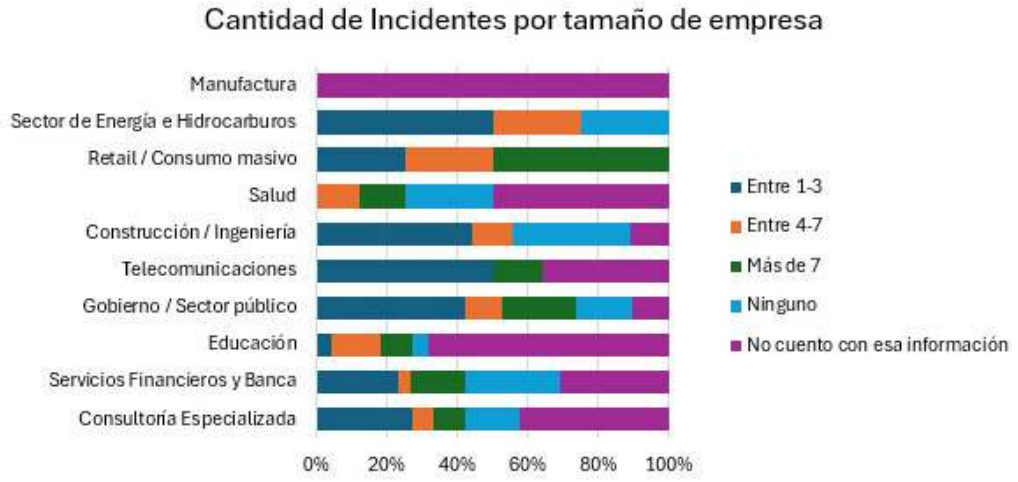
La consciencia hay que llevarla a la práctica, a través de la formalización y de la implementación, el 51% manifiesta no tener formalizado o la existencia de un procedimiento de este estilo en la empresa, y el 49% manifiesta que sí; y al revisar la implementación de estos procedimientos, el 36% manifiesta tener un procedimiento implementado para la gestión de incidentes, el 29% lo tienen de manera informal y el 35% no lo sabe o no lo tiene. Al revisar en más detalles y ver que tanto se han implementado estos procedimientos se encuentra que

Consideraciones de los datos

Frecuencias de los incidentes

Explorando la forma en como en Colombia los distintos sectores de la industria experimentan los distintos incidentes, la gráfica 17, muestra como los distintos sectores de industria sufren las distintas franjas de incidentes.

Lo primero para resaltar es que todos los sectores más representativos y los otros sectores experimen-



Gráfica 17: Cantidad de Incidentes por sectores

tan incidentes cibernéticos, tendencia que se confirma a través de reportes como (Verizon, 2024; CyberEdge, 2024; ITRC, 2024; Cano & Almanza, 2021).

Consecuente con las dinámicas de los ciberataques, vemos que el sector salud que es uno de los sectores más atacados de la industria (Kroll, 2024; Claroty, 2024), manifiesta que su mayor valor es no contar con la información sobre incidentes, esto puede estar explicado de dos maneras, una que quien diligencia la encuesta no conoce el proceso de gestión de incidentes, o dos que no se tengan los procesos de gestión de incidentes y lo exprese de esa manera, tendencia que también se puede ver reflejada en los reportes mencionados, así mismo, como tendencia global se ve que cada vez más los estados empiezan a preocuparse para que este sector tenga mayores regulaciones para poder gestionar los desafíos de ciberseguridad.

Al revisar con detalle estos datos, la tabla 7, los muestra por sectores, tamaños de empresas y la cantidad de estos, de los cuales se puede decir.

La tabla muestra que el sector de consultoría especializada en empresas pequeñas no tiene incidentes o al menos así lo manifiesta, posiblemente más asociado a la ausencia de procedimiento de gestión de incidentes y el monitoreo de estos a que los adversarios no consideren de valor dichos objetivos (Paloaltonetworks, 2024). En el mismo sector del tamaño de empresas de 50 a 200 empleados se presentan de 1 a 3 incidentes como el valor más presente, así mismo entre 4 y 7 incidentes tiene una re-

Tabla 7: Distribución de incidentes por sectores y tamaños

Cuenta de Incidentes 2023				
Sectores/Tamaños/Incidentes	**Entre 1-3**	**Entre 4-7**	**Más de 7**	**Ninguno**
Consultoría Especializada				
1 - 50 empleados	1,11%	2,22%		5,56%
51 - 200 empleados	4,44%			
501 - 1000 empleados	2,22%			
Mayor de 5001 empleados	1,11%		1,11%	
201 - 500 empleados	1,11%		1,11%	
1001 - 5000 empleados			1,11%	
Servicios Financieros y Banca				
1001 - 5000 empleados	2,22%			3,33%
501 - 1000 empleados	2,22%	1,11%	2,22%	
Mayor de 5001 empleados			2,22%	2,22%
201 - 500 empleados	1,11%			2,22%
51 - 200 empleados	1,11%			
Gobierno / Sector público				
1001 - 5000 empleados	3,33%	1,11%	3,33%	2,22%
51 - 200 empleados	2,22%			1,11%
501 - 1000 empleados	1,11%	1,11%	1,11%	
Mayor de 5001 empleados	1,11%			
1 - 50 empleados	1,11%			
Telecomunicaciones				
1 - 50 empleados	3,33%			
1001 - 5000 empleados	1,11%		1,11%	
51 - 200 empleados	2,22%			
Mayor de 5001 empleados			1,11%	
201 - 500 empleados	1,11%			
Construcción / Ingeniería				
1001 - 5000 empleados	1,11%	1,11%		
201 - 500 empleados	1,11%			1,11%
1 - 50 empleados	1,11%			1,11%
51 - 200 empleados	1,11%			1,11%
Educación				
1001 - 5000 empleados	1,11%		2,22%	
201 - 500 empleados		1,11%		1,11%
51 - 200 empleados		1,11%		

501 - 1000 empleados		1,11%		
Sector de Energía e Hidrocarburos				
Mayor de 5001 empleados				1,11%
501 - 1000 empleados	1,11%			
1 - 50 empleados	1,11%			
201 - 500 empleados		1,11%		
Salud				
51 - 200 empleados		1,11%	1,11%	
Mayor de 5001 empleados				1,11%
1001 - 5000 empleados				1,11%
Retail / Consumo masivo				
Mayor de 5001 empleados			2,22%	
1001 - 5000 empleados	1,11%	1,11%		
Total general	**42,22%**	**13,33%**	**20,00%**	**24,44%**

presentación mayor que las demás franjas de incidentes para el mismo sector.

El sector de Gobierno es el que más experimenta incidentes según los datos analizados en este periodo, es la franja de más de 7 incidentes la que tiene una porción mayor, cosa que se mantiene basado en las tendencias de reportes de industria, donde se muestran que uno de los sectores más atacados es precisamente el sector de gobierno (Darkreading, 2024; Kaspersky, 2024a)

No todas las verticales empresariales en Colombia tiene los mismos tipos de incidentes, la tabla 6, la cual muestra dos visiones, la primera visión resalta el top 3 de tipos de incidentes por sector, la segunda parte resalta el top 1 en materia de el tipo de incidente del total de veces que se presenta.

De las tablas se pueden resaltar los siguientes aspectos

1. Todos los sectores de la industria nacional sufren algún tipo de ciber incidente
2. El top 5 de los incidentes de todas las industrias son Errores humanos, phishing, acceso no autorizado al web, instalación de software no autorizado y los ataques de ingeniería social como lo más representativo
3. Los errores humanos es el incidente que es común a todos los sectores
4. Phishing es el segundo, sin embargo, no es el más presente en todos los sectores.

Tabla 8: Sectores representativos e incidentes

Sectores Representativos	Incidente más representativo
Consultoría Especializada	Manipulación de aplicaciones de software
Educación	Ransomware
Gobierno / Sector público	Pérdida/Fuga de información crítica
Salud	Virus/Caballos de Troya
Servicios Financieros y Banca	Pérdida de integridad de la información
Telecomunicaciones	Robo de datos

La tabla 8 muestra para los sectores más representativos de la industria colombiana, los incidentes más representativos.

Las tendencias de Colombia en materia de la presencia de los incidentes cibernéticos no se alejan de las tendencias internacionales, por una parte, los errores humanos se han resaltados en reporte de industria como, donde la variedad de técnicas novedosa que usan los adversarios digitales pone demasiada presión en las personas y los inducen en muchos casos a errores (Proofpoint, 2024; FS-ISAC, 2024).

Frente al año anterior, el Phishing, Ransomware, Ingeniería Social y Errores Humanos, son los que más variaciones tuvieron, fenómenos que no se alejan de los reportes y tendencias internacionales que son analizados a través de reportes de industria, el reporte de Verizon (Verizon, 2024; FBI, 2024) manifiesta que el Phishing sigue siendo la técnica más usada por los cibercriminales. la firma Knowbe4 resalta que los sectores de la industria como el sector salud, educación, consultoría y asegurador son los sectores que sin importar el tamaño de la empresa están más expuestos a ataques de phishing (Knowbe4, 2024). Intel471 en su reporte del año resalta que muchos de los ataques observados siguen evolucionando, usando la inteligencia artificial no solo para acelerar el proceso de phishing también para innovar en las técnicas alrededor del mismo (Intel471, 2024). Según Egress en su informe sobre los ataques de Phishing el 77% de los casos son ataques que personalizan a grandes marcas del mercado (Egress, 2024).

La ingeniería social como otra de las técnicas usadas es una tendencia global, donde las víctimas usan la conversación para construir confianza y se valen de cualquier método para poder engañar a sus víctimas y son los temas de la actualidad, relevancia y los que socialmente conectan los que son más usados (Proofpoint, 2023).

Aplicaciones, datos y nube, son tres de las grandes incógnitas de

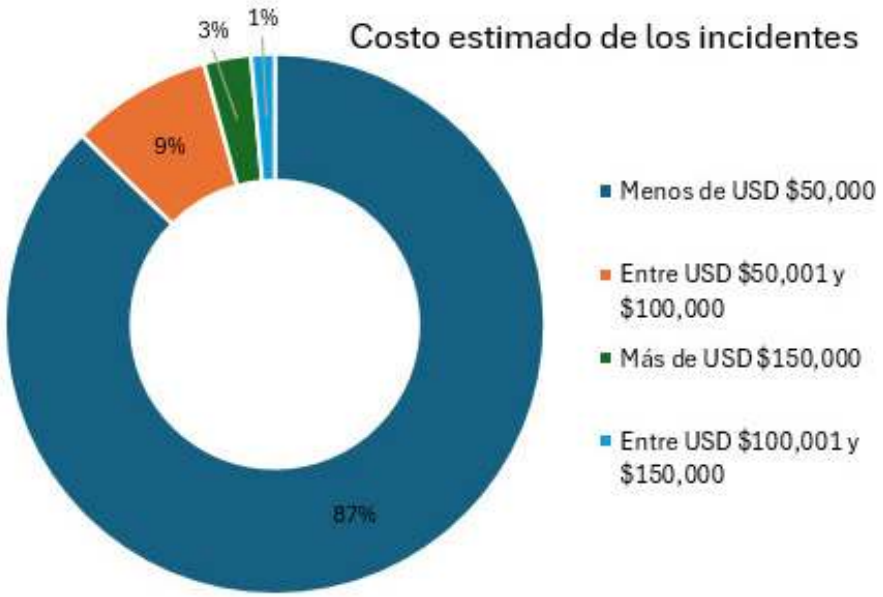
las empresas, el informe de Thales resalta que el 33% de los participantes del estudio tienen como prioridad la protección de ellos (Thales, 2024), gran relación con los ataques en la nube y aplicaciones que son uno de los criterios de incidentes representativos. En el reporte de Orca se identifica que el 62% de las organizaciones tienen vulnerabilidades severas en repositorios de la nube (Orca, 2024).

Costos de los incidentes

Los costos de los incidentes tienen un comportamiento y cada vez que hay en los distintos sectores de la industria colombiana nuevos patrones que muestran la dinámica de cómo son estos, y cuáles son sus costos. La gráfica 18, representa los costos de los incidentes por sectores de industria. Se ratifica la tendencia que los incidentes cuestan en su gran mayoría menos de 50.000 dólares americanos, con el 87%.

Del cuál se puede extraer lo siguiente:

1. Con relación al año anterior, hay una variación interesante del 3% en el valor estimado de los costos de un incidente en la franja de hasta 50 mil dólares americanos, esta lectura puede ser asociada a una mejor forma de estimación de los costos, o un poco más de conciencia de que un ataque cibernético, así mismo podría como lectura complementaria es empezar a visuali-

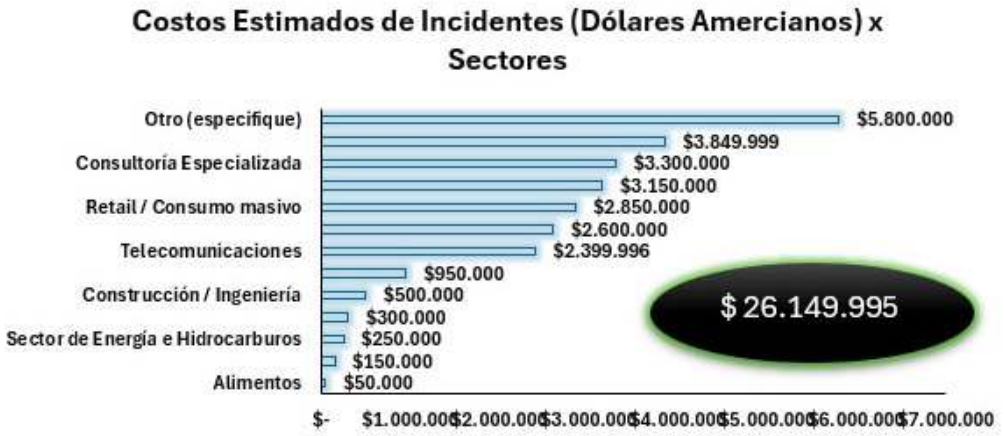


Gráfica 18: Costos de incidentes por industria

zar los costos ocultos de los ataques cibernéticos (Splunk, 20-24b).

2. Solo el sector financiero ha manifestado para este año tener incidentes que han costado más de 150 mil dólares americanos. El sector de gobierno y de las telecomunicaciones tiene valores entre los 100 mil y 150 mil dólares americanos.
3. El orden de la presencia de incidentes cibernéticos está determinado por el primer lugar la consultoría especializada, el sector financiero, educación, gobierno, telecomunicaciones y salud. Si bien la tendencia de Colombia se desconecta un poco de la realidad internacional donde el sector salud está entre los primeros, se mantiene en el margen de la tendencia pues si presenta incidentes cibernéticos, casos como CAFAM, Audifarma, Sanitas, pues muestran que es real la presencia de los incidentes en este sector.

Para este año analizando los datos recolectados, se ha determinado el costo total aproximado de los incidentes por sector de la industria, el cual se refleja en la gráfica 19. El costo total estimado de los incidentes para todos los tipos de incidentes monitoreados y sectores de la industria se estimó en un costo superior a los 26Millones de dólares americanos, teniendo un decrecimiento con el mismo ejercicio del año anterior del 7%. Se puede ver que, para otros sectores de la industria, aquellos que no se identifican con la clasificación oficial de la encuesta, el costo estimado es de 5,8 Millones de dólares americanos, sigue el sector de gobierno con casi 3,9 Millones de dólares, el sector de la consultoría con 3,3 Millones de dólares, siendo los sectores más representativos.

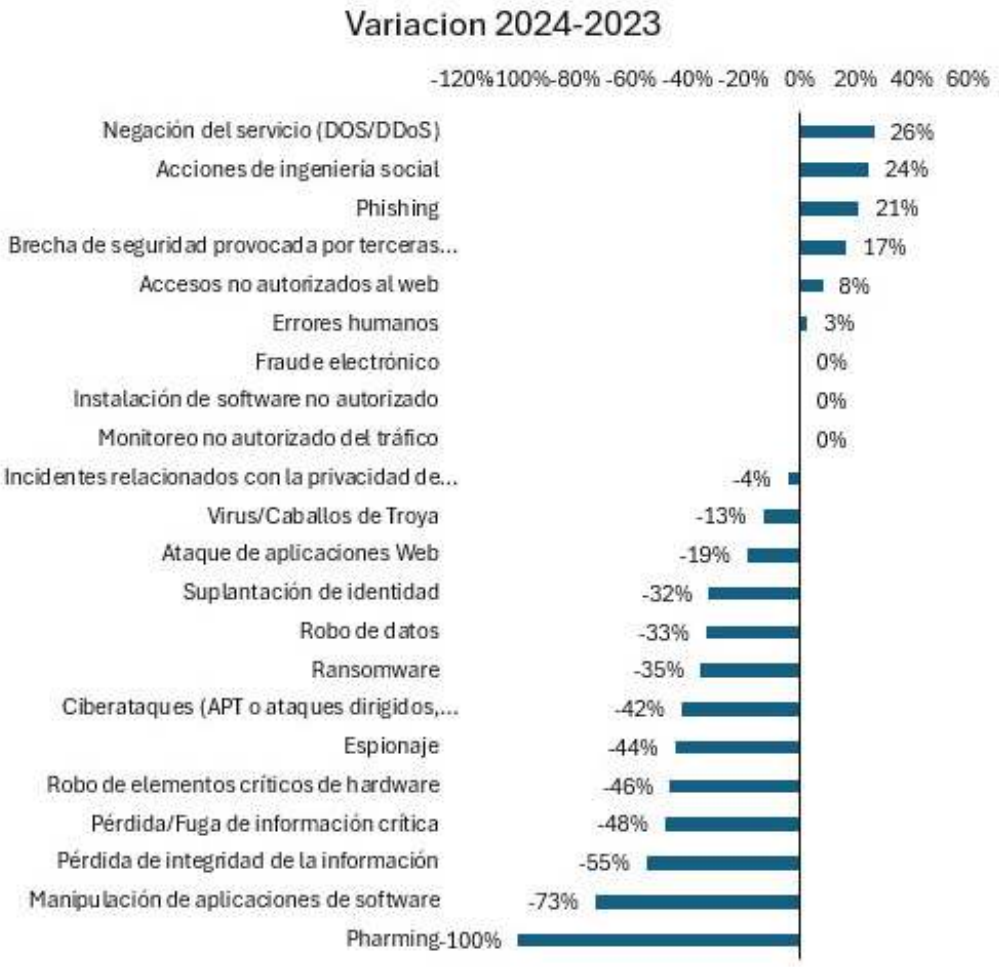


Gráfica 19 Costos de los incidentes x sectores de industria

Gráfica 20 Costos totales por tipo de incidente

La gráfica 20, muestra la distribución de los costos por tipo de incidente, en el cual tenemos que los errores humanos es el incidente que más les cuesta a las empresas colombianas en un total aproximado de $US 3.750.000 dólares, phishing seguido con 3.450.000 mil dólares, y acciones de ingeniería social $US2.550.000.

Comparando los datos con el año inmediatamente anterior y viendo que tanto crecieron los incidentes en los distintos sectores de la industria de Colombia, tenemos la gráfica 21, que muestra la variación del año 2023 al 2024. De los cuales se puede deducir lo siguiente, los ataques de denegación de servicio tuvieron un crecimiento importante en las empresas colombianas, el incremento fue del 26%, las acciones de ingeniería social con un 24% de crecimiento, phishing 21%, las brechas que involucran a terceras partes tuvieron un incremento del 17%, el acceso no autorizado al web tuvo un crecimiento del 8% y los errores humanos un crecimiento del 3%, estos fueron los que más crecieron y variaron, mientras que el que más decreció fue el pharming que este año no tuvo presen-



Gráfica 21 Variación de los incidentes 2023-2024

cia como incidente y por tanto su decrecimiento es del 100%, los ataques tradicionales también decrecen, y esto no significa que no sucedan, las implicaciones de esto están en que los adversarios cada vez aprovechan las múltiples vulnerabilidades que aparecen en las infraestructuras, soportadas en los cambios y las dinámicas de las empresas, (Sophos, 2024; Zidkova, 2024; Edgescan, 2024; Bugcrowd, 2024).

