No. 169 Octubre - Diciembre DOI: 10.29236/sistemas ISSN 0120-5919

SISTEMAS

Transformación digital y cambio organizacional

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

CONECTA CON NOSOTROS

@Comunidadacis

ACIS

ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

WWW.ACIS.ORG.CO

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

Octubre-Diciembre 2023
Calle 93 No.13 - 32 Of. 102
Teléfonos 616 1407 - 616 1409
A.A. 94334
Bogotá D.C.
www.acis.org.co

NOS RENOVAMOS

LA ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

ACIS

ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

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

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

Editorial

Transformación digital y cambio organizacional

DOI: 10.29236/sistemas.n169a1

Emir Hernando Pernet Carrillo

Maria Mercedes Corral Strassmann

En esta edición se propicia un espacio de conocimiento y reflexión sobre los retos que hoy en día enfrentan las organizaciones ante los cambios constantes en sus ecosistemas digitales, así como sus estrategias de adopción de buenas prácticas para una transformación digital exitosa a su interior.

Nuestro columnista invitado Álvaro Ernesto Carmona, CTO de Bancolombia, presenta la importancia de la interacción de componentes estratégicos, tecnológicos y operacionales en las organizaciones para establecer modelos operativos digitales basados en datos que, además de impulsar una transformación digital exitosa para lograr una escalabilidad organizativa, les genere ventajas competitivas. Álvaro destaca cinco (5) componentes esenciales en los procesos de transformación digital: la infraestructura (Nube, API, Datos), el trabajo colaborativo (Agilismo Organizacional), los modelos operativos digitales, la estructura organizacional y los procesos nativos digi-

tales. La combinación de estos componentes apalanca dicho proceso en favor de la escalabilidad organizacional.

La entrevista en esta edición es con Ana Carolina Ramírez, Gerente del Proyecto de Pagos Inmediatos Interoperados del Banco de la República. Ana Carolina presenta los objetivos del proyecto consistentes en modernizar y robustecer el ecosistema de pagos electrónicos de bajo valor de la economía, para lograr un mejor servicio y satisfacción a los clientes finales del sistema financiero. Este proyecto se fundamenta en los principios de inmediatez, interoperabilidad, seguridad, innovación, costo eficiencia y oportunidad. Adicionalmente, expone los retos que conlleva el proceso de transformación digital en frentes como: interacción con el ecosistema, ajustes en el cambio organizacional y en los procesos orientados a favorecer la prestación del servicio; todo lo anterior, garantizando la sostenibilidad del sistema y su resiliencia frente a futuros cambios tecnológicos.

La investigación se basa en la XXIII Encuesta de Seguridad Informática, capítulo Colombia, soportada por la Asociación Colombiana de Ingenieros de Sistemas (ACIS). En su análisis, el ingeniero Andrés Almanza, destaca cómo estos resultados proporcionan una proyección a nuestro entorno colombiano, que nos ayuda a enfrentar retos y desafíos en ambientes cada vez más digitalizados. El valor y beneficio de la ciberseguridad, se ha integrado a la estrategia de las organizaciones, y se proyecta como una respuesta ante los retos en la seguridad informática, a raíz de los procesos de cambio y transformación digital, evidenciados en los últimos años con el trabajo remoto, los ambientes híbridos, nuevas tecnologías, entre otros.

En el espacio tradicional del foro para la sección Cara y Sello, se contó con la participación de profesionales del sector privado y la academia, desempeñando distintos roles en sus organizaciones: Bogdan Djoric, director para Colombia de myCloudDoor; Luis Puerto, director de Transformación Digital en la Universidad Externado de Colombia; y Alberto Cueto Vigil, Asesor de Tecnología para Juntas Directivas de las Organizaciones. Cada participante presentó su perspectiva sobre los principales aspectos a considerar en un proceso de transformación digital en una organización, el perfil de un líder transformacional, los indicadores de avance y resultado en la transformación digital de una organización, los principales roles de los stakeholders en el proceso de transformación digital de una organización, y las estrategias conjuntas con aliados o socios para enfrentar y prevenir ciberataques. El foro concluyó con la exposición de los mayores retos y oportunidades de un proceso de transformación digital.