En el gráfico 22, se tiene la distribución normal de los incidentes cibernéticos de todos los sectores analizados. Hoy se puede afirmar con los datos obtenidos de la encuesta, que los incidentes cibernéticos en promedio le pueden costar a una empresa entre 50.000 dólares americanos y cerca de 3.8 millones de dólares, siendo la franja de $100.000 dólares hasta $US 2.900.000 millones de dólares el costo en el que más oscila los inci-

Gráfica 22 Distribución de costos de incidentes cibernéticos

Cuenta de Pais	Etiquetas de columna				
Etiquetas de fila	Menos de USD $50,000	Entre USD $50,001 y $100,000	Más de USD $150,000	Entre USD $100,001 y $150,000	Total general
Entre el 0 y el 2%	**21,57%**	**1,96%**	**1,96%**		**25,49%**
Entre 1-3	15,69%	1,96%	1,96%		19,61%
Entre 4-7	1,96%				1,96%
Más de 7	3,92%				3,92%
Entre el 6 y el 8%	**21,57%**	**1,96%**	**1,96%**		**25,49%**
Entre 1-3	15,69%	1,96%			17,65%
Entre 4-7	3,92%				3,92%
Más de 7	1,96%		1,96%		3,92%
Entre el 3 y el 5%	**21,57%**	**1,96%**			**23,53%**
Entre 1-3	9,80%				9,80%
Entre 4-7	9,80%				9,80%
Más de 7	1,96%	1,96%			3,92%
Más del 11%	**13,73%**	**1,96%**	**1,96%**		**17,65%**
Entre 1-3	5,88%				5,88%
Más de 7	7,84%	1,96%	1,96%		11,76%
Entre el 9 y el 11%	**5,88%**			**1,96%**	**7,84%**
Entre 1-3	3,92%			1,96%	5,88%
Entre 4-7	1,96%				1,96%
Total general	**84,31%**	**7,84%**	**5,88%**	**1,96%**	**100,00%**

Tabla 9: Costos de los incidentes vs Inversiones vs Cantidad de Incidentes

dentes cibernéticos en la industria nacional. Cabe mencionar que estos valores no son para un solo incidente sino la presencia de varios en las distintas industrias.

En este año al mezclar los datos de costos de incidentes vs inversiones del presupuesto global (Tabla 9), se puede determinar que las empresas que hacen menores inversiones tienen mayor probabilidad sin importar el tamaño, o el sector de evidenciar entre 1 a 3 incidentes, siendo esta la franja más probable, en la medida que se invierta más se puede disminuir la tasa de presencia de incidentes, sin embargo, no es que no se presenten ninguno de ellos.

Aquellos que invierten entre el 0 y 2% del total de su presupuesto para la ciberseguridad tienen un 22% más de probabilidad de que un incidente se presente, y exactamente un 16% que se presente entre 1 y 3 incidentes en las empresas de Colombia, si se revisa las otras franjas, lo que se puede ver es que en la medida que incremente las empresas su inversión en seguridad, disminuye en 2,3 y hasta 5 veces la posibilidad de que un incidente que se va presentar cueste menos de $US 50.000 dólares americanos. Es importante manifestar que invertir en seguridad no evitará que los incidentes no pasen, solo harán menos plausible que sus impactos tengan costos más manejables para la realidad de las empresas colombianas.

Al revisar las tendencias y reportes internacionales, se puede encontrar puntos en los cuales la realidad de Colombia se conecta la internacional.

Los ataques cibernéticos, siguen y seguirán creciendo en el caso de ataques usando el Phishing, los ataques de ingeniería social son marcas que se siguen viendo y más ahora con la presencia de la IA, (Mimecast, 2024), para Barracuda los ataques de correo electrónico y sobre todo el Business Email Compromose (BEC), suceden uno de cada 10 haciendo que exista y que sea exitoso, (Barracuda, 2024). El incremento de ataques con códigos QR incrementan y eso se ve inclusive en la realidad latinoamericana como tendencia, razón por la cual los ataques pueden ser exitosos (Cofense, 2024).

Los costos de los ciberataques crecen año tras año (Verizon, 2024; Sophos, 2024). En el caso de Ransomware para Colombia se siguen experimentando costos, es una tendencia creciente que ha mostrado que en la realidad nacional también este tipo de incidentes generan efectos en las empresas, y si bien el rigor diario de las noticias de ciberseguridad muestra permanentemente ataques de esta naturaleza, pues se ratifica que frente a otros tipos de ataques aún no están en los primeros lugares en términos de costos.

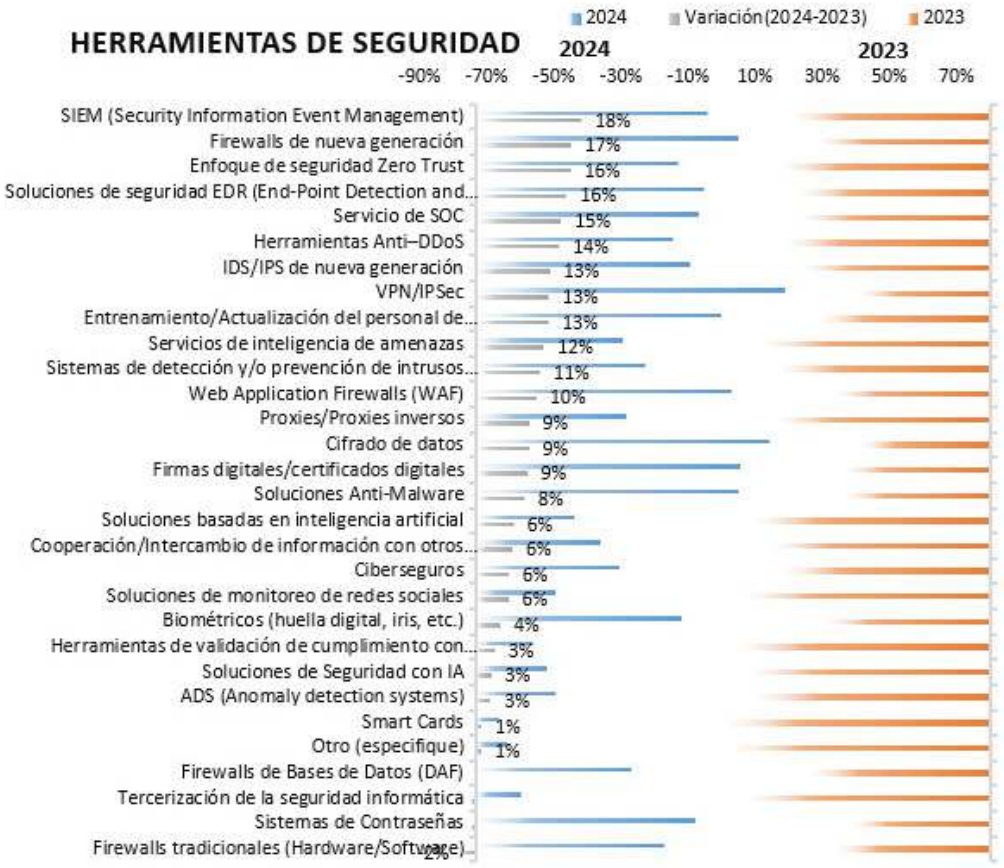
Los datos de Colombia muestran una desviación frente a la tendencia global en relación con el sector salud estudios como (Ponemon-Proofpoint, 2022; MinterEllison, 2023) muestran que es uno de los sectores más atacados (frecuencia) y su implicaciones e impactos (costos) elevados, mientras en Colombia no se ve esa misma tendencia, esto se puede explicar porque el sector de la salud de Colombia, se encuentra en un estado de aprendizaje y madurez de sus prácticas de ciberseguridad y por tanto las capacidades de tener procesos de gestión de incidentes y monitoreo de los mismos sea baja para poder identificar lo que sucede.

Herramientas

La gráfica 23, muestra la distribución del uso de las herramientas de seguridad en las empresas colombianas, en ella se evidencia que las VPNs, el cifrado de datos, los sistemas de contraseñas, las soluciones antimalware y las firmas digitales, corresponden al top 3 de herramientas más usadas en las empresas de todos los tamaños y sectores de la industria nacional.

Así mismo, la gráfica compara contra el año 2023, en las cuales se visualiza que las soluciones de SIEM, los firewalls de nueva generación, y el enfoque de zero trust son los tres frentes de trabajo que han variado más en ese orden respectivamente, es decir que para este año tuvo el uso de SIEM, los firewalls y los enfoque de zero trust fueron lo más usado (Scmagazine, 2024; Entrust, 2024; Moore et all, 2024).

La gráfica 24 muestra el comportamiento de como las organizaciones en Colombia por industria realizan una evaluación de la postura de se-



Gráfica 23: Herramientas de seguridad

Gráfica 24: Evaluaciones de Seguridad

guridad general. Para este año repunta al primer lugar que las empresas que realizan las evaluaciones de seguridad entre 2 y 4 veces al año en un 38%, una vez al año se hace en el 34% de las veces, 16% no hace ninguna valoración de seguridad y más de 4 veces al año la hacen cerca del 12%.

Al revisar los datos y disgregar por sectores y tamaños de empresas, podemos encontrar puntos de interés, el sector de gobierno en empresas de 1000 a 5000 empleados es la que más usa las evaluaciones de seguridad una vez por año, las evaluaciones de seguridad realizadas de 2 a 4 veces al año tienen un patrón distinto, por un lado las empresas de la consultoría especializada del tamaño de 1 a 50 empleados es quien lo hace, por el otro lado, las otras empresas del tamaño de 1000 a 5000 empleados es quien realiza las evaluaciones de seguridad, las empresas del sector de la consultoría especializada y otros sectores, en el tamaño de 1 a 50 empleados son las que más resaltan al no usar este mecanismo de mejora. Por último, las empresas del sector financiero de más 5000 empleados son los que usan más de 4 evaluaciones de seguridad, para valorar el estado de la seguridad de dichas organizaciones.

Consideraciones de los datos

Al hacer una inspección de como los mecanismos de seguridad son usados en las empresas colombianas y cuáles son las tendencias por sectores de la industria encontramos la tabla 10, la cual contiene la distribución por sectores de industria de los mecanismos de seguridad.

Tabla 10: Herramientas usadas por sectores de la industria.

Mecanismos	Construcción / Ingeniería	Consultoría Especializada	Educación	Fuerzas Armadas	Gobierno / Sector público	Otro (especifique)	Retail / Consumo masivo	Salud	Sector de Energía e Hidrocarburos	Servicios Financieros y Banca	Telecomunicaciones
VPN/IPSec	5%	13%	7%	2%	9%	26%	4%	3%	4%	20%	6%
Cifrado de datos	5%	13%	7%	2%	8%	25%	3%	3%	4%	23%	7%
Firmas digitales/certificados digitales	3%	16%	7%	1%	11%	26%	4%	3%	4%	21%	3%
Soluciones Anti-Malware	4%	12%	5%	2%	11%	27%	4%	2%	3%	22%	6%
Firewalls de nueva generación	2%	17%	6%	1%	9%	25%	4%	2%	4%	23%	5%
Web Application Firewalls (WAF)	2%	12%	10%	2%	8%	26%	3%	2%	3%	25%	5%
Entrenamiento/Actualización del personal de seguridad/ciberseguridad	1%	23%	6%	1%	5%	24%	3%	2%	5%	20%	9%
SIEM (Security Information Event Management)	2%	12%	4%	2%	9%	30%	2%	1%	5%	24%	7%
Soluciones de seguridad EDR (End-Point Detection and Response)	1%	14%	6%	1%	9%	31%	4%	1%	5%	21%	6%
Servicio de SOC	1%	15%	4%	1%	10%	24%	3%	3%	5%	25%	9%
Sistemas de Contraseñas	5%	12%	8%	0%	6%	27%	5%	4%	4%	21%	8%
IDS/IPS de nueva generación	4%	16%	7%	1%	4%	29%	4%	3%	5%	24%	4%
Biométricos (huella digital, iris, etc.)	3%	10%	5%	3%	5%	30%	3%	5%	5%	22%	7%
Enfoque de seguridad Zero Trust	1%	19%	4%	3%	6%	26%	4%	1%	4%	21%	10%
Herramientas Anti–DDoS	1%	13%	4%	3%	4%	29%	4%	1%	4%	30%	4%
Firewalls tradicionales (Hardware/Software)	4%	16%	10%	1%	13%	18%	4%	3%	4%	16%	6%
Sistemas de detección y/o prevención de intrusos IDS/IPS tradicionales	3%	12%	7%	2%	2%	28%	5%	2%	5%	25%	10%
Firewalls de Bases de Datos (DAF)	5%	13%	9%	2%	9%	20%	4%	4%	2%	25%	7%
Proxies/Proxies inversos	5,66 %	9%	9%	4%	8%	25%	4%	0%	4%	25%	8%
Servicios de inteligencia de amenazas	2%	19%	2%	2%	6%	25%	2%	2%	6%	25%	10%
Ciberseguros	2%	6%	6%	0%	2%	31%	4%	4%	6%	33%	6%

Cooperación/Intercambio de información con otros (estado, proveedores, aliados, sectores, pares)	0%	14%	5%	2%	9%	27%	5%	2%	5%	20%	11%
Soluciones basadas en inteligencia artificial	0%	17%	3%	3%	6%	26%	6%	3%	6%	26%	6%
Soluciones de monitoreo de redes sociales	0%	14%	4%	0%	0%	18%	4%	4%	14%	39%	4%
ADS (Anomaly detection systems)	4%	7%	4%	0%	4%	36%	4%	4%	7%	18%	11%
Soluciones de Seguridad con IA	0%	24%	4%	4%	0%	20%	4%	4%	8%	28%	4%
Herramientas de validación de cumplimiento con regulaciones internacionales	0%	10%	5%	0%	0%	25%	10%	5%	5%	35%	5%
Tercerización de la seguridad informática	6,25 %	13%	6%	0%	13%	25%	13%	0%	6%	13%	6%
Otro (especifique)2	0%	27%	27%	0%	0%	18%	0%	9%	0%	0%	9%
Smart Cards	0%	13%	13%	0%	0%	13%	13%	13%	0%	13%	13%

Algunas particularidades al revisar los datos los cuales se pueden describir así.

1. La tercerización de la seguridad solo es visible en el sector de construcción e ingeniería y el sector retail.
2. El sector de la consultoría especializada y educación, aparte de los mecanismos propuestos consideran otros mecanismos, entre ellos
3. El sector de las fuerzas armadas empieza a usar soluciones de seguridad con IA.
4. Los firewalls tradicionales son el mecanismo más usado en el sector gobierno.
5. Las Smart cards son un mecanismo usado en el sector de retail, telecomunicaciones y sector salud.
6. El monitoreo de redes sociales es más representativo en el sector financiero y el sector de hidrocarburos.

En el estudio de IBM, 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 (IBM 2024b; IBM, 2024c), 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 informe resalta que las soluciones *antimalware*, cifrado de discos, antivirus avanzados basados en inteli-

gencia artificial también están considerados.

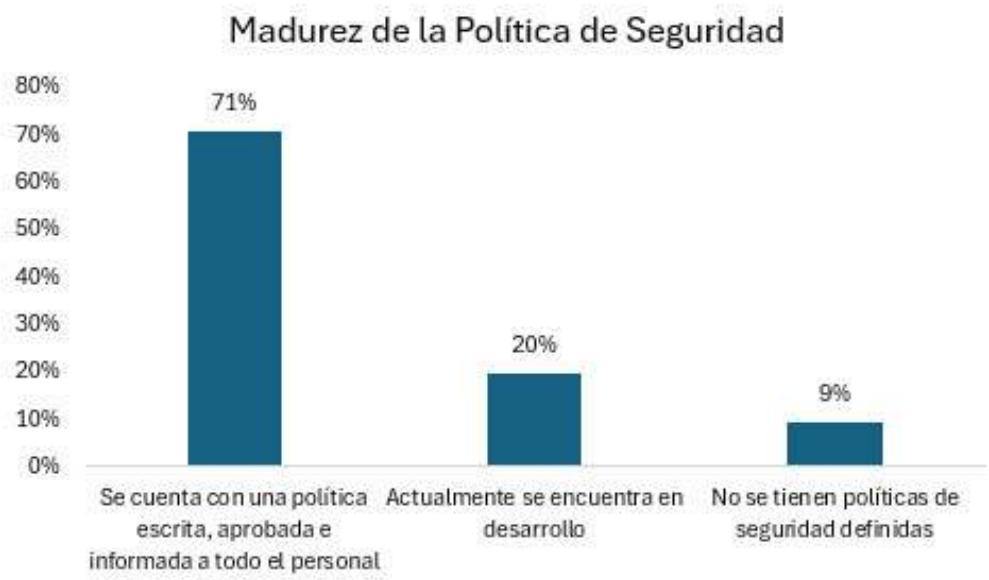
En cuanto a la protección de la capa de aplicaciones, los *Firewalls Web*, de bases de datos la protección de APIs son los controles que más se están usando y se tiene proyectado utilizar.

Los controles de seguridad siempre serán una herramienta indispensable para tener una higiene digital adecuada, en Colombia se ratifica la tendencia de uso de controles para combatir y contrarrestar a un adversario digital que cada vez acecha más, hace uso de capacidades adicionales y las empresas en su camino de desarrollar y sostener la resiliencia operacional cada vez más necesitan de estas soluciones (ATT, 2024).

Políticas

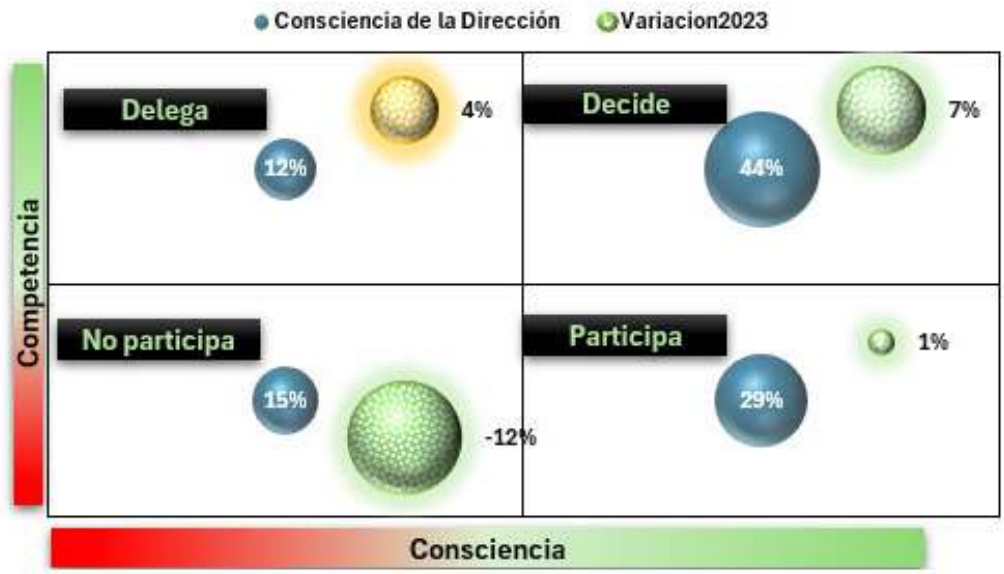
La gráfica 25, refleja el estado de las políticas de seguridad en las organizaciones colombianas, el 71% de los encuestados manifiesta que tienen formalizada sus políticas de seguridad aumento de 3 puntos porcentuales frente al año 2023, el 20% actualmente en desarrollo y con un aumento del 5% frente al año anterior, el 9% señala no tener políticas de seguridad de la información, disminución importante del 7%.

La gráfica 26, 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 47%, el cual incrementa un 5% frente al año anterior, para este año



Gráfica 25: Estado de las Políticas

Gráfica 26: Obstáculos de la seguridad



Gráfica 27: Consciencia de los directivos

la falta de colaboración entre áreas toma el segundo lugar con 26% con un incremento del 4% frente al año anterior, la complejidad tecnológica da un gran salto y pasa al tercer lugar con un 23% y un incremento del 12% frente al año anterior.

La gráfica 27 refleja el nivel de consciencia y competencia de los directivos en materia de seguridad, encontrando que, la alta dirección con un 44% toma decisiones en materia de ciberseguridad, 29% atiende las recomendaciones de sus

profesionales, 15% no participa en la toma de decisiones y no se involucra, y el 12% delega y espera informa de avances.

Un cambio interesante se ve en los miembros y equipos tanto directivos como ejecutivos de las empresas en Colombia, sin importar su tamaño hay un interés por el tema, que se ve reflejado en los datos, un 7% de incremento con respecto al año anterior en la capacidad de estos equipos directivos en tomar decisiones con respecto a la seguridad, muestra mejoras, un decrecimiento del 12% en el desinterés de los ejecutivos por no querer atender el tema es una lectura positiva que muestra importantes avances en el gobierno de la seguridad, que se ve reflejado en la confianza digital de las empresas, los directivos de las empresa, y sus ejecutivos entiende la necesidad de hacer lecturas más apropiadas sobre la ciberseguridad de cara a la sostenibilidad del negocio y la ganancia de confianza en el mercado en el que existen (IBM, 2024a; EY, 2024; PwC, 2024; Auditboard, 2024; Diligent Institute, 2024).

En cuanto al comportamiento en los sectores y tamaños, tenemos aspectos importantes que resaltar como que, la consultoría especializada es donde los equipos directivos más deciden sobre la agendad de la ciberseguridad en las empresas y particularmente la franja en donde este comportamiento es más consistente es en las empresas de 1 a 50 empleados, entienden sus ejecutivos que este tema debe ser atendido, en tiempos donde los datos se ven como la fuente fundamental para hacer negocios, máxime en la época de startups que usan la IA para monetizar sus datos (Haleliuk et all, 2024). El sector de gobierno tiene dos comportamientos interesantes, en las empresas de 1000 a 5000 empleados por un lado se expresa que los equipos directivos poco se involucran o no participan de las decisiones que tienen que ver con la ciberseguridad, sin embargo, también se resalta que ellos si atienden las recomendaciones de los profesionales de seguridad en la materia; esto podría tener lecturas aunque no contrarias, por un lado escuchan, pero deciden no participar, dejando a la regulación a que cumpla con su papel cuando esta exista (Auditboard, 2024). Por último, los solo deciden delegar también tienen matices, los otros sectores de la industria en los tamaños de 51 a 200 empleados son los que deciden tener este comportamiento, el que más llama la atención es el sector salud que en las empresas de 1000 a 5000 empleados, decide delegar la atención de los temas a comités alternos para que estos temas sean atendidos. Tendencia que no se aleja de los comportamientos internacionales, por un lado el sector salud es un sector de alto valor para el adversario digital, eso se entiende y es la razón para llevar el tema a los niveles ejecutivos, eso sumado a las noticias

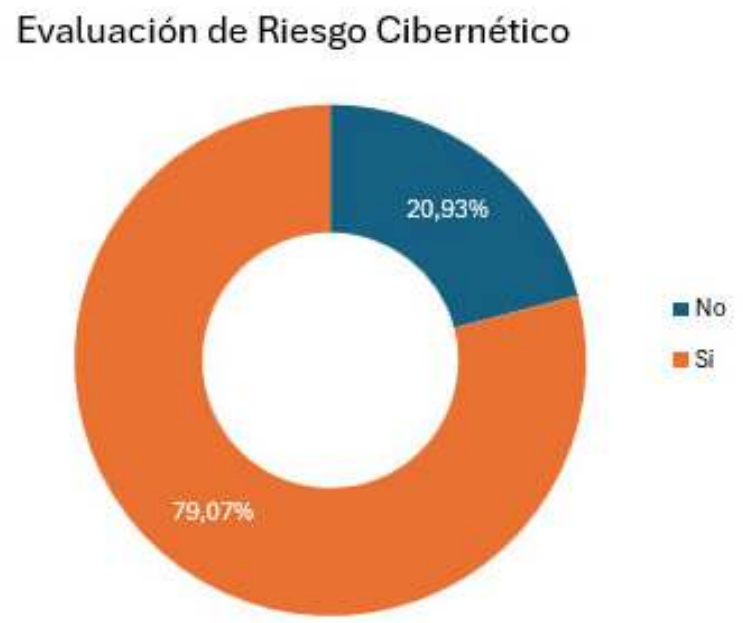
permanente de fugas y ataques en dicho sector, y segundo que los equipos directivos y ejecutivos pueden no estar entendiendo del todo la realidad de la ciberseguridad, y prefieren o asumen que un comité técnico que en muchos de los casos tienen miembros del equipo directivo en dichos comités tengan los espacios y tiempos para entender la complejidad de la situación (Kroll, 2024).

Riesgo Cibernético

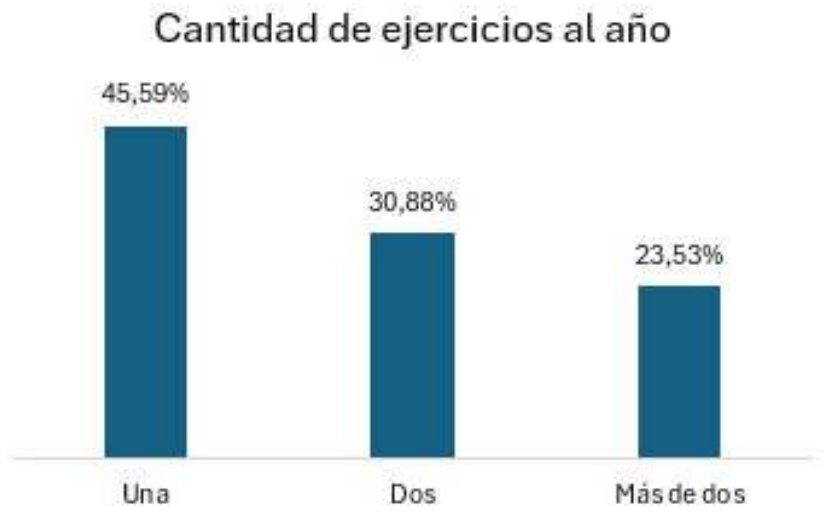
La gestión de riesgos de seguridad es un elemento esencial, en esa línea el 79% de los encuestados tiene un proceso de gestión de riesgos con un crecimiento del 4% frente al año anterior y solo 21% no lo posee, con una diminución de 4 puntos frente al año anterior, que se ve reflejada en la gráfica 28.

En la gráfica 29, se resalta cada cuanto son ejecutados dichos ejercicios, el 46% manifiesta que al menos la ejecuta 1 vez al año, disminuye en 10% frente al año anterior, el 31% lo hace dos veces al año, con un aumento del 5% con relación al año anterior, y más de 2 un 24% de los encuestados con un incremento del 6% Estos valores corresponden a aquellos que dijeron que si realizan la evaluación de riesgo en sus empresas.

Dentro de las personas que contestaron que no lo hacen, al indagar en las razones de por qué no es reali-



Gráfica 28: Ejecución de Evaluaciones de riesgo



Gráfica 29: Cantidad de veces que se ejecuta

zada la gestión de riesgos. El principal motivo que resaltan los participantes está relacionado con no tener un proceso formal de gestión de riesgos (36%), aumento con relación al año anterior en 5 puntos porcentuales, seguido por falta de presupuesto con un 22% un incremento de 11% frente al año anterior, seguido del desconocimiento del tema 17% un decremento de 5 puntos frente al año anterior, no se tiene asociado riesgos con el tratamiento de la información 11% que no manifiesta variación, realizado dentro del proceso de gestión de riesgo empresarial 8% y una gran disminución 15% frente al año anterior. Movimiento interesante pues también deja ver la importancia que tiene el riesgo cibernético en las empresas que, al incluirlo en la metodología corporativa de gestión de riesgos empresarial, transmite un mensaje de importancia para las empresas y denota madurez a la hora de tomar acciones (WEF, 2024a).

La tabla 11 muestra las metodologías de gestión de riesgos usadas por los participantes del estudio. En primer lugar, está ISO 31000 con un 33% de las veces y sigue la ISO 27005 con un 32%, revelando para este año una leve variación con respecto al año anterior.

La Gráfica 30 muestra la forma en como las organizaciones hacen las asociaciones entre incidentes de seguridad y el riesgo. El 70% asocia los incidentes de seguridad con riesgos de ciberseguridad con un incremento del 13%, el 55% los asocia con riesgos operacionales con un crecimiento del 7%, el 50% los asocia con riesgos reputacionales con un incremento del 14%, el 46% con riesgos legales que tie-

Tipos de Metodología	%
Cuenta de ISO 31000	33,50%
Cuenta de ISO 27005	32,51%
Cuenta de No se cuenta con metodología	19%
Cuenta de GRC (Governance, Risk & Compliance)	15%
Cuenta de SARO	13%
Cuenta de ERM(Enterprise Risk Management)	7%
Cuenta de Otro (especifique)3	5%
Cuenta de Magerit	5%
Cuenta de AS/NZ 4360	2%
Cuenta de Octave	1%

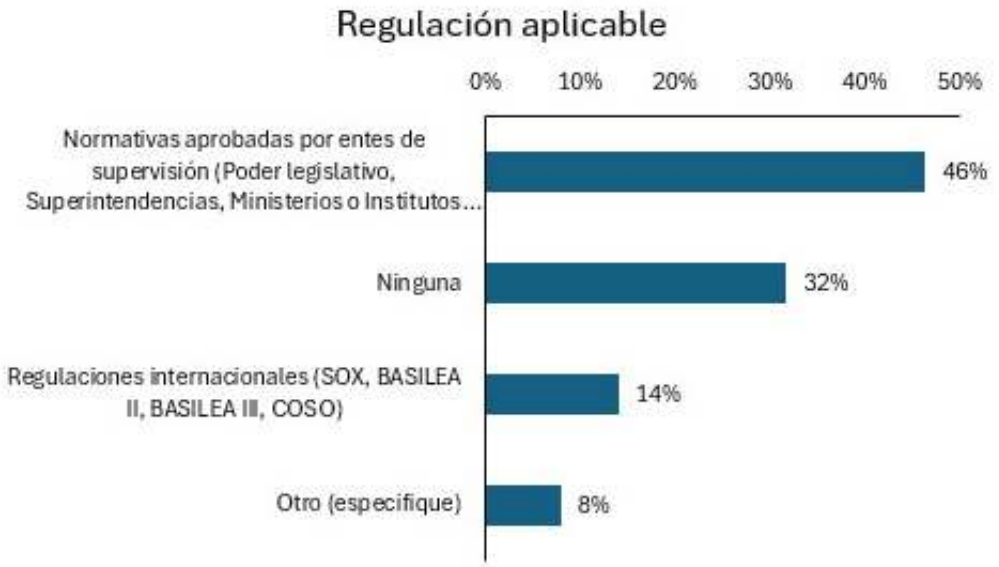
Tabla 11: Metodologías para la gestión de riesgos

Gráfica 30: Tipos de Riesgos

ne un aumento del 11%, el 44% con riegos económicos con un crecimiento del 12%, y por último el 31% los asocia a riesgos transversales con un incremento del 5% frente al año anterior.

La gráfica 31 relaciona en a quien se reportan los informes de riesgos en la organización. Siendo esta una nueva pregunta de la encuesta, se evidencian algunos datos interesantes, el 58% manifiesta que la

Gráfica 31: Reporte de la Gestión de Riesgos Cibernéticos.



Gráfica 32: Regulación aplicable

gestión de los riesgos cibernéticos se presenta a los equipos directivos y ejecutivos de las empresas. El 33% lo hace ante los equipos tácticos, como el comité de seguridad de la información, el 23% al equipo técnico como los comités técnicos de TI y solo el 11% manifiesta que eso no se hace, o no se presenta.

La gráfica 32, muestra si las empresas están sujetas a regulaciones nacionales o internacionales. El 50% está sujeto a la regulación del país, sin embargo, el 34% manifiesta que no tiene ninguna regulación, el 15% menciona que las regulaciones internacionales si tienen efecto sobre las empresas, por

último, el 8% menciona que otras regulaciones, que muchas de ellas son de nicho.

Consideraciones de los datos

Gobierno y Gestión de la Seguridad

La gestión y el gobierno de la seguridad son instrumentos de alto valor para hacer que las estrategias de seguridad tanto en el corto plazo como en el largo plazo funcionen y nutran a los negocios de condiciones que apalanquen la confianza digital en todas las partes interesadas, aumenten la resiliencia operacional del negocio y en últimas generen beneficios, máxime si hay fenómenos acentuados de disrupción, que obligan a las empresas a prestar atención a fenómenos sistémicos como los cibernéticos (Accenture, 2024; WEF, 2024a; Fdic, 2024).

En ese sentido la política de seguridad en Colombia en todos los sectores de la industria ha encontrado una consolidación importante al estar definida y formalizada en la realidad de las empresas colombianas. La gráfica 33, muestra esa distribución por sectores en donde se puede ver reflejada la madurez de la política como instrumento del programa para la gestión y el gobierno de la seguridad. La gráfica muestra que la madurez muy alta, relacionando la formalidad que existe de la política y en todos los sectores es marcada, otros sectores a primera vista tienen el valor mayor, sin embargo, al revisar ba-

Gráfica 33: Madurez de la política de seguridad por sectores de industria

sado en los tamaños de las empresas, encontramos como dato particular, que el sector de gobierno en las empresas de 1000 a 5000 empleados, es el dato más representativo, el sector educación resalta porque sigue trabajando por definir su esquema de políticas en la franja de los 1000 a 5000, y las empresas de 1 a 50 empleados, en el sector de consultoría y otros sectores no ha trabajado en definir la política de seguridad, esto muestra son las dinámicas que sufre cada sector, así mismo los tamaños de las empresas también inciden. El sector gobierno por el contexto regulatorio y de cumplimiento claramente debe tener definido su política de seguridad, Colombia es un país que tiene un marco regulatorio que hace que las empresas de dicho sector deban tenerlo definido, sorprende tal vez que los servicios financieros no sean el primero en esta categoría teniendo también un marco regulatorio avanzado que regula al sector.

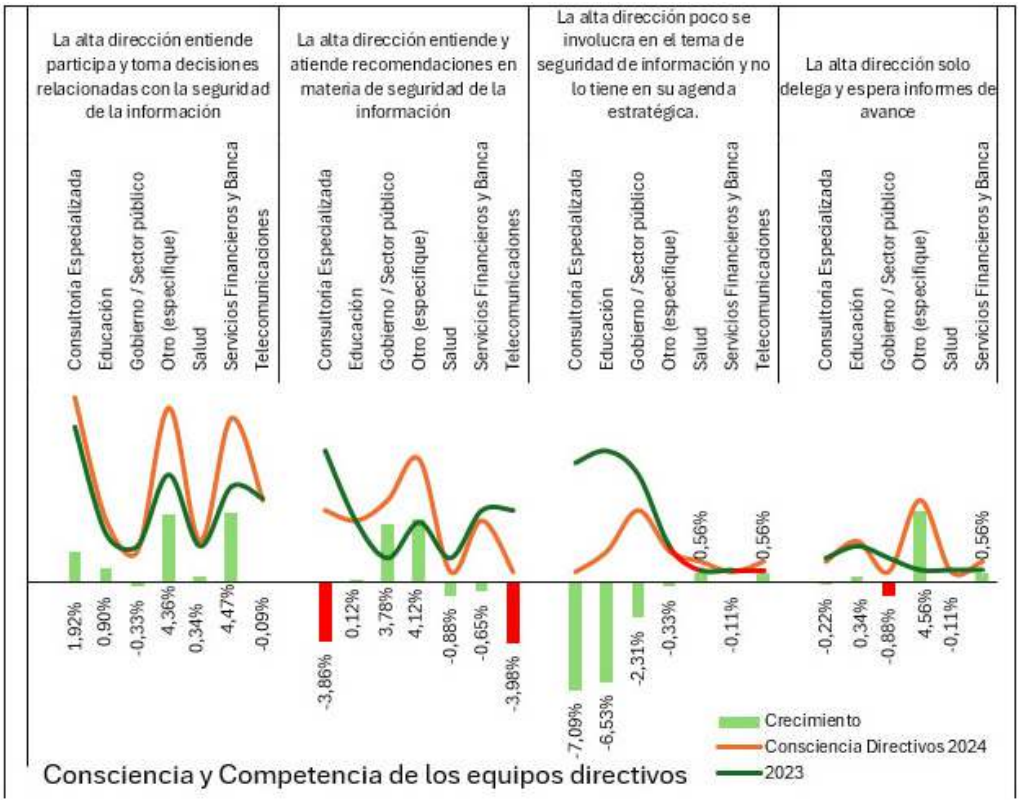
Hay que resaltar que frente al año inmediatamente anterior hay mejoras en sectores como el sector salud, que ha venido haciendo avances en el tema, o al menos así lo sugieren los datos, esto claramente responde a la realidad global, donde el sector salud es uno de los más apetecidos por los adversarios digitales (Verizon, 2024; Kroll, 2024; Allianz, 2024).

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, 2024a; WEF, 2024b, EY-IIF, 2024), el cual manifiesta que la prioridad de estos tipos de ataques es alta en las organizaciones del mundo.

Las responsabilidades de un gobierno de seguridad de la información está centrada en que sus miembros directivos tengan un contacto directo con la ciberseguridad (NACD,2024), participen de ella y tomen decisiones basados en los datos, tendencias recientes como las directrices propuestas por la Security Exchange Commission (SEC), que ha propuesto una responsabilidad más avanza en materia de responsabilidad de los cuerpos directivos y que planea para finalizar el año 2023 (Toscano, 2023).

En este sentido, al revisar la forma en como los cuerpos directivos se involucran en la toma de decisiones de la seguridad por sectores de la industria y se compara con el año inmediatamente anterior, se tiene la gráfica 34.

Al revisar los datos, vemos avances importantes y alentadores en todas las dimensiones, las juntas y equipos directivos les interesa el tema y buscan de alguna manera estar al día con un reto que ha puesto a las empresas en aprietos a nivel global. Un interesante decrecimiento importante en el sector de consultoría y educación por seguir



Gráfica 34: Juntas directivas x sectores

el paso de los retos de la ciberseguridad, al dejar atrás la figura de no participar o involucrarse en atender los retos y desafíos que implica la confianza digital para generación de valor en los negocios digitales. Sin embargo, los datos muestran también que el sector el mismo sector de consultoría especializada y telecomunicaciones decrecen las empresas que atienden y entiendan a los temas de ciberseguridad.

Al inspeccionar o ampliar la exploración y revisar el tamaño de las empresas y sectores en este criterio, tenemos que las empresas de consultoría pequeñas de 1 a 50 empleados, es donde sus directivos más se involucran, las entidades del sector gobierno tienen dos comportamientos en el tamaño de 1000 a 5000 y es, por un lado, atienden las recomendaciones de las áreas de seguridad, así mismo, los equipos directivos poco se involucran en el tema, por último las empresas del sector de la educación de las empresas de 1000 a 5000 empleados delega a comités especializados para que atiendan la seguridad de las empresas y solo esperan reportes de lo que suceda en esos comités.

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, 2024).

Es claro que existen obstáculos para que la postura de seguridad de una organización fluya en los ambientes organizacionales, la postura 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, así mismo maximizar el valor de las inversiones, y el beneficio que los programas produzcan (NACD, 2024).

Algunas consideraciones claves frente a los obstáculos que impiden a las organizaciones en Colombia tener posturas de seguridad más sólidas y que se enfoquen en mantener una mejor resiliencia operacional.

1. Cada sector tiene un sentir con particularidades de como los obstáculos hacen que los programas de seguridad no fluyan de la manera más adecuada posible.
2. La cultura de seguridad es el factor más resaltado como un obstáculo para todos los sectores de las empresas de distintos tamaños, pero de todos se resalta las empresas pequeñas de 1 a 50 empleados del sector de la consultoría especializada como el más representativo.
3. La complejidad tecnológica que es el segundo factor este año, se manifiesta en todos los sectores, pero con especial atención en las empresas de 1000 a 5000 empleados, en otros sectores, los servicios financieros y banca y telecomunicaciones, esto es explicable desde la óptica de las transformaciones digitales que están experimentando muchas de las empresas, y por tanto a mayor densidad digital, mayor complejidad, por tanto los retos de atender los riesgos en estas condiciones necesitan de enfoques sistémicos que puedan ayudar a resolver esa complejidad (Bankofengland, 2024)
4. Para el sector de la educación, telecomunicaciones, gobierno y salud, en especial las empresas de 51 a 200 empleados y para las empresas de 1000 a 5000, las limitadas habilidades gerenciales y de liderazgo de los CISOs el principal obstáculo, no dista de las situaciones internacionales que han venido señalando la necesidad en relación a que los profesionales de seguridad necesitan no solo ser unos excelentes profesionales técnicos, como ya lo son, sino que necesitan expandir y ampliar sus capacidades para mejorar la

confianza hacia las partes interesadas (Trendmicro, 2024; Trellix, 2024; IANS, 2024a).

5. La falta de formación técnica en el sector de las telecomunicaciones en las empresas de 1 a 50 empleados es uno de los factores fundamentales para que no exista una mejor postura de seguridad, que está conectado con que las personas no tengan formación en gestión segura de la información.
6. Sorprende que las empresas de 500 a 1000 empleados del sector financiero manifiestan que no tienen obstáculos como el primer factor, sin embargo, en el mismo sector y otros tamaños es llamativo que es el factor que resaltan.

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, 2024a; Diligent Institute, 2024).

Gestión del Riesgo

Gestionar el riesgo es una de las formas eficientes para no solo dar soporte y resiliencia operacional a los negocios, adicional es una forma de tomar decisiones que soporten el desarrollo de los negocios en el corto, mediano y largo plazo (Thompson, C., & Hopkin, P., 2021).