Finaliza esta edición con tres artículos, los cuales contemplan diferentes enfoques frente al tema de la transformación digital y cambio organizacional. El Ingeniero Jeimy José Cano PhD, director de la revista Sistemas y experto en Seguridad, nos comparte en su artículo el rol de las juntas directivas junto con el riesgo cibernético, y la adaptabilidad de las organizaciones a las transformaciones del entorno. El segundo artículo presentado por el ingeniero Néstor Nova, profesor asistente e investigador de la Pontificia Universidad Javeriana, expone la importancia de los modelos de madurez digital en la orientación estratégica de las organizaciones, en particular en el mejoramiento de su competitividad y en el desarrollo de sus capacidades de transformación digital. Daniel Andrés Penagos, Ingeniero de Red Hat, nos comparte en su artículo los conceptos básicos de implementación exitosa de transformación digital, que comprende el conocimiento de las nuevas tecnologías, la visión para su correcta aplicación e implementación. Destaca el uso de las plataformas Open Source.

Para finalizar queremos dejar un mensaje a las organizaciones sobre la importancia de un abordaje estratégico para los procesos de transformación digital que incluya los distintos frentes de: talento humano, tecnologías, procesos, y cambio organizacional.

Emir Hernando Pernet Carrillo, DBA, PMP. Asesor en Negocios de Tecnología. Ingeniero de Sistemas y Computación de la Universidad de los Andes, Colombia, y MBA de ese mismo centro educativo. Master of Computer Science de Arizona State University, USA. Doctor of Business Administration de Newport University, USA. Project Management Professional del Project Management Institute. Experiencia de más de 20 años como Asesor de Soluciones Tecnológicas del Departamento de Sistemas de Información del Banco de la República, y Subdirector de Computación Corporativa del Departamento de Tecnología Informática del Banco de la República.

María Mercedes Corral Strassmann, PhD (C)., Ingeniero de Sistemas y Computación de la Universidad de Los Andes; Maestría en Comunicación de datos, University College London de la Universidad de Londres; Programa de Desarrollo Directivo - PDD de Inalde. Experiencia, como Director de Proyectos en el Banco de la República; Gerente de TI de CIFIN - Asobancaria; Vicepresidente de Tecnología de Deceval. Experiencia de más de 20 años como Profesor Universitario en áreas de Ingeniería de software, y Gerencia de proyectos, Maestría y Especialización de Ingeniería de Sistemas en la Universidad Javeriana. Actualmente candidato del Doctorado de Comunicación, Lenguajes e Información en la Universidad Javeriana.

Transformación digital para la escalabilidad

DOI: 10.29236/sistemas.n169a2

Este artículo explora cómo la interacción de algunos componentes estratégicos, tecnológicos y logísticos puede habilitar a las organizaciones para establecer modelos operativos digitales que les den ventaja competitiva.

Álvaro Ernesto Carmona Ruiz

Transformar sin una visión es inútil, pero aún más desafiante sin capacidad de ejecución. La transformación digital es clave para la adaptación de las organizaciones a entornos cambiantes. Algunas organizaciones logran gestionar estos cambios internamente, otras van más allá y logran impactar también su ecosistema empresarial.

En los próximos párrafos, exploraré cómo la interacción de algunos componentes estratégicos, tecnológicos y logísticos puede habilitar a las organizaciones para establecer modelos operativos digitales que les den ventaja competitiva. Estos modelos no solo impulsan una transformación digital exitosa, sino que se centran en la escalabi-

lidad organizativa y en la implementación de modelos operativos digitales basados en datos. Una nota al margen, en este artículo no voy a desarrollar el tema de cultura y talento humano. Es tan importante que requeriría un capítulo aparte para analizar estos elementos en el contexto de la transformación digital.

Cloud, APIs y datos

Quiero destacar dos situaciones significativas en la industria. La primera se remonta a 2002, cuando Jeff Bezos, CEO de Amazon, redactó lo que hoy se conoce como el 'Mandato de las APIs'. Este mandato establecía que todos los equipos dentro de la organización debían comunicarse exclusivamente mediante interfaces de programación de aplicaciones (APIs). Bezos enfatizó la importancia de que no hubiera otro medio de comunicación entre equipos, promoviendo la interacción a través de interfaces y llamadas a métodos remotos, sin importar la tecnología utilizada por cada equipo.

El segundo evento tuvo lugar en 2011, cuando Satya Nadella, CEO de Microsoft, anunció la estrategia de nube, datos e inteligencia artificial de esta compañía. Este anuncio marcó el rumbo de la compañía hacia una 'nube inteligente' basada en plataformas y datos, enfocada en la integración de la inteligencia artificial. Esta estrategia significó un paso importante en la evolución de Microsoft hacia la era de la computación basada en la nube y la analítica de datos.