En la realidad colombiana los diferentes sectores de la industria ven a riesgo como un instrumento de conexión con la seguridad y ciberseguridad, sin embargo, la madurez en la práctica aún sigue un camino de aprendizajes propio de las dinámicas organizacionales, tendencia que no se aleja de la realidad global (ECIIA, 2024; WEF, 2024a; FAIR, 2024; Absolute, 2024)).

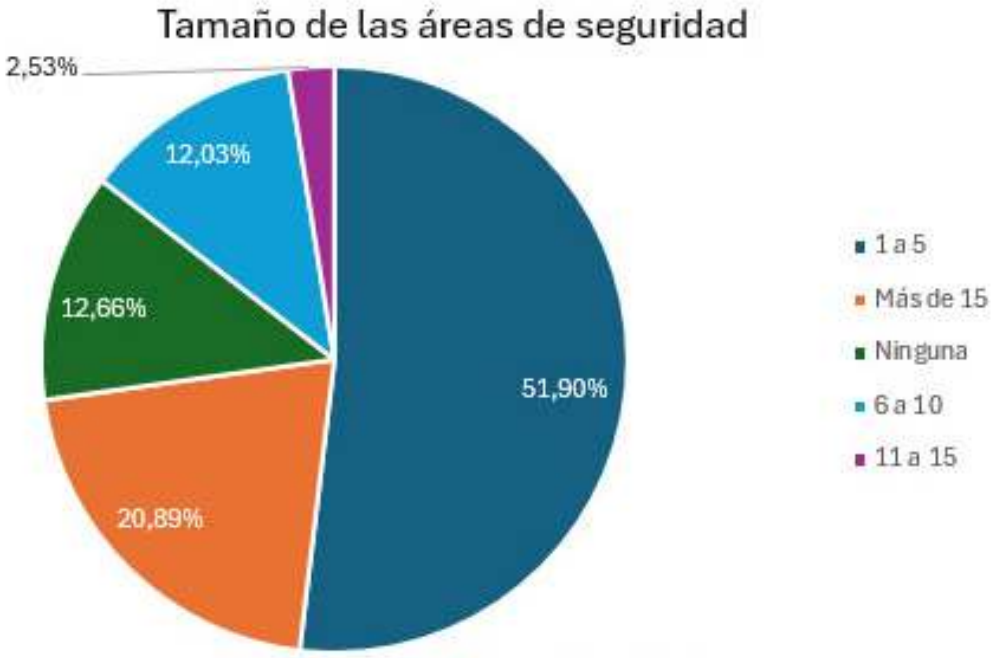
La radiografía de la gestión de riesgo en Colombia puede ser descrita de la siguiente manera:

1. Las empresas colombianas realizan al menos un ejercicio al año de valoración de riesgos. Siendo el sector del gobierno del tamaño de 1000 a 5000 empleados las que más usan este método.
2. Llama la atención que el sector de la consultoría especializada en empresas de 1 a 50 empleados realice dos evaluaciones de riesgos, mientras que las empresas del sector financiero de 500 hasta 5000, usan esta misma figura.
3. Mas de dos son realizadas por las empresas de más de 1000 empleados y en particular el sector de la consultoría y otros sectores, usan la práctica de realizar más de dos evaluaciones de riesgo en las empresas.

4. Para este año el marco más usado es el modelo 31000 por encima de 27005, esto puede ser explicable pues cada vez más el riesgo cibernético es visto como un riesgo más de naturaleza sistémica y con una alta complejidad, que solo un riesgo específico y con enfoque como podría ser considerado al usar dichas metodologías (Zongo, P., 2018; Chaput, B., 2024)
5. Sin excepción de los sectores de la industria analizados, todos catalogan sus incidentes como un ejercicio asociado al riesgo cibernético, tema no menor porque muestra que en Colombia se empieza a entender que el riesgo cibernético merece un tratamiento diferencial a otros riesgos, esto mismo podría dar luz para que la resiliencia operacional tenga cabida en las empresas y de la misma manera se comprenda que el riesgo cibernético deja de ser un asunto de tecnologías y es más un asunto de negocio (Leirvik, R, 2024).
6. Reportar los riesgos cibernéticos es una herramienta esencial e insumo significativo para hacer de la gestión de riesgos cibernético un ejercicio de valor, sin embargo, no es solo reportar el riesgo, es que exista la información suficiente para que los equipos directivos y ejecutivos puedan tomar decisiones adecuadas en procura de prepararse, anticipar y adaptarse frente a los riesgos a los que se ven expuestos en el ecosistema digital (Oh, K, 2024). En la realidad de Colombia se encuentra las siguientes anotaciones, primero reporte se hace en todas las instancias, sin embargo, al desagregar los datos encontramos que el valor más representativo lo tienes las empresas del sector financiero en empresas mayores de 5000 empleados, que reportan a los equipos tácticos de las empresas como los comités de seguridad la información, otros sectores reportan a los equipos técnicos, en las empresas de 1000 a 5000 empleados. Sectores como consultoría especializada en el tamaño de 1 a 50 empleados, educación en la franja de las empresas desde 500 a 5000, y otros sectores en el tamaño de 1 a 50 empleados son las que no reportan nada. Sorprende que en las empresas de consultoría del tamaño de 1 a 50 empleados si reporta a las instancias directivas de las empresas, llama la atención que las empresas medianas y grandes si bien lo hacen, lo hacen en menor proporción.

Capital intelectual

La gráfica 35, muestra el tamaño de las áreas de seguridad, el primer lo ocupa de 1 a 5 con un 52%, con un decrecimiento de 6 puntos con relación al año anterior, el segundo lugar y más llamativo es que las áreas de ciberseguridad tienen más de 15 personas con un 21% y un crecimiento de 7 puntos con relación al año anterior, seguido de



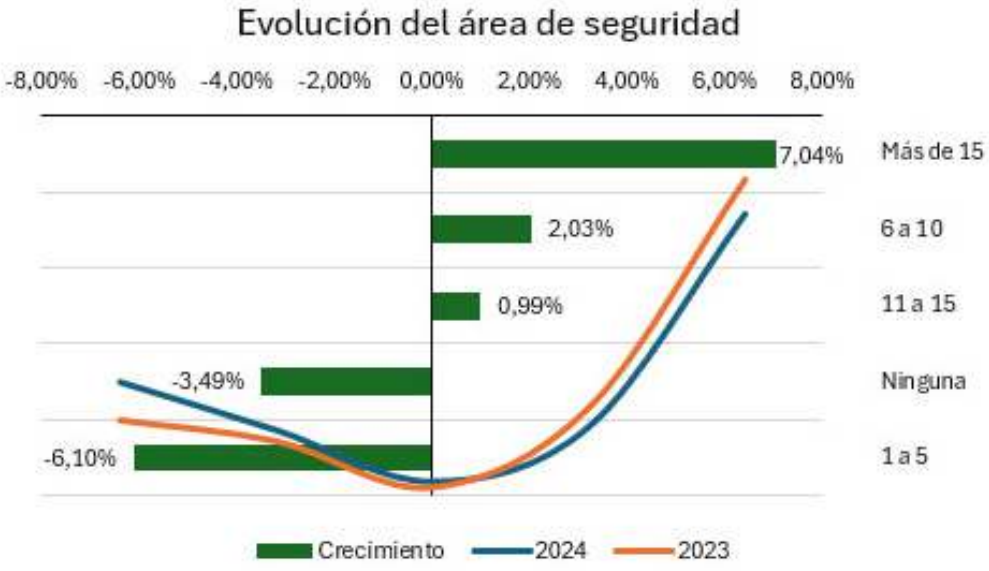
Gráfica 35: Tamaño del área de Seguridad

ninguna persona 13% con un decrecimiento de tres puntos, de 6 a 10 tiene una representación del 12% y un crecimiento de 2 puntos en relación con el año anterior y por último de 11 a 15 personas con un 3% y un crecimiento de 1 punto con relación al año anterior.

Consideraciones de los datos

Las áreas de seguridad son diversas en la realidad de Colombia, se encuentran los grandes avances frente a su crecimiento, la gráfica 36 es la muestra que las áreas de seguridad siguen evolucionando y en ellas se pueden ver cambios importantes para este año.

Las áreas de más de 5 empleados crecen en sus diferentes franjas, definitivamente se sigue consolidando el área de seguridad en las empresas decrece el que las empresas no tengan una, así como las que solo tienen a una persona como máximo 5. Al entrar en el interior de los datos se encuentran con interesantes puntos. En las áreas de 1 a 5 empleados es el sector de la consultoría de empresa pequeñas el que es más representativo, son las empresas del sector financiero y exactamente las de más de 5000 empleados las que tienen un área de seguridad de más de 15 personas, son otros sectores y no los representativos de la industria los que no tienen definidas áreas de seguridad y en la franja de las empresas pequeñas es el que más se destaca, las áreas de seguridad de 6 a 10 y 11 a 15 empleados se des-



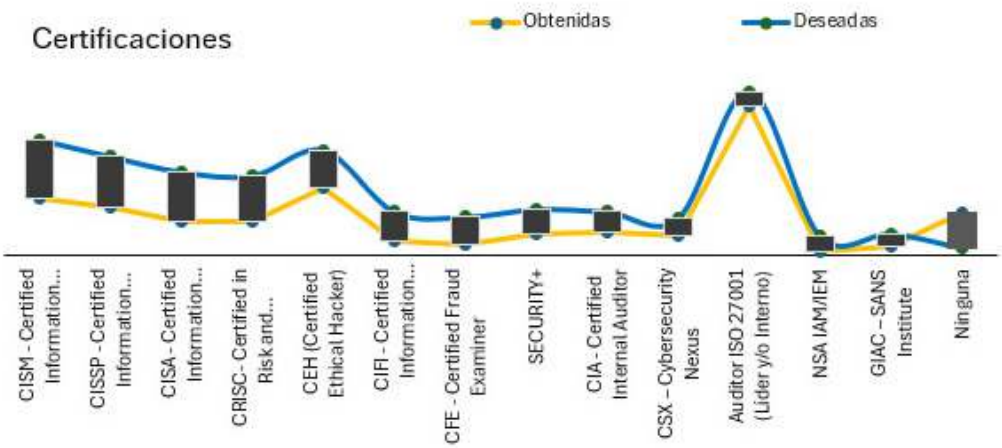
Gráfica 36: Área de Seguridad

tacan en oros sectores en el tamaño de más de 5000 empleados.

Estos datos estan conectados con la tendencia que habla de la necesidad de profesionales de seguridad, de la escasez de estos, y de las crecientes presiones que existen por conseguir talentos con las habilidades y capacidades para soportar las demandas en materia de seguridad en las empresas (WEF, 2024b, WittKieffer, 2024; ISC2, 2024b; Gitguardian, 2024).

Las certificaciones son parte esencial de la vida del profesional de seguridad y alcanzarlas hace parte del desarrollo de su carrera (ISSA-ISG, 2023; ISACA, 2024; Fortinet, 2024). La gráfica 37, representa las certificaciones alcanzadas y proyectadas a alcanzar.

Esta gráfica representa dos momentos, el primer momento está relacionado con las certificaciones que hoy el profesional de seguridad posee, en ese orden de ideas, lo que más hoy se ha alcanzado en el horizonte es la certificación de Auditor ISO 27001 en Colombia, seguido de CEH y CISM respectivamente, sin embargo, al revisar lo que el profesional de seguridad desea lograr, se invierten los papeles y encontramos que la certificación de ISO 27001, CISM y CEH, ahora bien si analizamos las diferencias de personas que la desean entonces encontramos que CISM, CISSP y CISA son las que tienen



Gráfica 37: Certificaciones de los profesionales de seguridad

una marcada diferencia entre los que la tienen y la desearían obtener.

Los profesionales de seguridad en busca del desarrollo de su carrera profesional ven en las certificaciones una forma de mejorar no solo sus conocimientos, sino su valor de mercado. (ISSA-ESG, 2023).

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, 2024).

El CISO un ejecutivo en aprendizajes

Un rol profesional que ha tenido una relevancia importante en los tiempos de transformación de las empresas en el contexto digital (Wolfe, T., 2024), con los cambios drásticos que la tecnología y los negocios vienen experimentando, los incrementos de la actividad hostil del adversario digital y la necesidad de las empresas de hacerse sostenibles en un ecosistema digital toma relevancia el rol y sobre todo la información que entrega (Splunk, 2024a).

La confianza que genera el CISO se vuelve una piedra angular de su función que se hace necesario tener presente y atender como un reto no resuelto de los profesionales de seguridad de la actualidad (TrendMicro, 2024; Wolfe, T., 2024).

Gráfica 38: Información que entrega el CISO por sector de la industria

La gráfica 38, muestra precisamente que tipo de información entrega en las empresas. Cabe destacar que cada sector de la industria tiene unos matices importantes de la forma en como es percibido el rol y así mismo evalúan el valor del ciso.

El Rol del CISO como ejecutivo de la seguridad varia dependiendo de los sectores y tamaños de las empresas, los datos muestran que la función ejecutiva de entregar información relacionada con la gestión de la seguridad para la toma de acciones tiene una alta valoración en el sector financiero, sin embargo, al ahondar en los datos y ver por tamaños de empresas, es el sector de la consultoría en las empresas de 1 a 50 empleados, donde hay una leve variación mayor con relación al sector financiero en el mismo tamaño donde es menor, pero es mayor en conjunto en el sector financiero, porque en todos los tamaños del sector financiero se hace más que en el sector de la consultoría y a sumar y totalizar es la razón por la que en el sector financiero se resalta como la gráfica 36.

No tener un CISO es un riesgo para las empresas en sí mismo (Metomic, 2024), al revisar este criterio en la realidad colombiana, el sector de otros es el que representa un alto valor, sin embargo, al explorar en profundidad los datos, encontramos las empresas muy grandes de más de 5000 empleados en los sectores representativos lo marcan en 0, lo que se lee como que si exis-

ten y eso es un interesante avance, en otros sectores en la franja de 1 a 50 y de 200 a 500 marcan que no los tienen, el que sorprende son las empresas de salud que en las empresas de 500 a 1000 empleados, igualan a los otros sectores al decir que no lo poseen. A todas luces un riesgo alto, toda vez que el sector salud es un sector de alto valor para los adversarios digitales, como lo han expresado los ataques recientes no solo en Colombia, caso Keralti, Audifarma, y Cafam, sino a nivel internacional alrededor del mundo y la región.

No entregar información es otros de los criterios explorados que tiene un comportamiento similar, el CISO en las empresas grandes de todos los sectores incluido otros manifiestan que, si lo hace y eso es muy interesante, al revisar donde no lo hace hay varios matices a considerar, en las empresas de 200 a 500 empleados del sector de educación el responsable de seguridad no entrega información, y el caso más llamativo es que en las mismas proporciones en las entidades del gobierno de 1000 a 5000 empleados tampoco lo hace dicho responsable, esto supone un riesgo para las empresas en si mismas, pues necesitan la información para tomar decisiones y sobre todo garantizar la debida diligencia del profesional de seguridad; si bien en Colombia no existen regulaciones como las actuales que existen a nivel de Estados Unidos (SEC), y las del caso de Europa con (DORA), donde exigen que eso sea constante para garantizar el gobierno de la seguridad, si existe la ley 1581 para el tratamiento de datos personales, y puede ser un riesgo no solo para el profesional y las empresas. La buena entrega de información matiza los niveles de confianza entre los ejecutivos y el CISO (TrendMicro, 2024).

Tomar decisiones es un aspecto clave de la gerencia y liderazgo actual (Owen, J., 2018), para ello es necesaria la información, y entregarla por parte del responsable de seguridad es clave, para que eso suceda, en ese sentido los datos muestran y resaltan algo para analizar, las empresas del sector de consultoría pequeñas son en donde eso más se presenta, sin decir que en otros sectores y tamaños no se haga. Sin embargo, el lunar de estos datos es que es en casi todos los sectores y tamaños donde no se hace, ejemplo de ello, sector de la educación, gobierno, salud, financiero y telecomunicaciones, llama la atención que otros sectores en cualquier tamaño si lo hace y eso muestra un poco que las empresas de sectores tradicionales pueden estar rezagadas en el desarrollo de un modelo de gobierno de seguridad acorde con la realidad de la confianza digital que se busca crear en el ecosistema digital actual.

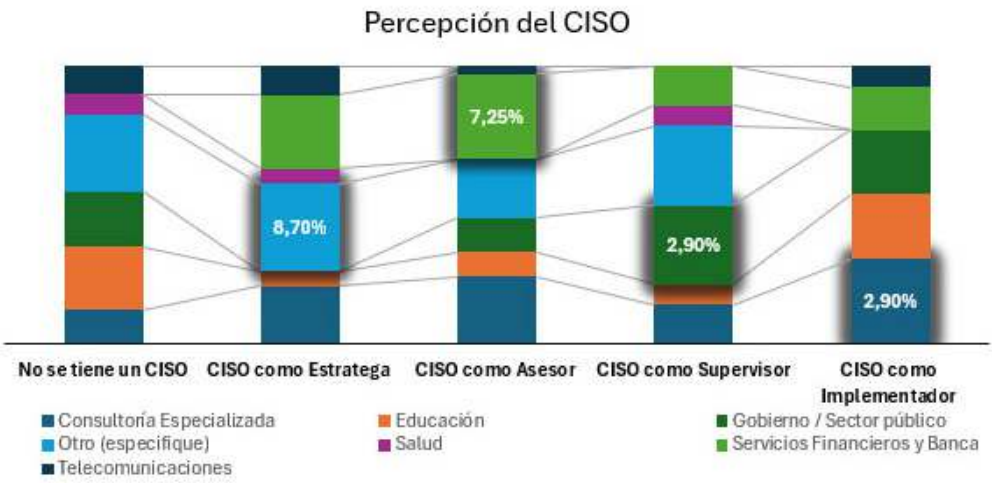
Las brechas son un elemento que no solo es probable, sino posible, día tras día se evidencian brechas

de seguridad en todas las empresas sin importar tamaño, o sector de la industria, por tanto, reportar la información de las brechas es algo clave, y más de cara a regulaciones que cada vez más se mueven en esa línea, buscando transparencia que es un componente importante de la confianza digital (ISACA, 2024). Para el caso de Colombia, el sector financiero de las empresas de más de 500 empleados hasta 5000 son los valores que resaltan que más lo hacen, igual sin decir que otras no. Sectores como la educación, el gobierno, telecomunicaciones y salud no lo realizan y bueno muestran que se necesita mejorar en dicha práctica si se desea avanzar en los frentes de la transformación digital (Foundry, 2024; Infotech, 2024; Logicalis, 2024).

La entrega de información técnica como último de los elementos analizados, se hace en la mayoría de los sectores, es decir que el responsable de seguridad es lo que hace, sin embargo, llama la atención dos sectores educación y salud que, en estos en la mayoría de las franjas de tamaños de empresas, no lo hacen. En el sector de la consultoría en la franja de las empresas pequeñas es donde más se hace.

Todas las organizaciones de una u otra manera perciben al CISO (Wolfe, T., 2024), para el caso de la realidad nacional existen posiciones interesantes y encontradas que pueden ser explicadas por la realidad y madurez de las empresas y el sector en el que ellas se desempeñan. La gráfica 39, pretende explicar este comportamiento.

La figura de un CISO ejecutivo, un rol que va más allá de una visión netamente técnica y que esté más



Gráfica 39: Percepción del CISO por industria

orientada al negocio parece ser por los datos que no es la lectura que están haciendo los distintos sectores de la industria, a excepción del sector financiero todos los demás sectores señalan que esa figura no existe, en especial el sector de la educación que es el que más lo resalta.

El sector de la consultoría especializada ve al CISO como un implementador del programa de seguridad y los controles, tendencia que se mantiene con relación al año anterior, aunque hay avances en su nivel de reportes e integración con los equipos directivos y ejecutivos de la empresas, se sigue viendo como una figura técnica que su labor fundamental es resolver los retos técnicos que demanda la ciberseguridad y seguridad de la información, de lo cual se puede determinar que la lectura es de un CISO táctico en el mejor de los casos que ayuda en la implementación y eso aunado a la información que entrega información de gestión se ratifica este nivel de lectura.

El sector financiero tiene interesantes vistas, se consolidad que el sector financiero mantiene la figura, en ningún tamaño de empresa del sector manifiesta que existe, el valor que más preferencia tiene es el CISO como un Asesor en las empresas de 500 a 1000 empleados, que busca estar 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.

El sector de Gobierno ve la figura como un supervisor el cual es visto en 3 de los 6 tamaños de empresas analizadas, y se resalta en especial que en las entidades del sector de más de mil empleados es donde más se evidencia la lectura de este rol con la función de velar 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.

En cuanto a la forma como el CISO prefiere incrementar su valor y conocimientos es variado, la principal fuente para ello son las certificaciones con un 65% y un crecimiento del 27% con relación al año anterior, la educación formal 53% con un incremento del 28%, seguido de las charlas especializadas con un 30% y un crecimiento del 25% con relación al año anterior. La gráfica 40 muestra los valores mencionados.

En el ejercicio de comparar con el año inmediatamente anterior, realmente son los diplomados los que tuvieron un incremento mayor, estos crecieron 30% frente a los otros criterios que crecieron por debajo de ese valor.

Al explorar los datos por sectores de la industria hay cosas muy llamativas, primero las certificaciones

Gráfica 40: Preferencia de formación del CISO

es el mayor valor, pero solo porque la sumatoria de todos los sectores lo hacen así, pero en ningún sector inclusive otros sectores es el valor más representativo. La consultoría especializada ve en las charlas especializadas el más atractivo y representativo, los diplomados son más apetecidos en sectores como educación, gobierno y salud, en otros sectores la educación formal es la más llamativa, en el sector financiero y telecomunicaciones los programas de formación ejecutiva son los más adecuados o de preferencia para los profesionales de seguridad.

El crecimiento del profesional de seguridad, CISO y los demás roles, siempre buscan mejorar sus habilidades, no deben olvidar mejorar también sus capacidades para incrementar su valor de mercado, por tanto, todas las fuentes que puedan usar para el desarrollo de sus competencias, destrezas, habilidades y capacidades para ser más integrales, los ayudará en gran medida a poder ofrecer un mejor valor en las empresas a las que sirven (Trellix, 2024; IANS, 2024a; IANS 2024b).

Siendo el CISO un ejecutivo nuevo dentro de la esfera de los ejecutivos de las empresas, es claro que tiene que empezar a pulir sus capacidades, al revisar lo que consideran los encuestados que debe mejorar el ciso, en primer lugar, sus capacidades estratégicas se colocan en primer lugar con un 47% y un incremento del 15% con relación al año anterior, seguido de las capacidades intelectuales con un 39% el cual crece un 52%, en tercer lugar

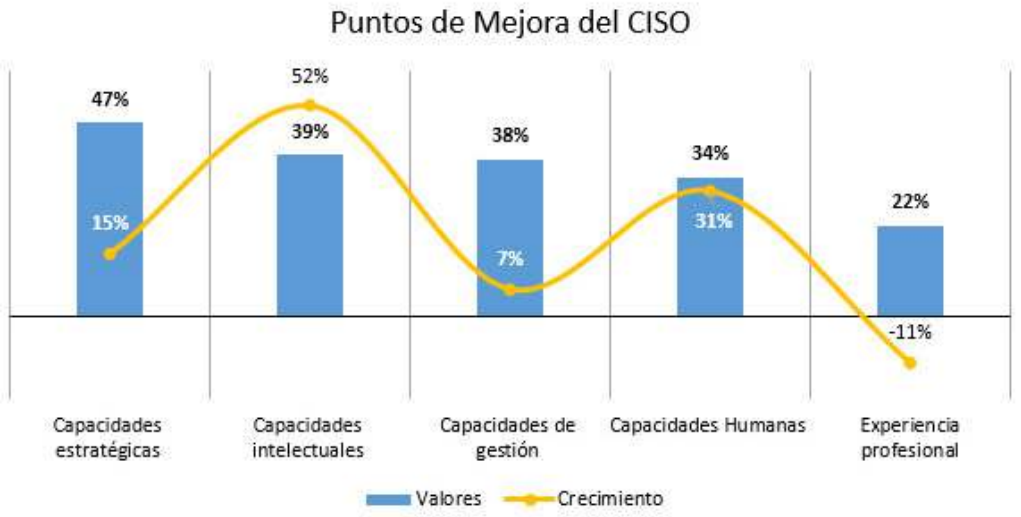
capacidades de gestión con un 38% y un crecimiento del 7% con relación al año anterior, estas pueden verse reflejadas en la gráfica

Es de anotarse que las dinámicas de las empresas y sectores de la industria colombiana hacen que se tengan algunos matices interesantes de estos datos, que se representan en la gráfica 41.

En la profundización de análisis y revisando sectores, y tamaños de las empresas que encontramos, el sector de la consultoría considera en las empresas de 1 a 50 empleados que las capacidades de liderazgo son esenciales para mejorar de los profesionales de seguridad que existen en la actualidad, sin embargo, las capacidades humanas siguen en la profundidad de los datos como una capacidad que requiere ser desarrollada, sectores como educación en tamaños de 1000 a 5000 empleados, telecomunicaciones en las empresas de 1 a 50 empleados, y sector financiero en las empresas de más de 5000 empleados consideran que esta capacidad debe ser desarrollada.

El sector de gobierno en las empresas de 1000 a 5000 empleados resalta que las capacidades intelectuales son las que debe mejorar. Se ha definido el criterio de Capacidades intelectuales como las siguientes (formación académica, conocimientos técnicos, análisis, síntesis). Otros sectores del tamaño de empresa pequeña de 1 a 50 empleados consideran que la experiencia es lo que debe mejorar.

Mejorar en capacidades y habilidades requiere de un proceso sis-



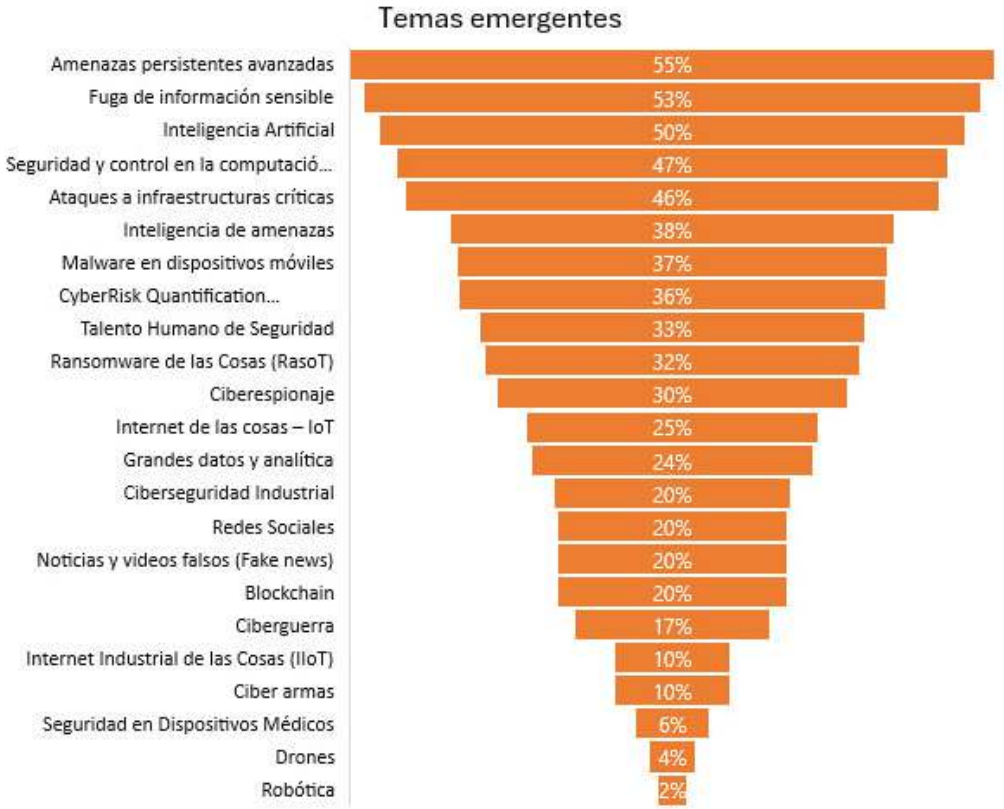
Gráfica 41: Puntos de mejora del CISO

temático y continuo, no solo se trata de la obtención de un certificado de algo, lo que se necesita conciliar son las necesidades de las empresas con las capacidades de los profesionales de seguridad (Pluralsight, 2024; CoderPad, 2024; Harris, B., 2024; Cantrell, S., et all; 2024).

Temas emergentes

La gráfica 42 muestra los temas relevantes y emergentes que tienen en la mira los profesionales de seguridad. Para este año amenazas persistentes avanzadas, fuga de información sensible, y como novedad la inteligencia artificial son los tres primeros temas que están en el radar del profesional de seguridad.

El primero tiene un incremento con relación al año anterior de 22%, el segundo del 15% y el tercero 32%, siendo el último un incremento notorio, que coinciden con los datos de industria que han evidenciado



Gráfica 42: Temas emergentes

claramente a la Inteligencia Artificial como una de las tendencias del año 2024 (WEF, 2024c), ataques a infraestructuras críticas, seguridad y control en la computación en la nube y la inteligencia artificial, son los temas que más están en el radar de los profesionales de seguridad. Parámetros que coinciden con algunas de los temas que han tenido la atención de la agenda de los ejecutivos de seguridad en este 2023 y cosas que se verán en el 2024 (Google, 2024; Brunswick, 2024; Deloitte, 2024b; Verbree et all, 2024; Gartner, 2024).

Consideraciones de los datos

Al revisar los datos comparados con el año inmediatamente anterior hay temas que se ponen en la agenda con más interés de cara al año atipo que es el 2024, un año donde hay la mayor cantidad de elecciones en el mundo y que pueden minar la confianza del globo por los resultados y las tensiones que existen (Atalan, Y., 2024; Edelman, 2024).

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 postpandemia que ha revolucionado y cambiado la forma en cómo la seguridad se tiene que plantear en las organizaciones.

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 Goverment Summint – EY, 2020).

Crear valor en un contexto digital, implica crear nuevos y novedosos esfuerzos por desarrollar programas de ciberseguridad que atiendan a las necesidades de las organizaciones, 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 encontrar equilibrio entre el valor de las nuevas tecnologías y los ciberriesgos que esto conlleva (WEF, 2024a).

La resiliencia cibernética, y los ciberriesgos son un tema clave en el desarrollo de posturas de seguridad que permitan a las organizaciones crear ecosistemas digitales confiables, pasando de una visualización de la seguridad como un objeto de rigidez e intolerancia a un elemento de valor muy flexible y adaptable para las empresas (Istari, 2023; Chaput, 2024).

Las tensiones geopolíticas, la reciente guerra en Ucrania, los conflictos entre Israel y Palestina, las tensiones entre China y Taiwan son parte de las cosas que hoy modelan al ecosistema digital global y que no solo debe ser visto como un reto del ahora sino del largo plazo (WEF, 2024c).

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, que hacen que en Latinoamérica se sientan los efectos y muchos adversarios se sientan motivados a usar esos fenómenos como cortinas de humo para realizar operaciones en la región (Google, 2024; Grupo-IB, 2024).

Las operaciones cibernéticas están disponibles para todos los estados y naciones y en medio de ellas es clave pensar en que se requiere acciones claves para asegurar el ecosistema digital, es por ello por lo que es clave desarrollar medidas no solo los estados sino las empresas en tal sentido, no es solo una labor del estado, es una responsabilidad de todas las empresas (Duke University, 2024).

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 evo-

lucionar, 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 (IANS, 2024a; IANS, 2024b), que deben poder actualizar el conjunto de herramientas como la comunicación para que puedan interactuar con mayor determinación en los equipos de trabajo.

Sin embargo, dichos profesionales deben cuidarse de un mal silencioso que está aquejando a la población de profesionales del mundo, el agotamiento o burnout, del cual se resalta que ha despertado mucho interés pues se empiezan a ver los efectos de este agotamiento en el rendimiento de las personas, la productividad de las empresas y el ecosistema digital en general, que de alguna manera ha ayudado a incrementar la escasez de profesionales de seguridad que se menciona en la actualidad (Vendict, 2024; ISMS Forum, 2024; Almanza, A., 2023).

Los datos de la realidad colombiana 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:

Afianzamiento:

1. Para este año se hizo una profundización al revisar dos variables, no solo los sectores de la industria, sino profundizar en relación con los tamaños de estas, se encuentra que las empresas del sector pequeño entre 1 y 500 empleados, viene desarrollando sus prácticas de ciberseguridad, las empresas grandes consolidan el trabajo que vienen haciendo, y las empresas medianas, frenan un poco sus trabajos.
2. 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, han empezado a ver a la resiliencia como una capacidad necesaria para operar.
3. 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.
4. Generar confianza es un esfuerzo complejo que los CISOs debe hacer, y que a través del afianzamiento y crecimiento en la realidad colombiana, pues ha

dados sus frutos, hoy se ve mejor la posición del CISO, aunque hay mucho camino por recorrer, la visión de un ejecutivo que ayude a las organizaciones a moverse del punto A al punto B en materia de una postura de seguridad, requiere de gran trabajo, y en los sectores maduros está pasando, sin embargo, en los sectores y tamaños que no lo son, se requiere mucho más trabajo.

5. En la misma línea la dirección de las empresas mejora su comprensión del riesgo cibernético, mejora su actuar frente a él, aun así, hay mucho trabajo por desarrollar, mucha más alfabetización digital que explorar, para que dichos cuerpos directivos y ejecutivos puedan mejorar la toma de decisiones en relación con los riesgos a los que se ve expuesto el negocio.
6. 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 organizaciones 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.

Exploración:

7. 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.
8. 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 a repensar sus saberes previos, salir de su zona de confort de manera permanente, entrenarse y continuamente estar en proceso de aprendizaje (Martínez, 2022).
9. 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.
10. 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.

11. 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.
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.

El Futuro:

14. 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).

16. No solo se trata de anticipar al adversario digital, se hace necesario desarrollar capacidad de resiliencia, una buena confianza digital requiere que las empresas y sus miembros entrenen y desarrollen sus capacidades cibernéticas de manera permanente, las simulaciones son un ejercicio que hoy por hoy tiene gran acogida por los beneficios que ofrece para definir un marco de que se puede hacer ante lo inevitable, el día en que ataquen a la empresa.

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.

Referencias

Absolute. (2024). Report: Absolute security's Cyber Resilience Risk Index 2024. Absolute.com. https://www.absolute.com/go/reports/cyber-resilience-risk-index-2024/

Accenture. (2024). Hyper-disruption demands constant reinvention. Accenture.com. https://www.accenture.com/content/dam/accenture/final/accenture-com/document-2/Accenture-Risk-Study-2024-Edition.pdf

Allianz. (2024). Allianz Risk Barometer 2024. Allianz.com. https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024.pdf

Almanza, A. (2023). Cybersecurity and burnout: The cybersecurity professional's silent enemy. ISACA. https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-48/cybersecurity-and-burnout-the-cybersecurity-professionals-silent-enemy

Atalan, Y., Jensen, B., Macias III. (2024). Eroding Trust in Government: What Games, Surveys, and Scenarios Reveal about Alternative Cyber Futures. Csis.org. https://www.csis.org/analysis/eroding-trust-government-what-games-surveys-and-scenarios-reveal-about-alternative-cyber

ATT. (2024). 2024 LevelBlue FuturesTM Report: Cyber Resilience. Att.com. https://cybersecurity.att.com/resource-center/futures-reports/2024-futures-report-cyber-resilience

Auditboard. (2024). Decode the new SEC cybersecurity disclosure ruling. Auditboard.com. https://www.auditboard.com/resources/ebook/decode-the-new-sec-cybersecurity-disclosure-ruling/

Bankofengland. (2024). Systemic Risk Survey results - 2024 H1. Bankofengland.co.uk. https://www.bankofengland.co.uk/systemic-risk-survey/2024/2024-h1

Barracuda. (2024). Top Email Threats and Trends. Barracuda.com. https://assets.barracuda.com/assets/docs/dms/top-email-threats-and-trends-vol1.pdf

Brunswick. (2024). Cyber trends - spring 2024. Brunswick. https://www.brunswickgroup.com/cyber-trends-spring-2024-i26583/

Bugcrowd. (2024). Inside the platform: Bugcrowd's vulnerability trends report. Bugcrowd. https://ww1.bugcrowd.com/inside-the-platform-2024/

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

Cantrell, S., Griffiths, M., Jones, R., & Hiipakka, J. (2022). The skills-based organization: A new operating model for work and the workforce. Deloitte Insights; Deloitte. https://www2.deloitte.com/us/en/insights/topics/talent/organizational-skill-based-hiring.html

Chaput, B. (2024). Enterprise cyber risk management as a value creator: Leverage cybersecurity for competitive advantage (First Edition). APRESS.

Claroty. (2024). STATE OF CPS SECURITY REPORT. Claroty.com. https://web-assets.claroty.com/state-of-cps-security-healthcare-2023.pdf

CoderPad. (2024). State of tech hiring 2024. CoderPad. https://coderpad.io/survey-reports/coderpad-and-codingame-state-of-tech-hiring-2024/

Cofense. (2024). 2024 Annual State of Email Security Report. Cofense. https://cofense.com/annualreport/

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. (2024). Cyberthreat defense report 2024. CyberEdge Group. https://cyberedgegroup.com/cdr/

Darkreading. (2024). How Enterprise Are Responding to the incident response challenge, free dark reading Report. Darkreading.com. https://dr-resources.darkreading.com/free/w_defa5680/?p=w_defa5680

Deepinstinct. (2024). Voice of SecOps 2024. Deepinstinct.com. https://info.deepinstinct.com/voice-of-secops-v5-2024

Deloitte. (2024a). Deloitte cybersecurity threat trends Report 2024. Deloitte United States. https://www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-threat-trends-report-2024.html?id=us:2el:3dp:wsjspon:awa:WSJRCJ:2024:WSJFY24

Deloitte. (2024b). Fortune/Deloitte CEO survey. Deloitte.com. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/us-winter-2024-fortune-deloitte-ceo-survey.pdf

Diligent Institute. (2024, March 26). Cybersecurity, audit and the board. Diligent Institute. https://www.diligentinstitute.com/report/cybersecurity-audit/

Duke University. (2024). Cyber Readiness. Leasson fron the front lines. Website-files.com. https://assets-global.website-files.com/660ab0cd271a25abeb800460/662a5a6baa3e24e7b6f323a4_LATAM%20CISO%20Report%202024.pdf

Edelman. (2024). 2024 Edelman Trust Barometer. Edelman. https://www.edelman.com/trust/2024/trust-barometer

Edgescan. (2024). Vulnerability statistics report. Edgescan. https://www.edgescan.com/stats-report/

Egress. (2024). 2024 phishing threat trends report: January - march insights. Egress.com. https://pages.egress.com/whitepaper-phishing-trends-threat-report-04-24.html

Entrust. (2024). 2024 State of Zero Trust & Encryption Study. Entrust.com. https://www.entrust.com/resources/reports/2024-state-of-zero-trust-and-encryption-study

EY. (2024). Americas board priorities 2024. Www.ey.com; MIT OpenCourse Ware. https://www.ey.com/en_gl/board-matters/americas-board-priorities-2024

EY-IIF. (2024). 13th annual EY/IIF global bank risk management survey. Iif.com. https://www.iif.com/portals/0/Files/content/Regulatory/32370132_2312-4407639_eyiif-global-bank-risk-mgmt-survey_final2.pdf

FAIR. (2024). Cybersecurity risk report. Fairinstitute.org. https://www.fairinstitute.org/2024-annual-cybersecurity-risk-report

Fdic. (2024). Risk Review 2024. Fdic.gov. https://www.fdic.gov/analysis/risk-review/2024-risk-review/2024-risk-review-full.pdf

Fortinet. (2024). 2024 Cybersecurity Skills Gap. Fortinet.com. https://www.fortinet.com/content/dam/fortinet/assets/reports/2024-cybersecurity-skills-gap-report.pdf

Foundryco. (2024). State of the CIO executive summary 2024. Foundryco.com. https://resources.foundryco.com/download/state-of-the-cio-summary

Fsisac. (2024). Navigating Cyber: Annual Threat Review and Predictions. Fsisac.com. https://www.fsisac.com/hubfs/Knowledge/NavigatingCyber/2024/FSISAC-NavCyber24-Report.pdf

Gartner. (2024). Gartner Top 9 Trends in Cybersecurity 2024. Gartner.com. https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends

Gitguardian. (2024). Voice Of Practitioners. The State of Secrets in AppSec. Gitguardian.com. https://www.gitguardian.com/files/voice-of-practitioners-the-state-of-secrets-in-appsec

Google. (2024). M-trends 2024. Google Cloud. https://cloud.google.com/security/resources/m-trends?hl=en

Group-ib. (2024). Hi-Tech Crime Trends 2023/2024 – Latin America. Group-ib.com. https://www.group-ib.com/resources/research-hub/hi-tech-crime-trends-2023-latam/

Haleliuk, R., Sima, C., & Grossman, J. (2024). Cyber for builders: The essential guide to building a cybersecurity Startup. Venture in Security Press.