En el caso de estas organizaciones y otras similares, los datos, la nube y las APIs son componentes esenciales de una estrategia unificada. Al combinarlos correctamente, ofrecen un potencial de escalabilidad extraordinario en una organización, permitiendo un crecimiento exponencial y un desarrollo arquitectónico que potencia su posicionamiento en el mercado.

La APIficación, entendida como la creación de APIs que expongan las capacidades de la organización, facilita la comunicación eficiente entre equipos al permitir que diversas capacidades se utilicen a través de las APIs. Esto posibilita, incluso, reutilizar esas capacidades en situaciones no planeadas originalmente, democratiza las capacidades funcionales impulsando la creación de nuevos negocios, la adaptación a múltiples canales y promoviendo el crecimiento escalable de la empresa.

En cuanto al segundo punto, la nube y su elasticidad, definida como la capacidad de expandirse o reducirse según la demanda, permite la experimentación ágil y la creación de productos mínimos viables de manera más rápida y sin limitaciones grandes de presupuesto o conocimiento.

En tercer lugar los datos, y de manera más precisa su democratiza-

ción dentro de una organización posibilita el uso extensivo de analítica, ML y AI. Esto facilita la delegación de decisiones a algoritmos entrenados con estos datos, permitiendo la automatización de la toma de decisiones en diversos ámbitos.

Integrar estos tres aspectos como capacidades consolidadas en una sola suite ofrece oportunidades competitivas enormes para una organización. Veámoslos juntos: Los equipos internos exponen sus habilidades a través de APIs, permitiendo su consumo tanto interno como externo para la creación de nuevos productos y servicios; Sumemos el uso de capacidades elásticas en la nube, costos variables, creciendo solo cuando se genera verdadero valor y ofreciendo la característica adicional de un crecimiento potencialmente ilimitado; por último y al agregar la utilización de datos empaquetados en modelos analíticos, Ml y AI facilita la toma de decisiones basadas en datos, evitando la necesidad de escalar con personal.

Estos tres niveles de escalabilidad - APIs para alcance sin aumentar el número de aplicaciones, nube para capacidad sin gastos desbordantes en infraestructura y datos para automatización sin expansión de personal- representan juntos una receta poderosa que permite el crecimiento sostenible de una organización.

Agilismo a escala organizacional

Algunas organizaciones están adoptando modelos operativos ágiles, donde equipos de negocios y tecnología trabajan juntos en tribus. Estos equipos semi autónomos operan como startups dentro de la organización, con el objetivo de reducir la burocracia en la toma de decisiones y capitalizar la premisa de que **equipos pequeños empoderados y alienados técnicamente desde una plataforma pueden desarrollar y mejorar productos y servicios de manera más eficiente para sus clientes.**

El manifesto Ágil, http://agilemanifesto.org)/, creado en 2001 por un grupo de expertos y programadores destacados en esta era tecnológica, es fundamental en esta conversación, ya que sentó las bases para el desarrollo de organizaciones ágiles. Su declaración inicial, aunque se centraba en el ámbito del software y las entregas incrementales, puede aplicarse perfectamente a nivel organizacional.

Los cuatro valores principales del Manifesto ágil y que son fácilmente transportables al mundo del agilismo a escala son los siguientes:
1. Personas e Interacciones sobre Procesos y Herramientas → Iteraciones.
2. Software Funcional sobre Documentación Excesiva → Entregas continuas de valor.
3. Colaboración con el Cliente sobre Negociación Contractual → Priorización basada en valor.

4. Adaptabilidad ante el Cambio sobre Seguir un Plan → Todo cambia, todo puede fallar.

Modelos operativos digitales y plataformas

En un mundo de cambios constantes, el paradigma de las organizaciones tradicionales, con especialización definida por silos de negocio y estructuras proyectizadas heredaron una gran cantidad de aplicaciones empresariales y sistemas de información, empleando diferentes lenguajes, sistemas operativos, bases de datos y estructuras. Integrar datos entre estos diversos silos suele ser un proceso lento, complicado y poco confiable. Requiere una gran inversión y personalización de código y datos. Si bien estos modelos fortalecen la autonomía y la especialización, tienen limitaciones a medida que los sistemas se vuelven más complejos.