Harris, B. (2024). The shift to skills-based hiring. Careersinfosecurity.com. https://www.careersinfosecurity.com/blogs/shift-to-skills-based-hiring-p-3643?rf=2024-06-13_ENEWS_SUB_CAIS__Slot1_BLOG3643

IANS. (2024a). State of the CISO, 2023–2024 Benchmark Summary Report. IANS. https://www.iansresearch.com/resources/infosec-content-downloads/research-reports/2023-2024-state-of-the-ciso-benchmark-report

IANS. (2024b). The compensation, budget and satisfaction benchmark for tech CISOs, 2023-2024. IANS.

https://www.iansresearch.com/resources/infosec-content-downloads/detail/the-compensation--budget-and-satisfaction-benchmark-for-tech-cisos--2023-2024

IBM. (2024a). 6 hard truths CEOs must face. Ibm.com. https://www.ibm.com/downloads/cas/QJ2BYLZG

IBM. (2024b). IBM X-Force Threat Intelligence Index 2024. IBM. https://www.ibm.com/account/reg/es-es/signup?formid=urx-52629

IBM. (2024c). Securing generative AI: What matters now. IBM. https://www.ibm.com/account/reg/us-en/signup?formid=urx-52780

Infotech. (2024). CIO Priorities 2024. Infotech.com. https://go.infotech.com/it-cio-priorities-2024-report

Intel471. (2024). Cybercriminals and AI: Not just better phishing. Intel471; CamelCase Collective. https://intel471.com/blog/cybercriminals-and-ai-not-just-better-phishing

ISC2. (2024a). How much do U.S. cyber professionals make? Isc2.org. https://www.isc2.org/Insights/2024/04/How-Much-Do-US-Cyber-Professionals-Make

ISC2. (2024b). The real-world impact of AI on cybersecurity professionals. Isc2.org. https://www.isc2.org/Insights/2024/02/The-Real-World-Impact-of-AI-on-Cybersecurity-Professionals

ISC2. (2024c). Women in cybersecurity: Women in the profession. Isc2.org. https://www.isc2.org/Insights/2024/04/Women-in-Cybersecurity-Report-Women-in-the-Profession

ISMS Forum. (2024). Factores críticos en la generación del estrés de los CISOs y cómo evitarlos. Advens.Fr. https://info.advens.fr/hubfs/2024_ES_Advens-ISMSForum-Estres-CISO.pdf

ISSA-ESG. (2023) Life and times 2023 download landing page. https://issai.informz.net/issai/pages/life_and_times_2023

ITRC. (2024). Identity theft resource center 2023 Annual Data Breach Report reveals record number of compromises; 72 percent increase over previous high. ITRC; Identity Theft Resource Center. https://www.idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high/

ISTARI (2023). The CEO report on cyber resilience. https://istari-global.com/insights/articles/ceo-report/

Kaspersky. (2024a). Incident Response Report 2024. Kasperskycontenthub.com. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2024/05/13125640/Kaspersky-IR_Analyst_report_2023_EN.pdf

Kaspersky. (2024b). The portrait of modern InfoSec professional. Kaspersky.com. https://www.kaspersky.com/blog/portrait-of-infosec-professional-report-2024/

Knowbe4. (2024). Phishing by industry benchmarking report. Knowbe4.com. https://www.knowbe4.com/hubfs/2024-Phishing-by-Industry-Benchmarking-Report-EN_US.pdf?hsLang=en-us

Kroll. (2024). The State of Cyber Defense: Healthcare edition. Kroll.

https://www.kroll.com/en/insights/publications/cyber/state-cyber-defense-healthcare

Leirvik, R. (2023). Understand, Manage, and measure cyber risk: Practical solutions for creating a sustainable cyber program (2nd ed.). APRESS.

Logicalis. (2024). Logicalis CIO Report 2024. Logicalis.com. https://www.logicalis.com/cio-report

Martinez, J. (2021). N°179 Aprender del futuro. http://www.javiermartinezaldanondo.com/n179-aprender-del-futuro/

Metomic. (2024). Metomic's 2024 CISO survey: Insights from the security leaders keeping critical business data safe. Metomic.Io. https://metomic.io/resource-centre/metomics-2024-ciso-survey-insights-from-the-security-leaders-keeping-critical-business-data-safe

Mimecast. (2024). The State of Email & Collaboration Security Report 2024. Mimecast.com. https://assets.mimecast.com/api/public/content/state-of-email-and-collaboration-security-2024?v=f1995772

Moore, M. F. H. D., King, M. F. R., & Sellers, M. F. T. (2024). Download the runZero Research Report. runZero. https://www.runzero.com/research-report/

NACD. (2024). 2024 GOVERNANCE OUTLOOK. Nacdonline.org. https://www.nacdonline.org/globalassets/public-pdfs/nacd_2024-governance-outlook.pdf

Oh, K.-B. (2021). Cybersecurity risk management: An ERM approach. Nova Science Pub.

Orca. (2024). 2024 state of cloud security report. Orca Security. https://orca.security/lp/sp/ty-content-download-2024-state-of-cloud-security-report/

Owen, J. (2018). Mitos de liderazgo: Jo Owen, 3R Editores.

Paloaltonetworks. (2024). Incident Response Report 2024. Paloaltonetworks.com. https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2024-unit42-incident-response-report.pdf

Pluralsight. (2024). 2024 Technical Skills Report. Pluralsight.com. https://www.pluralsight.com/resource-center/technical-skills-report-2024

Proofpoint-Ponemon. (2023). 2023 Ponemon healthcare cybersecurity re-port. https://www.proofpoint.com/us/resources/threat-reports/ponemon-healthcare-cybersecurity-report

Proofpoint. (2023). WHAT WE KNOW overview. https://www.proofpoint.com/sites/default/files/threat-reports/Proofpoint_Threat_Research_Social_Engineering_Report_2022.pdf

Proofpoint. (2024). 2024 State of the Phish report: Phishing statistics & trends. Proofpoint. https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

PWC. (2024). The boardroom mosaic: piecing together the future. Pwc.com. https://www.pwc.com/us/en/services/governance-insights-center/library/assets/pwc-trust-gic-csuite.pdf

scmagazine. (2024). The zero-trust dilemma. SC Media.

https://www.scmagazine.com/whitepaper/the-zero-trust-dilemma

Sophos. (2024). Unpatched Vulnerabilities: The Most Brutal Ransomware Attack Vector. Sophos.com. https://www.sophos.com/en-us/whitepaper/unpatched-vulnerabilities-brutal-ransomware-attack-vector

Splunk. (2024a). The CISO report. Splunk. https://www.splunk.com/en_us/form/ciso-report.html

Splunk. (2024b). The hidden costs of downtime. Splunk. https://www.splunk.com/en_us/form/the-hidden-costs-of-downtime.html

Thalesgroup. (2024). The 2024 Thales Cloud Security Study. Thalesgroup.com. https://cpl.thalesgroup.com/sites/default/files/content/CLOUD_AMI_pages/2024/2024-thales-cloud-security-study-global-edition.pdf

Trellix. (2024). The Mind of the CISO. Trellix.com. https://www.trellix.com/solutions/mind-of-the-ciso-decoding-the-genai-impact/

TrendMicro. (2024). How a communication breakdown in the boardroom is hurting cyber-resilience. Trend Micro. https://www.trendmicro.com/explore/thecisocredibilitygap/2608-tl-en-rpt

Toscano, J. Final decision on SEC's cybersecurity disclosure rules pushed to. https://www.forbes.com/sites/joetoscano1/2023/07/02/final-decision-on-secs-cybersecurity-disclosure-rules-pushed-to-october-2023/

Thompson, C., & Hopkin, P. (2021). Fundamentals of risk management: Understanding, evaluating and implementing effective enterprise risk management (6th ed.). Kogan Page.

Vendict. (2024). CISO Burnout Report. Vendict.com. https://vendict.com/ciso-burnout-report?submissionGuid=dc7112ca-f404-4fc9-9473-54b5a550ab75

Verbree, M., O'Keefe, M., Flint, D., & Winzer, G. (2024). Eight key cyber security trends to watch in 2024 - KPMG Australia. https://kpmg.com/au/en/home/insights/2024/03/cyber-security-trends-predictions.html

Verizon. (2024). 2024 Data Breach Investigations Report. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

WEF. (2024a). Global Cybersecurity Outlook 2024. Weforum.org. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

WEF. (2024b). Strategic Cybersecurity Talent Framework. Weforum.org. https://www.weforum.org/publications/strategic-cybersecurity-talent-framework/

WEF. (2024c). The Global Risks Report 2024. Weforum.org. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

WittKieffer. (2024). Healthcare CISOs: A deep dive into talent & leadership trends. WittKieffer. https://wittkieffer.com/insights/healthcare-cisos-a-deep-dive-into-talent-leadership-trends

Wolfe, T. (2024). CISO REDEFINED: NAVIGATING C-SUITE PERCEPTIONS & EXPECTATIONS. FTI Strategic Communications. https://fticommunications.com/ciso-redefined-navigating-c-suite-perceptions-and-expectations/

World Government Summint – EY. (2020) Cyber Resilience in the Digital Age. https://www.worldgovernmentsummit.org/api/publications/document?id=24717dc4-e97c-6578-b2f8-ff0000a7ddb6

Zidkova, J. (2024). Software vulnerability ratings report 2024. Action1 | Action1 Risk-Based Patch Management. https://www.action1.com/software-vulnerability-ratings-report-2024/

Zongo, P. (2018). The five anchors of cyber resilience: Why some enterprises are hacked into bankruptcy, while others easily bounce back. Ciso Advisory.

***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 Comunnidad CISOS.CLUB, CISOS-COL y CISOS-LATAM (Linkedin) y Miembro del comité editorial de la revista sistemas de ACIS.*

Computación confidencial: Eficiencia de la seguridad en la nube

DOI: 10.29236/sistemas.n171a5

La nube vs OnPremise.

A medida en que los líderes de la empresa confían más en el público y los servicios de nube híbrida, la privacidad de los datos en la nube es imperativa. El objetivo principal de la informática confidencial es brindar una mayor garantía a los líderes de que sus datos en la nube están protegidos y son confidenciales, también se trata de alentarlos a mover más de sus datos confidenciales y cargas de trabajo de computación a servicios de nube. Esto implica que la protección de los datos se da durante el procesamiento.

El control exclusivo de las claves de cifrado ofrece una mayor seguridad de los datos de un extremo a otro en la nube. El contenido del enclave (los datos que se procesan y las técnicas que se utilizan para procesarlos) son accesibles solo para el código de programación autorizado y son invisibles e incognosci-

bles para cualquier otra persona, incluido el proveedor de la nube.

Para tratar tales asuntos fueron invitados Diego Bueno, director del equipo de Ingeniería Cloud en Oracle, para la región denominada multicountry que comprende Ecuador, Colombia, Centroamérica y el Caribe, sin México. Y Alonso Verdugo Medina, chip medical officer de la vertical de salud para Latinoamérica en Microsoft.

En este sentido la idea es conversar sobre los retos, oportunidades y desafíos que esta tendencia de un futuro cercano puede ofrecerles a los servicios de negocios, en un ambiente con una densidad digital más compleja, unos datos que cada vez son más un impulsor del negocio, y un adversario cada vez más sofisticado, señalaron Jeimy J. Cano M. y Andrés R. Almanza J., moderadores del encuentro, quienes formularon la primera pregunta a los invitados:

¿Por qué la computación confidencial es el nuevo paradigma de seguridad y control para las empresas en la nube? ¿Cómo moverse a este nuevo escenario?

Diego Bueno
Ingeniería Cloud
Oracle
Uno de los mayores temores que normalmente representa no sólo para las empresas, sino para cualquier persona es tener la certeza sobre la seguridad de los datos en el momento de moverse hacia una computación en la nube y de ahí surge el concepto de computación confidencial, para que exista una seguridad de los datos en tránsito, servicio ofrecido por los proveedores de nube.

Hablando de una herramienta analítica en términos de seguridad, entra en juego la computación confidencial, muchos proveedores hoy en día lo ofrecen y AWS, Microsoft, GCP, e IBM, Oracle también ya lo tiene porque es una necesidad imperiosa para las empresas, sí, de qué manera señor proveedor de nube usted me garantiza a mí que durante el procesamiento de los datos esto realmente sí va a estar seguro y ni siquiera usted que me los está alojando, va a tener acceso a esa información, entonces entra el concepto de paradigma de seguridad en el sentido de tengo que confiar que ya no solamente el momento en que yo muevo mi data desde un punto origen hacia la nube, van a estar encriptados, sino que también cuando ya estén allá y los empiece a procesar, me ofrecen una capa adicional de seguridad y ahí viene todo el tema de contratos y bueno de más acuerdos que tienen los diferentes proveedores de nube con base también en regulaciones internacionales donde yo tengo que garantizarle al cliente que sus datos van a estar resguardados.

En tal sentido, podemos hablar de tres beneficios clave que me ofrece

la tecnología en la computación confidencial y es la seguridad mejorada de los datos. Otro aspecto es el relacionado con los estándares internacionales como el GDPR de la Unión Europea, uno de los más estrictos del mundo y por último el HIPAA sobre manejo de datos de salud.

Alonso Verdugo Medina
Chip Medical Officer
Microsoft Latinoamérica

Parte del negocio está en analizar el tráfico de la navegación web de los usuarios para entender sus patrones de comportamiento y hacer ofertas, proceso en el que entran en juego algunos aspectos de ética y de moral. En la actualidad no sólo se trata de saber cómo lo almacenamos o cómo lo transportamos de forma segura. Redondeo dos aspectos clave, la privacidad y la confidencialidad. Datos que sean confidenciales y no quiero que queden expuestos y luego los datos sensibles relacionados con la identificación de la persona, sus gustos y condiciones. En los últimos años la relevancia ha ido hacia el uso de datos que no puede ser empleado para segregar. Cuando aparecen los proveedores de nube nativos, o sea un Google o Amazon en donde el tráfico y la información personal es utilizada. Parte del negocio es conocer su tráfico para entender los patrones de comportamiento y hacer ofertas y luego pasarlo a un tercero. Ahí aparecen aspectos de ética y moral que son relevantes. Nosotros los humanos no usamos datos, usamos información, los algoritmos y mecanismos de inteligencia artificial.

Jeimy J. Cano M.
¿Por qué no se conoce tanto este nuevo paradigma en las empresas de Colombia? ¿Es un tema de difusión? ¿Es un tema de demanda? ¿Es un tema de costo?

Alonso Verdugo M.
Chip Medical Officer
Microsoft Latinoamérica
La falta de conocimiento es uno de los principales factores. Los ingenieros y responsables de tecnología en las empresas deben mantenerse actualizados no solo en las nuevas tendencias tecnológicas, sino también en las regulaciones pertinentes. Sin embargo, esto no siempre sucede.

Un ejemplo claro fue la adopción de la tecnología de Message Queues

o colas de mensajes, que facilita la integración de aplicaciones (MQ).

En mi experiencia, el primer gran cliente en adoptar esta tecnología fue el Banco Santander. Cuando la Superintendencia reconoció su potencial, esto incentivó su implementación, generando una ola de adopción en Colombia. Este caso ilustra cómo la difusión y la adopción de nuevas tecnologías pueden depender de la validación y el impulso inicial de entidades reconocidas.

Además, el entrenamiento y la capacitación son fundamentales. En Microsoft, he descubierto que existen muchas capacidades avanzadas, como la computación confiable. Sin embargo, un cliente que ya usa Azure debe no solo habilitar estas capacidades, sino también integrar estos procesos dentro de su organización. No se trata solo de activar una función, sino de gestionar la seguridad y ciberseguridad adecuadamente.

Otro aspecto crucial es la gestión de la información. Por ejemplo, muchas empresas desconocen que pueden utilizar las herramientas de etiquetado de información confidencial en Word o Excel para mejorar su seguridad. Microsoft ofrece alertas cuando se envía información sensible fuera de la compañía, pero estos controles requieren un nivel de conciencia y entrenamiento que impide la correcta implementación.

En última instancia, las barreras son las personas. La adopción de tecnologías como la inteligencia artificial mediante los asistentes como Copilot, en herramientas de desarrollo, (GitHub Copilot) depende no solo de la disponibilidad de la tecnología, sino también de un cambio cultural dentro de las organizaciones. Es crucial capacitarse y entender dónde y cómo estas tecnologías pueden ser aplicadas para aprovechar todo su potencial.

Estas son, en mi experiencia, las principales razones por las que el nuevo paradigma no es ampliamente conocido en las empresas de Colombia. Es un desafío de difusión, demanda, costo y, sobre todo, de educación y cultura organizacional.

Diego Bueno
Ingeniería Cloud
Oracle

Yo agregaría dos aspectos importantes a lo que mencionaba Alonso, uno es el tema de la difusión, lo cual definitivamente juega un papel significativo, no solo en lo relacionado con la computación confidencial, sino en diferentes tecnologías, puesto que lastimosamente eso va pegado al segundo factor y es la demanda de tecnologías avanzadas de seguridad. Recordemos que el año pasado aquí en Colombia hubo una situación fuerte en entidades gubernamentales que fue una noticia, en temas de seguridad. Eso fue un boom, fue terrible, ya que varias entidades se vieron afectadas,

entre esas el Ministerio de Defensa tuvo una afectación importante, entre otras entidades. Después de eso, fue que a nivel presidencial se sancionó una ley para temas de ciberseguridad y que cada entidad debía tener un protocolo y un plan asociado a eso, entonces como bien lo mencionaba hace un momento, se trabaja de manera muy reactiva, se trabaja en temas de seguridad en muchos campos no solo a nivel gubernamental, sino en diferentes empresas, entonces el hecho de que no se hace una difusión constante de nuevas tecnologías y como bien lo mencionó el Doctor Cano hace un momento, también hay muchas personas que no conocen sobre computación confidencial, aún cuando trabajan en el campo de la tecnología. Entonces sí, es muy común, que haya desconocimiento, pero vuelvo al punto anterior, también va muy asociado a la demanda, hasta que no se presenta una eventualidad no se toman las medidas y a consultar qué existe, para qué existe, más allá de un firewall o de un antivirus, sino que existen otros métodos de encriptación adicionales que me van a brindar esas capas de seguridad, entonces es totalmente un tema de difusión y de desconocimiento, a tal punto que hay empresas que ni siquiera saben que existen ya regulaciones en Colombia para el tema de manejo de datos en la nube que existe algo como la circular 005 emitida por el gobierno; que existe la Ley de Protección de Datos 1581 que el gobierno la sacó con base en el estándar GDPR, precisamente que mencionaba yo hace un momento es el estándar internacional más estricto en manejo de datos y que eso ya da unos puntos de partida para yo decir este tipo de datos yo si los puedo tener en la nube, o estos otros definitivamente no, pero eso todavía sigue siendo un mundo desconocido para muchas empresas, entonces eso hace que como bien lo mencionó el Doctor Cano, la computación confidencial es algo que se debe promover, es algo que yo como proveedor entrego, es algo que tengo que contarle al cliente o en general a la industria de tecnología, o en las universidades.

Jeimy J. Cano M.

¿Cómo plantear una transición de los esquemas tradicionales de seguridad y control en la nube a uno basado en computación confidencial? ¿Cuáles serían los pasos y qué cosas se deben tener en cuenta?

Diego Bueno

Comienzo mi respuesta haciendo un breve resumen sobre seis circulares importantes que existen en Colombia con base en el manejo de los datos, una es la circular 007 de 2018 que habla específicamente de los requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad luego en el 2019 sale la circular 005 que ya habla de reglas para el uso de servicios de computación en la nube, ahí fue cuando Colombia hizo como los primeros acercamientos a decir una realidad vamos a ponerlo en la ley y sale esta circular. Luego en el 2020, la circular 008 donde ya hubo una instrucción para el fortalecimiento de la Gestión de Riesgo Operacional de esos datos de lo que pasa a nivel financiero, si se llega a vulnerar de alguna manera los datos. Posteriormente en el 2020 también sale otra circular que fue la 033, en donde nuevamente y digamos que reforzando la 007 requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad, realmente esta 033 fue como una actualización. Por último, en el 2022, que es la más reciente, hace dos años, es emitida la circular 01 para recomendaciones de uso de servicios de la nube, cómo mitigar riesgos de seguridad digital, pero estas circulares, si usted va y se las menciona a muchas personas en empresas, no saben que esto existe y dice, no, no es que en Colombia todavía no hay un marco normativo para eso. Entonces, si hay unos primeros pasos y estas son seis seculares importantes que muchas empresas deberían conocer.

Ahora, respondiendo la pregunta con base en lo anterior, yo lo englobaría en seis pasos sencillos, uno, evaluación y planificación de lo que quiero hacer a nivel de computación confidencial, cuál es mi postura actual de seguridad, es decir, cómo estoy hoy en día y cuál es el caso de uso al que necesito llegar. Dos, compromiso y capacitación de las partes interesadas, entonces cuál es la postura que voy a tener a nivel de compañía para lo que quiero hacer, puesto que muchas veces esto es lo que hace fracasar los proyectos, lo que normalmente se llama el *Change Management*; yo puedo tener un proyecto súper exitoso, pero nadie me lo compró al interior, de tal manera que no se podrá ejecutar, por lo tanto, de qué manera realmente va a

haber una postura de seguridad en todas las áreas o al menos desde el director general hacia abajo y que sea un mensaje en cascada para que eso sea una realidad en la organización. Tres, selección de la tecnología requerida, puesto que las empresas deben optar por proveedores de nube que ofrezcan servicios robustos de computación confidencial y herramientas adicionales de seguridad, llámese cómo se llame dicho proveedor. Cuarto, implementación de un proyecto piloto, ya que este tipo de tecnologías siempre es recomendable probarlas, testear que si funciona más allá de la teoría y que hace lo que yo como cliente final requiero y en tecnología pasa mucho y son los *quick wins* o las victorias tempranas, a través de pruebas que me permitan a mí realmente demostrar que eso sí funciona que eso que yo quiero hacer sirve y que se aplica mi negocio a través de una prueba de concepto o una prueba piloto, pero que yo vea esta seguridad funcionando realmente con lo que necesito hacer. Quinto, integración y migración, ya que una vez seleccionado el proveedor, el siguiente paso es integrar la computación confidencial en los flujos de trabajo existentes, así como en mi ecosistema de aplicaciones, ya que esto a menudo implica reestructurar algunas de ellas, para aprovechar los enclaves seguros que me ofrece el proveedor. Por último, sexto, alineación de políticas de cumplimiento, cuál o cuáles van a ser esas políticas o procedimientos que yo como empresa voy a adoptar con base en la computación confidencial, que requiero de acuerdo con la industria o al propósito del negocio de mi compañía. En resumen, yo lo englobaría en esos seis pasos.

Jeimy J. Cano M.

¿Dónde no están conectados, dónde sí están conectados, dónde hay turnos va a haber una serie de cosas mixtas e híbridas cuando eso ocurre, entonces eso también va a ser un desafío de seguridad para la empresa como tal, ¿no?

Alonso Verdugo M.

Nosotros en Microsoft tenemos un marco de trabajo para la adopción de nuevas tecnologías disruptivas. (Innovación en la economía digital - Cloud Adoption Framework | Microsoft Learn). Mi experiencia me ha permitido observar que los centros de excelencia son un factor clave para adoptar rápidamente este tipo de tecnologías. (Información general sobre el Centro de excelencia (CoE) - Power Platform | Microsoft Learn).

Los centros de excelencia no son un concepto nuevo, han existido durante mucho tiempo. Son elementos indispensables para que las empresas adopten nuevas tecnologías, ya sea computación confiable u otras innovaciones. La evolución tecnológica actual es extremadamente rápida y disruptiva, por lo que estos centros deben incluir

tanto a personas del área de negocio como del área de tecnología, trabajando juntos en torno a la cadena de valor para aplicar las nuevas propuestas tecnológicas.

Dentro de estos equipos, lo primero es una evaluación inicial que incluye cuatro o cinco puntos clave. Se debe analizar los datos y procesos críticos que requieren seguridad. No todo necesariamente requiere el mismo nivel de seguridad, por lo que es crucial priorizar según la regulación y otros factores. Por ejemplo, la protección del capital intelectual de la empresa es fundamental, especialmente en industrias como la farmacéutica, donde se maneja información muy sensible.

Los ciberataques, actualmente, son una amenaza constante. Por ejemplo, hemos visto ataques a gran escala en Ucrania que Microsoft ha documentado, destacando la necesidad de proteger la información en entornos confiables, especialmente en sectores sensibles como energía, agua, transporte público y servicios esenciales.

La evaluación inicial permite identificar necesidades, analizar riesgos y priorizarlos. A partir de ahí, se define una estrategia, se desarrollan objetivos, y se crea un plan de proyecto. Es fundamental capacitar y concientizar al personal, ya que los humanos suelen ser el factor limitante en la seguridad. Luego se realiza una prueba de concepto o un MVP, seleccionando un área piloto para probar la tecnología, evaluar su impacto y ajustar según sea necesario.

El centro de excelencia juega un papel crucial en la implementación, escalado, integración, monitoreo y optimización de la nueva tecnología. Siguiendo principios similares a ITIL, se gestiona la operación y el mantenimiento, incluyendo acuerdos de servicio, manejo de requerimientos y actualizaciones.

En Microsoft, facilitamos cursos sobre computación confiable y otros temas, proporcionando ejemplos prácticos y procesos de certificación para ayudar a las empresas en la adopción y capacitación. (Introducción a la computación confidencial de Azure | Microsoft Learn).

En Latinoamérica hemos visto casos donde la banca ha liderado en la adopción de estas tecnologías, protegiendo información sensible y controlando intentos de acceso no autorizado. Por ejemplo, en Europa, una aseguradora ha implementado un esquema de salud con información gestionada de manera segura, cumpliendo con diversas regulaciones nacionales y permitiendo una gestión eficaz de pacientes con enfermedades crónicas.

Estos ejemplos demuestran que la seguridad de la información es crítica y que la adopción de nuevas tecnologías requiere un enfoque

integral, desde la gestión de datos en la nube hasta el uso seguro de dispositivos personales.

Jeimy J. Cano M.
Diego, puede contarnos algún caso también en algún sector de América Latina.

Diego Bueno
Ingeniería Cloud
Oracle
Mencionaré cuatro casos de éxito, independientemente del proveedor, sobre computación confidencial; en el caso de Colombia, tenemos al Banco de Bogotá, esta compañía aplicó computación confidencial para mejorar la seguridad y entre los datos personales de sus clientes sí que volvió exitoso este proyecto, ya que le ofrecen a sus clientes una capa adicional que permite reducir temas de riesgos de fraude y ciberataques, eso va a repercutir necesariamente en la confianza del cliente y que este diga, o sea, yo como banco, publico datos y digo este año le apostamos a que la tasa de fraude baje o que baje el número de ciberataques, o no tuve ninguno de ellos. Bueno, pues es un banco bastante seguro, creo que vale la pena meter mi información allá, ¿No? Y pues esto muy alineado, con el cumplimiento normativo, por ende, podemos decir esos tres aspectos volvieron exitoso ese proyecto en Banco de Bogotá. En Argentina hay otro caso y muy de la mano con lo que mencionaba Alonso previamente, el Hospital Alemán también hizo una adopción de soluciones de computación y confidencial y es el hecho de ellos poder hacer análisis de los datos médicos sin riesgo de la privacidad de los pacientes, puesto que yo no estoy buscando si Diego está enfermo, si Alonso está enfermo, lo que quiero ver son patologías, patrones, de qué manera yo identifico que está enfermedad tuvo cierta evolución o cierto comportamiento en el tiempo, independientemente del paciente que la tuvo; entonces, qué hace exitoso este tipo de proyectos, la privacidad de los pacientes que me permite a mí hacer una investigación colaborativa con demás médicos probablemente de otras instituciones independientemente del paciente que tiene la enfermedad y eso necesariamente me permite a mí como hospital generar un avance en salud. En Brasil también en temas de Turismo existe un caso, de una empresa que se llama *cereza experience*, que digamos ellos son turismo y crédito, quiénes también para el procesamiento de sus datos, aplicaron computación confidencial. Otros dos casos a mencionar son banco de Crédito del Perú y Banco de Chile Banco, este último básicamente es el banco más grande de ese país, en donde nuevamente muy similar al caso de Banco de Bogotá, usaron esta tecnología para detección de fraudes, transparencia y confianza hacia sus usuarios y nuevamente el tema normativo que yo como empresa prestadora de servicios financieros pueda garantizarle a mis clientes,

que estoy cumpliendo con las leyes de mi país en el caso de Brasil se llama la LGPD que es la Ley General de Protección de Datos y demás estándares que yo tenga en cada país. Por tanto, yo puedo englobar tres factores claves para decir cómo puedo medir que la computación confidencial sea exitosa, uno, cumplimiento normativo; dos, un tema de mejora o aumento de la confianza de mi cliente; y tres, a través de esa innovación tecnológica que hago con la computación confidencial, cómo creo algo más colaborativo, como en el caso de la salud, por ejemplo, sin ver afectada la identidad de mis pacientes, sin importar su enfermedad.

Jeimy J. Cano M.
Interesantes los casos que se tienen en varias industrias, donde muchas personas pueden estar de alguna manera experimentando los efectos positivos de esta nueva tecnología instalada, sin percatarse que están en un ambiente de computación confiable (*Trusted Computing Environment*), con un mayor nivel de aseguramiento y confianza en el procesamiento de sus datos particularmente en la nube.

Jeimy J. Cano M.
¿Cuál es el futuro de la computación confidencial? ¿Qué pueden esperar las empresas en el mediano plazo (3-5 años)?

Diego Bueno
En mi opinión, es algo que promete mejorar significativamente, puesto que los temas de privacidad y seguridad de los datos siguen preocupando en diversas industrias, sobre todo ahora por el boom que hay de la inteligencia artificial, sí, y ahí vienen dos grandes preocupaciones y son, ¿Qué tanta información puede acceder la inteligencia artificial? ¿Qué cantidad de motores de búsqueda por debajo son los que están realmente trabajando y voy a decirlo así, perdón, el término machacando los datos cierto, pero a qué nivel van a llegar y qué tan vulnerable puede estar la información en ese proceso? Aquí el problema es que existe una línea muy delgada para entrar en temas éticos, que es otro de los dilemas en temas de Inteligencia Artificial, dicho lo anterior, básicamente el futuro de la de la computación confidencial puede estar asociado a qué tan acelerada va a ser la adopción y la estandarización de esto en varias industrias, eso va a ser algo determinante para establecer si va a ser una tecnología que va a durar en el tiempo y que a su vez se vuelva más accesible, que se difunda de manera más masiva, con mejores soluciones a nivel de *hardware* y *software*, que proveedores como como Intel y AMD, ofrezcan mejores soluciones, no solo a nivel de máquinas virtuales sino a nivel de desarrollo también, que los SDKs tenga incorporada esta tecnología de manera embebida, ya que los software también son algo que en el día a día se usan tremendamente en todas las industrias y muchas cosas se hacen a través de APIs y cada vez

existen más APIs en diferentes lenguajes, pero yo tengo que también pensar en que tan vulnerable va a estar mi información y simplemente no consumir un servicio, sino de qué manera no va a ser vulnerada dicha data; qué sectores realmente lo van a aprovechar, ya hablamos aquí del sector salud, asimismo es clave para el sector financiero, pero muy seguramente las agencias gubernamentales también se van a montar en ese bus, porque todos los usuarios de un país, usamos muchas entidades gubernamentales, pero muchas veces no sabemos qué está pasando y vuelvo al comentario que hice hace un rato, qué pasa cuando existen esos ataques de seguridad y las primeras que caen son las agencias gubernamentales, uno como usuario piensa, ¿Cuál es la confianza que tengo en el gobierno? Es decir, qué estamos haciendo con los datos, definitivamente el tema regulatorio es algo clave que tiene que ir de la mano con la computación confidencial, lo cual me obliga a mí como proveedor y como usuario, a que entre más estándares haya y entre más la normativa cambie conforme la tecnología avanza, así mismo me debo adaptar a esto. Cierro con el tema de la inteligencia artificial, puesto que esto sigue avanzando muy rápido, pero las primeras conversaciones sobre la confidencialidad y el alcance de esto, se están teniendo en Europa, sobre qué tanto alcance vamos a permitirle a la inteligencia artificial para que esto no se descontrole, entonces, a medida que la computación confidencial tome mucha más fuerza y se vuelva un *MUST*, se va a masificar y evolucionar más rápido en el tiempo.

Jeimy J. Cano M.

Ahora bien, el tema de costos para desplegar las características de la computación confidencial. ¿Son características que se activan de productos ya existentes o se deben instalar nuevos productos? ¿Cómo sería la visión del tema?

Diego Bueno

Yo lo veo desde los puntos de vista uno como lo mencionó Alonso y es nuevamente desconocimiento incluso a muchas empresas les pasa y con todos los proveedores de nube, eso pasa con todos, que este ya ofrecer características de seguridad asociadas que no generan ni una factura adicional, ni un consumo de créditos, ni algo extra en el costo, pero el cliente no lo sabe o el usuario no lo sabe y no lo utiliza. Sí, ahí digamos que también el reto para nosotros como proveedores de nube, es cambiar esa mentalidad del usuario y enseñarle sobre esas funcionalidades o características, para ello hacer workshops de seguridad, hacer talleres de trabajo sobre el funcionamiento de dichas herramientas o por medio de un evento masivo, así como también realizar Assessment de seguridad, para validar el estado actual a nivel de seguridad de su ambiente o qué otras cosas puedes activar como cliente, no necesariamente pagan-

do más. Segundo punto, a medida que esta tecnología avance como pasa con todo cuando se masifica su costo baja, automáticamente eso hace que su costo vaya empezando a ser más asequible para las personas.

Jeimy J. Cano M.
Diego, puede contarnos algún caso en algún sector de América Latina.

y nuevamente vuelvo a los ejemplos de acciones de hardware propiamente dichas para temas de computación confidencial, pero si ellos empiezan a ver qué, pues hay una mayor demanda de esto la ley básica de la microeconomía no a mayor demanda baja la oferta y al revés a mayor oferta, baja la demanda. Eso hace que los costos pues empiecen a equipararse y a hacer mucho más accesibles para las personas.

Alonso Verdugo M.
El futuro de la computación confidencial es prometedor y hay varios aspectos clave que las empresas pueden esperar en el mediano plazo (3-5 años). En primer lugar, veremos una mayor estandarización en los conceptos y una adopción más amplia de estas tecnologías. La colaboración entre los desarrolladores de hardware y software está abriendo nuevas fronteras, impulsando la evolución de la computación confidencial.

Un ejemplo de adopción temprana es el caso de una pequeña empresa en 2021 que utilizó entornos seguros para proteger información sensible, demostrando que no es necesario ser una gran corporación para beneficiarse de estas tecnologías. Además, la demanda por transparencia en el manejo de datos está creciendo. Los clientes y gobiernos están exigiendo saber dónde están sus datos, cómo se usan y qué medidas se toman para protegerlos.

La conciencia sobre la ciberseguridad ha aumentado. Hace unos años, no éramos tan conscientes de quién manejaba nuestra información. Hoy en día, estamos más alertas. Un ejemplo claro es la inversión en seguridad digital por empresas como Telefónica, que, a pesar de invertir millones, deben asegurarse de que los usuarios también adopten prácticas seguras. (Chema Alonso: “Lo verdaderamente peligroso es dejar solos a los niños en Internet con el ordenador en su habitación, sin saber qué hacen y con quién” - Telefónica (telefonica.com)).

En cuanto a la adopción de la computación confidencial, existen mitos que aún deben ser desmentidos.

Muchas empresas aún des-confían de la nube, pensando que exponen sus datos, cuando en realidad, un servicio de nube hiperescala puede ofrecer mayor seguridad que un centro de datos local mal gestionado.

Para startups y empresas que buscan internacionalizar sus soluciones, especialmente en sectores como la gestión de pacientes diabéticos o hipertensos, cumplir con los estándares de seguridad y privacidad es esencial. Esto no solo protege la información, sino que también abre puertas en términos de comercialización y expansión internacional.

Las empresas pueden esperar un aumento en la adopción de tecnologías de computación confidencial, mayor concientización sobre ciberseguridad, y un entorno regulatorio más exigente. Es crucial que las empresas comprendan estas tecnologías y las integren en su cadena de valor para proteger su capital intelectual y ofrecer transparencia a sus usuarios finales.

Jeimy J. Cano M.
En esta conversación encontrar, que incluso dentro del personal de los mismos proveedores de tecnología, la computación confidencial no se conozca, evidencia una oportunidad para detallarlo en profundidad y validar sus ventajas y limitaciones en las organizaciones en Colombia. Lo anterior nos confirma que es necesario abrir un espacio de reflexión y diálogo alrededor del tema en el gremio de tecnologías de información para avanzar en una postura de seguridad y control que ahora no sólo dispone controles para los datos en reposo y en tránsito, sino que pone igualmente el énfasis a los datos cuando están en uso, particularmente en la ejecución de las aplicaciones en entornos locales y de terceros.

Jeimy J. Cano M.
Para cerrar nuestra sesión agradezco una perspectiva resumen de cada uno sobre lo conversado alrededor de la computación confidencial.

Diego Bueno
Bien, yo creo que queda y de nuevo, no solamente por el hecho de trabajar en Oracle sino por estar en la industria de tecnología, en la cual llevo un poco más de 12 años, y es que a la final uno también debe tener una responsabilidad social de hablar de este tipo de temas con la gente en espacios sociales, no necesariamente en el trabajo, pero ayudar en ese proceso de difusión y que se conozca y que sea una preocupación para el común de las personas, otra vez, y a veces yo también doy algunas charlas de temas de inteligencia artificial y hoy en día el activo más valioso que tiene cualquier empresa son los datos, la información, ese es el activo más importante que tienen las compañías, sin embargo, no todos saben el nivel de madurez que tienen de sus datos, ni la capacidad de explotarlos y cómo eso me ayuda a mí y a mi negocio a mejorar, cómo mi marca mejora su Market share, como puedo atraer más clientes, así las cosas, yo me llevo de esta conversación, la responsabilidad de hablar un poco más de este tema en términos generales, claramente

empezando por mi equipo de trabajo, a quienes les dije que debíamos conocer mucho más de esto y promoverlo con los clientes.

También me gusta mucho que ustedes como promotores de la revista se preocupen por estos temas, porque eso hace que seguramente mucha gente cuando lo vea independientemente que sea Diego y Alonso los que hablen, se interesen por el tema y digan oiga, esto es una necesidad imperiosa en mí industria y tengo que ejecutarlo sin duda.

Alonso Verdugo M.
El futuro de la computación confidencial es prometedor y hay varios aspectos clave que las empresas pueden esperar en el mediano plazo (3-5 años). En primer lugar, veremos una mayor estandarización en los conceptos y una adopción más amplia de estas tecnologías.

La colaboración entre los desarrolladores de hardware y software está abriendo nuevas fronteras, impulsando la evolución de la computación confidencial.

Un ejemplo de adopción temprana es el caso de una pequeña empresa en 2021 que utilizó entornos seguros para proteger información sensible, demostrando que no es necesario ser una gran corporación para beneficiarse de estas tecnologías. Además, la demanda por transparencia en el manejo de datos está creciendo. Los clientes y gobiernos están exigiendo saber dónde están sus datos, cómo se usan y qué medidas se toman para protegerlos.

La conciencia sobre la ciberseguridad ha aumentado. Hace unos años, no éramos tan conscientes de quién manejaba nuestra información. Hoy en día, estamos más alertas. Un ejemplo claro es la inversión en seguridad digital por empresas como Telefónica, que, a pesar de invertir millones, deben asegurarse de que los usuarios también adopten prácticas seguras. (Chema Alonso: “Lo verdaderamente peligroso es dejar solos a los niños en Internet con el ordenador en su habitación, sin saber qué hacen y con quién” - Telefónica (telefonica.com)).

En cuanto a la adopción de la computación confidencial, existen mitos que aún deben ser desmentidos. Muchas empresas aún desconfían de la nube, pensando que exponen sus datos, cuando en realidad, un servicio de nube hiperescala puede ofrecer mayor seguridad que un centro de datos local mal gestionado.

Para startups y empresas que buscan internacionalizar sus soluciones, especialmente en sectores como la gestión de pacientes diabéticos o hipertensos, cumplir con los estándares de seguridad y privacidad es esencial. Esto no solo protege la información, sino que también abre puertas en términos de

comercialización y expansión internacional.

Las empresas pueden esperar un aumento en la adopción de tecnologías de computación confidencial, mayor concientización sobre ciberseguridad, y un entorno regulatorio más exigente. Es crucial que las empresas comprendan estas tecnologías y las integren en su cadena de valor para proteger su capital intelectual y ofrecer transparencia a sus usuarios finales.

Computación confidencial

Cinco realidades (y una mentira) en el contexto organizacional.