"La arquitectura tradicional impone restricciones significativas al crecimiento y la capacidad de generar valor. A medida que las organizaciones tradicionales crecen, sufren de desventajas en economías de escala, alcance y aprendizaje. La complejidad originada por la especialización y el trabajo en silos puede anular los beneficios, llevando a la destrucción de valor con cada nuevo aplicativo construido". *Iansiti, M., & Lakhani, K. R. (2020).*

Las organizaciones pueden diversificar sus negocios más allá de su enfoque inicial. Actualmente, vemos bancos en otros sectores además del financiero y gigantes tecnológicos incursionando en áreas como el cine, autos autónomos o el comercio minorista. Estos movimientos reflejan la búsqueda de las empresas por expandirse y adaptarse a diversos sectores para mantener su relevancia en un entorno empresarial dinámico y competitivo.

El mandato de APIs de Jeff Bezos, la visión de nube y AI de Microsoft, junto con el enfoque ágil, ha dado lugar a otra capacidad poderosa que se convierte en la herramienta de transformación por excelencia para estas organizaciones. **Estas empresas han creado plataformas tecnológicas que sirven como el fundamento arquitectónico para todas las soluciones tecnológicas desarrolladas internamente**.

Estas plataformas tecnológicas no son simplemente conjuntos de herramientas, sino más bien ecosistemas de interoperabilidad que aprovechan la disponibilidad de datos dentro de la organización. Esto habilita una capacidad significativa de experimentación y desarrollo de soluciones entre tribus dentro de la empresa, lo que resulta en una escalabilidad mucho más efectiva que la de las organizaciones tradicionales. Las organizaciones digitales se configuran en suites modulares e integradas de activos digitales conformados por herra-

mientas de desarrollo, capacidades de interoperabilidad como APIs o Eventos y datos disponibles para que puedan ser utilizados por diferentes aplicaciones en la toma de decisiones.

Las tecnologías de la información ya no son simplemente habilitadoras y optimizadores de procesos y métodos tradicionales. **En cambio, el software conforma el núcleo operativo real de la organización,** *Iansiti, M., & Lakhani, K. R. (2020).*

Esta transformación implica un cambio fundamental en cómo se concibe y se opera una empresa. En lugar de considerar la tecnología como un soporte a las operaciones, se convierte en el elemento esencial que impulsa y da forma a la actividad diaria y a los servicios ofrecidos por la organización.

Gracias a estos cimientos digitales, la organización adquiere la capacidad de generar retornos crecientes a medida que escala y aprende. La capacidad de utilizar datos de manera efectiva, junto con algoritmos que los analizan y procesan, se convierte en un habilitador esencial para el éxito y la innovación continua de la organización en un entorno cada vez más digitalizado.

Estructura organizacional

Según Wikipedia, la Ley de Conway indica que las organizaciones diseñan sistemas que reflejan su estructura de comunicación interna. Melvin Conway la formuló en 1967, estableciendo que la arquitectura de los sistemas de una organización refleja su estructura organizativa y funcional.

Entendiendo lo anterior, es evidente que, para llevar a cabo una transformación digital en una empresa, la estructura organizacional debe ser diseñada para concretar la visión de la arquitectura deseada. En el ámbito de la arquitectura empresarial, por ejemplo, nada de lo que se defina en esta práctica a nivel técnico organizacional será factible si los equipos encargados de construir y transformar no se alinean con las capacidades establecidas en la arquitectura.

No pretendo afirmar que la arquitectura empresarial deba dictar el diseño exacto de la estructura organizativa. Sin embargo, sugiero que, para una correcta implementación de la visión de la transformación digital, las estructuras organizativas deben considerar la visión de la arquitectura de los sistemas que sustentarán dicha transformación. *Iansiti, M., & Lakhani* , A., en su libro “Competing in the age of AI” definen esto como 'the mirroring hypothesis'.

Procesos nativos digitales

En las organizaciones establecidas por años la experiencia diseñando procesos basados en interacciones humanas puede enfrentar dificultades al concebir la automatización nativa digital. Mientras los startups,

por necesidad, desarrollan procesos con mínima o nula interacción humana, las empresas consolidadas, debido a la inercia, tienden a optimizar los procesos existentes. Utilizan, por ejemplo, minería de procesos o métricas centradas en la automatización de etapas en los procesos. Este enfoque rara vez desafía el 'qué' de los procesos, limitándose más bien a mejorar el 'cómo'."