DOI: 10.29236/sistemas.n171a6

Resumen
La transformación digital acelerada de las organizaciones demanda la incorporación de proveedores de servicios en la nube como apalancadores de las capacidades necesarias para concretar las iniciativas digitales claves para su promesa de valor. En este sentido, el tratamiento de la información en reposo (en los servidores), en tránsito (a través de las redes) y en uso (en el procesamiento de las aplicaciones) establecen retos particulares de seguridad y control que demandan una atención especial. La computación confidencial como nuevo paradigma de seguridad y control para la información en uso establece un nuevo referente para la seguridad en la nube donde ahora fluyen y se procesan los datos de los clientes como fundamento de los objetivos estratégicos de las compañías. Por tanto, este artículo hace una revisión básica de esta temática, plantea algunas realidades (y una mentira) sobre la implementación de este nuevo paradigma y establece algunas conclusiones prácticas sobre sus retos e implicaciones tanto para las empresas como para los proveedores de servicios en la nube.

Palabras clave
Computación confidencial, riesgo cibernético, servicios en la nube, cifrado, entorno de ejecución confiable

Introducción

En la actualidad el tratamiento de la información tanto a nivel individual como organizacional representa no sólo un reto para las empresas, sino un mandato legal que implica fortalecer sus medidas tecnológicas, procedimentales y humanas para demostrar el compromiso y debido cuidado con este activo, sin perjuicio de los eventos adversos que tarde o temprano se van a materializar generando impactos negativos en la reputación de la compañía. En consecuencia, más allá de proteger la información frente a situaciones y riesgos conocidos, el ejercicio de defensa será el que marque la pauta para que tanto los ejecutivos corporativos como los profesionales de seguridad/ciberseguridad desarrollen una postura vigilante que se traduzca en hábitos automáticos que las personas apliquen en el desarrollo de sus actividades (Saydjari, 2018).

En este sentido, la información bien esté en reposo (guardado en servidores), en tránsito (transmitida por redes) o en uso (utilizado por aplicaciones y procesos) deberá contar con mecanismos de seguridad y control que permitan a los operadores adelantar su tratamiento de forma confiable y con la menor exposición, sin perjuicio de las acciones avanzadas o no previstas que un adversario pueda generar y concretar más allá de las medidas instaladas y disponibles para disuadir la acción de éstos últimos. En consecuencia, se requieren articular esfuerzos en estos tres momentos de la información para hacer más resistente a la organización a posibles brechas de datos (Kohnke et al., 2016).

A la fecha se cuentan con diferentes mecanismos de control para la información en reposo y en tránsito que se han venido utilizando con relativo éxito en las organizaciones. Temas como el cifrado de datos, el control de integridad, las soluciones de prevención de fugas de información, las listas de control de acceso y la implementación de esquemas administrativo de segregación de funciones se han configurado como la base fundamental de la custodia y aseguramiento de la información, que aún fuesen comprometidos, es posible contar con alguna evidencia o rastro que permita saber qué ocurrió con la información (Kohnke et al., 2016).

Sin perjuicio de lo anterior, la información en uso mantiene un margen de oportunidad donde es posible encontrar nuevas posibilidades para dejar un menor margen de acción para los atacantes. A la fecha los mecanismos de seguridad disponibles para la información en uso (aquella que se procesa o manipula activamente, reside en la memoria o en dispositivos) como son la autorización y autenticación de usuarios, gestión de permisos

de usuario y métodos seguros para compartir archivos, no consideran el entorno de ejecución de estas medidas lo que mantiene una ventana de exposición clave que puede ser aprovechada por los atacantes de forma silenciosa y posiblemente no detectable (ManageEngine, s.f).

Así las cosas, surge la computación confidencial (CC) como la nueva frontera de aseguramiento de la información en un entorno de procesamiento confiable, esto es, procesar datos en una zona protegida del procesador de un servidor, generalmente situado en la nube, manteniendo la confidencialidad de los datos cifrados en memoria hasta que la aplicación le indique al entorno de ejecución que los descifre para su procesamiento. Esta nueva realidad, poco conocida en la actualidad y disponible a través de muchos de los proveedores de servicios, representa una oportunidad para aterrizar las expectativas de las organizaciones respecto de su apuesta al hacer su transición a la computación en la nube (Mulligan et al., 2021).

Por tanto, este breve artículo presenta una revisión de esta propuesta de seguridad y control para la información en uso, ilustrando al menos cinco realidades a las cuales se van a enfrentar las organizaciones que se decidan por esta opción y una mentira, que pondrá a prueba los supuestos de los ejecutivos de seguridad y control, así como de los directivos respecto del tratamiento de la información ahora y en el futuro.

Evolución, fundamentos y riesgos de la computación confidencial

El *Confidential Computing Consortium* (CCC) define la computación confidencial (CC) como la protección de los datos en uso mediante la realización de procesamientos en un entorno de ejecución de confianza (EEC) (TEE – *Trusted Execution Environment* en inglés) basado en hardware y debidamente certificado (CCC, 2021). En este sentido, la CC más que un conjunto de arquitecturas que se basan en un ECC, es un nuevo paradigma de computación que cubre la seguridad en el hardware, la seguridad de los sistemas y la seguridad de los datos. Es una vista integrada de la protección de los datos en uso que tiene como objetivo que las aplicaciones se ejecuten con una mayor seguridad en un ECC.

Si bien el concepto no es nuevo, ha venido evolucionando desde finales de los 90s y durante la primera década del segundo milenio cuando se introduce la computación de confianza (*Trusted Computing*), y las funciones de seguridad se aíslan en coprocesadores criptográficos o chips de seguridad como TPM/TCM (*Trusted Platform Module* /*Trusted Cryptography Module*), el reto para ese momento era asegurar un procesamiento interno seguro que disuadiera a los adver-

sarios de llegar a funciones críticas del procesador, a pesar de contar con una ejecución de aplicaciones en plataformas posiblemente no confiables (Feng et al., 2024).

A mediados de la segunda década del nuevo milenio, se advierte la evolución de uno de los componentes centrales de la computación confidencial como lo es el ECC, para lo cual Intel introduce la tecnología hardware *Software Guard Extensions* (SGX), que podía construir "enclaves" seguros en espacios de procesos de usuario, esto es, segmentos aislados de ejecución dentro del entorno propio de un servidor. El código y los datos dentro de los enclaves eran inmunes a los ataques de software, y el cifrado de memoria podía evitar ciertos ataques físicos (Feng et al., 2024).

Finalizando el 2019 se consolida el concepto de computación confidencial, se acepta formalmente y comienza su expansión comercial. Se crea el CCC que vincula a proveedores de hardware como Intel, Arm y AMD, así como proveedores de servicios en la nube como Microsoft, Google, Huawei, Alibaba, Baidu y ByteDance, que toman el concepto de ECC tanto para software como para el hardware como paradigma fundamental para desarrollar una arquitectura de computación confiable que termine en entornos virtualizados seguros y resistentes a los ataques (Feng et al., 2024).

El objetivo de la computación confidencial es cifrar los datos en uso en la memoria principal del sistema sin comprometer el rendimiento. La protección de los datos en memoria presenta dos aspectos: (Felk, 2023)

- Cifrar toda la memoria del sistema.
- Cifrar la memoria individual de la máquina virtual (MV) y aislar la memoria de la MV del hipervisor (el hipervisor es un tipo de software, firmware o hardware que crea y ejecuta máquinas virtuales).

En este contexto, la computación confidencial busca asegurar: (Sardar & Fetzer, 2023).

- Confidencialidad de los datos: Las entidades no autorizadas no pueden ver los datos mientras se utilizan en el ECC.
- Integridad de los datos: Las entidades no autorizadas no pueden añadir, eliminar o alterar datos mientras estén en uso dentro del ECC.
- Integridad del código: Las entidades no autorizadas no pueden añadir, eliminar o alterar el código que se ejecuta en el ECC.

Considerando diferentes aproximaciones de una arquitectura de confianza tecnológica colaborativa y las distintas hojas de ruta relacio-

nadas con el desarrollo de la computación confidencial, se detalla a continuación una vista básica de los componentes para la configuración de este nuevo paradigma de computación: (Feng et al., 2024)

- *Capa de hardware-firmware*, que proporciona la base de seguridad de hardware para toda la plataforma computación confidencial, proporcionando las primitivas de seguridad de hardware necesarias y el arranque de seguridad inicial del entorno.

- *Capa de software del sistema*, que gestiona la seguridad de los recursos de hardware de la plataforma de computación confidencial, así como el aislamiento y la transferencia segura entre los componentes de software.

- *Mecanismo de seguridad y capa de servicio*, que presenta un conjunto de mecanismos de seguridad y servicios de confianza para aplicaciones de computación confidencial, y ofrece una abstracción universal de la plataforma de computación confidencial para aplicaciones de alto nivel.

- *Capa de interfaz y aplicación*, que proporciona interfaces de programación unificadas y SDK (*Software Development Kit* – Paquetes de desarrollo de software) para el desarrollo de aplicaciones de computación confidencial.

Si bien este nuevo paradigma busca alcanzar un nuevo nivel de protección y aseguramiento para los datos en uso en tiempo de ejecución, no está exento de retos y riesgos de seguridad situados en el ECC. Un resumen de los riesgos a considerar en este nuevo entorno son: (Feng, 2024).

- Los ataques al sistema y al software incluyen principalmente ataques al kernel del sistema operativo y ataques a las llamadas al sistema. Los ataques al kernel incluyen principalmente ataques de escalada de privilegios y rootkits a nivel del kernel.

- Los ataques de canal lateral se deben principalmente a la gran cantidad de recursos del sistema compartidos entre el entorno normal y el ECC: memoria cache.

- El ataque de ejecución transitoria es un método de ataque que utiliza mecanismos de ejecución especulativa y de ejecución fuera de orden en las arquitecturas de CPU modernas para obtener información sensible:

  - Mecanismos de anticipación de bifurcaciones.
  - Mecanismos de ejecución fuera del orden.
  - Muestreo de datos de microarquitectura, que permite a los adversarios recopilar datos de recursos compartidos de microarquitectura de CPU, como cachés

de datos, búferes de almacenamiento, etc., filtrando así información confidencial a través de dominios de seguridad.

- Los ataques de inyección de fallos exponen información secreta al provocar fallos físicos o basados en software en los cálculos.

Cinco realidades (y una mentira) de la computación confidencial en una organización

Realidad 1. Se puede (y se debe) arreglar las cosas antes de que un incidente en la nube ocurra.

Prepararse de forma preventiva -antes de que se configure una brecha de seguridad- significa transformarse desde una posición pasiva, basada en riesgos conocidos a una de posición proactiva, que trabaja con los proveedores de servicios en la nube para configurar y desplegar un entorno de computación confiable ajustado a sus necesidades de seguridad y control. Los ejecutivos y los profesionales de ciberseguridad están facultados para centrarse en identificar nuevas iniciativas digitales que acompañen la promesa de valor, en lugar de sólo concentrarse en asegurar la protección de la información y asegurar el cumplimiento normativo (Cano, 2023).

Realidad 2. El liderazgo en ciberseguridad empresarial hará la diferencia en la implementación.

Las implementaciones exitosas de la computación confidencial no sólo serán impulsadas por la visión prospectiva del panorama de amenazas de la empresa, sino también, por cuestionar y retar el modelo de gestión del riesgo cibernético actual basado en certezas, y cambiar los modelos mentales y las estructuras organizacionales que subyacen tanto en los profesionales de las áreas de negocio, como en los ejecutivos de la compañía. La voluntad y el compromiso con la implementación del nuevo modelo a nivel directivo será un factor fundamental, sobre todo en un momento en el que la participación de las áreas de negocio en el proceso esté disminuyendo.

Realidad 3. No puede tomar atajos en el camino hacia un nuevo nivel de seguridad y control.

Es determinante que las empresas elaboren un plan de transformación y una narrativa convincentes de implementación de la computación en la nube al comienzo de este viaje, con una agenda de comunicación clara para sus diferentes grupos de interés (Reeves et al., 2024). En este sentido, tanto los ejecutivos como las áreas de negocio deberán asegurar victorias tempranas basada en historias de éxito con sus clientes, de tal forma que se fortalezca la confianza digital en las iniciativas digitales que se despliegen en la nube. De esta forma, en un ejercicio de colaboración, cooperación, coordinación y confianza

tanto los proveedores de servicios en la nube, la organización y los clientes, encuentren en esta nueva apuesta de seguridad y control las mejores razones para hacer la diferencia y hacerse más resistente a los ataques.

Realidad 4. La implementación es un ejercicio de transformación a largo plazo.

Lograr una implementación de la computación confidencial sostenible y un modelo operativo preparado para el futuro exige abordar las transformaciones a nivel de la cultura organizacional de seguridad de la información con una orientación a largo plazo, donde la información se transforme de ser un recurso más de la empresa y pase a ser un activo estratégico para la organización, y no centrarse simplemente en resolver los problemas de control de acceso tradicionales o procurar el aseguramiento de las buenas prácticas de seguridad y control vigentes. El reto es encontrar el equilibrio adecuado entre la creación de experiencias distintas para los clientes y el apetito de riesgo cibernético de la corporación.

Realidad 5. No se pueden inventar cosas sobre el desarrollo de la implementación.

Las implementaciones y despliegues de la computación confidencial requieren planeación y aseguramiento en al menos dos vías: de la empresa hacia los clientes y del proveedor de servicios en la nube hacia la empresa. Lo anterior exige la consecución simultánea de varios objetivos claves, tanto para el cliente como para la empresa, normalmente bajo una inmensa presión externa e interna. Por ello, las empresas no pueden inventar o incorporar elementos distintos de la planeación de estos proyectos sobre la marcha, so pena de comprometer la promesa de valor articulada en los proveedores y materializada en la experiencia del cliente.

Esto implica una gobernanza y un proceso claro para coordinar y asegurar los avances, comunicando y probando los resultados conforme se implementa los componentes de la computación confidencial.

Una mentira: la computación confidencial es especial y no se aplica a todas las empresas.

Cuando se trata de computación confidencial, nadie es especial. Las organizaciones que se deciden a transformar su modelo de seguridad y control en la nube, no tienen motivos para confiarse dada la evolución y sofisticación de los ataques cibernéticos. En este sentido, más que motivar un paradigma de protección se movilizan a uno de defensa que permite tanto a la organización como al proveedor de servicios en la nube configurar un entorno de computación más confiable y resiliente, que permite aumentar la eficiencia de las operaciones, la resistencia a los eventos adver-

sos y el aseguramiento de la cadena de suministro digital que cubra la información en reposo, en tránsito y en uso.

Conclusiones

La seguridad de la información ha avanzado a lo largo del tiempo en la protección de los datos en tránsito y en reposo. Sin embargo, asegurar la protección de los datos en uso sigue siendo un reto en múltiples dimensiones para los propietarios de los datos, la seguridad de los sistemas para los operadores de plataformas y la seguridad de los algoritmos para los procesadores de datos. En este sentido, la computación confidencial aparece como un nuevo paradigma de seguridad y control que enfrenta estos retos mediante el aislamiento de los sistemas a nivel de hardware y la protección colaborativa que implica tanto al hardware como al software.

No obstante lo anterior, al ser no sólo un reto de implementación de tecnología de información, es una apuesta de transformación de la cultura de la seguridad de la información y la apertura de un nuevo panorama de riesgos emergentes con los proveedores de servicios en la nube. Por tanto, implica entender ahora en detalle y profundidad cómo la organización se sitúa en una cadena de suministro digital, donde los diferentes participantes de un ecosistema digital buscan de forma conjunta hacerse más resistentes a los ataques y concretar mejores mecanismos de resiliencia cibernética frente a la inevitabilidad de la falla.

Ahora la gestión del riesgo cibernético orientada por tres elementos básicos: reducir las amenazas, reducir los impactos de un ataque exitoso y disminuir las vulnerabilidades inherentes propias de la organización, se convierte en un mandato base para acompañar el apetito de riesgo cibernético de las empresas, habida cuenta de las iniciativas digitales que las organizaciones comienzan a desplegar de forma acelerada para ganar nuevos posicionamientos en sus diferentes sectores de negocio. Esto implica, reconocer la información y los datos como activos estratégicos que la organización configura y custodia con el consentimiento de sus clientes para lograr las transformaciones que son necesarias en los diferentes grupos de interés.

La computación confidencial se configura como ese nuevo paradigma de la protección de la información en uso que busca disuadir los planes de los atacantes concentrados en los activos estratégicos de información, no para cambiar sus intenciones, sino para aumentar la incertidumbre en su modelo de riesgos dadas la condiciones y características de seguridad y control que este paradigma sugiere, ahora con aseguramiento del hardware y del software de forma conjunta a través de algoritmos de cifrado que hacen opaco el proce-

samiento de las aplicaciones en entornos de ejecución confiables.

El paradigma de la computación confidencial no busca crear seguridad por oscuridad, sino incorporar una nueva capa de protección y confianza para el procesamiento de las aplicaciones y el uso de los datos sensibles, de forma que a pesar de contar con un entorno hostil y agreste de operaciones cibernéticas adversas, las organizaciones se puedan concentrar en desarrollar propuestas digitales novedosas sabiendo que ahora la información en reposo, en tránsito y en uso adquiere un nivel de confiabilidad mayor: incorporar las prácticas y estándares previos para asegurar los controles de acceso tradicionales con una experiencia más confiable al procesar y tratar los datos de sus diferentes grupos de interés con los proveedores de servicios en la nube.

Referencias

Cano, J. (2023). Cyber risk assessment A conceptual framework for executives. *Proceedings 2023 18th Iberian Conference on Information Systems and Technologies (CISTI)*, Aveiro, Portugal. 1-7. doi: 10.23919/CISTI58278.2023.10211418

Confidential Computing consortium (CCC) (2021). Confidential Computing consortium: a technical analysis of confidential computing v1.2. https://confdentialcomputing.io/wp-content/uploads/sites/85/2022/11/CCC-A-Technical-Analysis-of-Confdential-Computing v1.2_updated_2022-11-02.pdf

Felk, Y. (2023). Confidential computing. En Mulder et al. (eds.) (2023) *Trends in Data Protection and Encryption Technologies*. Cham, Switzerland: Springer Nature Switzerland AG. 103-107. https://doi.org/10.1007/978-3-031-33386-6_19

Feng, D., Qin, Y., Feng, W., Shang, K. & Ma, H. (2024). Survey of research on confidential computing. *IET Communications*. 1-22. https://doi.org/10.1049/cmu2.12759

Kohnke, A., Shoemaker, D. & Sigles, K. (2016). *The complete guide to cybersecurity risk and controls*. Bocaraton, Florida. USA: CRC Press

ManageEngine (s.f.). Data in use. https://www.manageengine.com/data-security/what-is/data-in-use.html

Mulligan, D. P., Petri, G., Spinale, N., Stockwell, G. & Vincent, H. J. M. (2021). Confidential Computing—a brave new world. *2021 International Symposium on Secure and Private Execution Environment Design (SEED)*. 132-138, doi: 10.1109/SEED51797.2021.00025.

Reeves, M., Gruß, C., Ellmer, K., Job, A., Bouslov, G. & Catchlove, P. (2024). Five Truths (and One Lie) About Corporate Transformation. *BCG Research*. https://www.bcg.com/publications/2024/five-truths-and-a-lie-about-corporate-transformation

Sardar, M. U. & Fetzer, C. (2023). Confdential computing and related technologies: a critical review. *Cybersecurity*. *6*(10). 1-7. https://doi.org/10.1186/s42400-023-00144-1

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

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–.*

Prevención de fuga de información en cualquier lugar

Servicios de seguridad administrada

CsRA - Ciberseguridad Resiliente Automatizada

Herramientas para análisis de código

Remediación de vulnerabilidades

Tecnologías de ciberengaño

Doble factor de autenticación

Administración de identidades privilegiadas

Consultoría SGSI, BCP, Ethical hacking y análisis de vulnerabilidades

Automatización de procesos

Globaltek

Somos una empresa boutique con más de 29 años de experiencia y permanencia en el mercado colombiano sirviendo a numerosos clientes del sector público y privado.

(+57) 310 2335760
comercial@globalteksecurity.com
Calle 26 No. 69d - 91 Torre 2 Oficina 406 - Centro empresarial Arrecife Bogotá DC
PAGINA WEB www.globaltek.co
LINKEDIN Globaltek
YOUTUBE Globaltek Security

ACIS

ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

JORNADA INTERNACIONAL DE SEGURIDAD INFORMÁTICA

LA CONFIANZA DIGITAL

JULIO AGOSTO

30 - 31 1

Más información en :

www.acis.org.co

3015530540 - 3013670359

https://www.acis.org.co/JISI2024/