En una organización exitosa, la ejecución de estrategias a lo largo del tiempo es altamente deseable. Sin embargo, existe un riesgo inherente en la inercia organizativa que tiende a preservar el conocimiento actual en lugar de adoptar nuevas formas de pensar. Los startups aprovechan este aspecto y, por ende, suelen ser más exitosas innovando que las empresas establecidas. Este fenómeno se hace especialmente evidente en el diseño de procesos y por ello si bien parece obvio, el trabajo de automatización y optimización de los procesos debe involucrar un mindset retador a los comportamientos aprendidos por años.

Conclusión

A lo largo de este texto, he explorado cómo la coordinación de varias estrategias técnicas, como la adopción de la nube, la APIficación del backend, la democratización de los datos, el agilismo, los modelos operativos digitales y las plataformas integradas, junto con elementos logísticos como el diseño de estructuras organizacionales y la mentalidad de procesos nativos digitales, puede constituir una combinación poderosa para concebir y ejecutar la transformación digital en favor de la escalabilidad. Reconozco que este enfoque se hace desde una visión tecnológica del negocio. Mi expectativa es que estas ideas aporten al debate sobre la transformación y evolución tecnológica de las empresas y su capacidad de escalar en el tiempo.

Referencias

Beck, K., et al. (2001) The Agile Manifesto. Agile Alliance. http://agilemanifesto.org/

Conway, Melvin. "Conway's Law". Mel Conway's Home Page. Archived from the original on 2019-09-29. Retrieved 2019-09-29.

Iansiti, M., & Lakhani, K. R. (2020). Competing in the age of AI: strategy and leadership when algorithms and networks run the world. Boston, MA, Harvard Business Review Press.

Rubini, A. (2018). Fintech in a flash. In De Gruyter eBooks.

Álvaro Ernesto Carmona Ruiz: *CTO de Bancolombia. Arquitecto y Líder de TI con 28 años de experiencia en diseño de organizaciones, productos y proyectos. Liderazgo de grandes equipos de ingeniería con más de 30 proyectos exitosos y más de 14 productos de software. Becario Fulbright 2020. Ingeniero de Sistemas de la Universidad Nacional de Colombia, 1999. Msc en Ingeniería de Sistemas y Computación de la Universidad de los Andes, 2003 y Msc in Technology Innovation at University of Washington, 2021.*

Sistema de pagos inmediatos

DOI: 10.29236/sistemas.n169a3

Ana Carolina Ramírez, gerente de Pagos Inmediatos del Banco de la República, dio respuesta a las inquietudes formuladas por los editores técnicos de este número de la revista: María Mercedes Corral y Emir Pernet.

La metodología de trabajo implementada para este proyecto marcará un punto de referencia interesante en la planeación de los proyectos que el Banco de la República emprenda en el futuro, asegura la entrevistada.

¿En qué consiste el Sistema de Pagos Inmediatos y cuales aspectos motivaron el desarrollo de esta iniciativa?

El proyecto de pagos inmediatos interoperados está enfocado en modernizar y robustecer el ecosistema de pagos electrónicos de bajo valor de la economía, fundamentado en los principios de inmediatez, interoperabilidad, seguridad, innovación, costo eficiencia y oportunidad (24/7*365).

Si bien en Colombia ya existen sistemas que permiten operaciones inmediatas, la forma como se presta el servicio hoy en día presenta oportunidades de mejora para contribuir en la promoción de su usabilidad. Por ejemplo, hay diferencias

en costos para el usuario final, carencia de interoperabilidad plena y una experiencia de usuario que no es homogénea.

Sumado a esto, en 2021 el Fondo Monetario Internacional y el Banco Mundial hicieron algunas recomendaciones para los sistemas de pago de bajo valor, entre las que se señalaba la importancia de generar un mecanismo de liquidación de transferencias en dinero de banco central y la puesta en marcha de un Comité de Pagos.

Así las cosas, el Banco de la República decidió abordar estas oportunidades mediante el proyecto de pagos inmediatos interoperados procurando un servicio que cumpla los estándares internacionales de operación y bienestar para los usuarios.

¿Cuáles son los retos más importantes que enfrenta el proyecto de parte del ecosistema financiero y regulatorio?

El Banco de la República está facultado para operar sistemas de pago de bajo valor, no obstante, para lograr los objetivos planteados era necesario hacer varios ajustes regulatorios. Con esto en mente, el Banco, a través del artículo 104 del Plan Nacional de Desarrollo 2022-2026, se convierte en el regulador de los sistemas de pago de bajo valor inmediatos.

Este cambio en el arreglo institucional es importante y estamos convencidos en que es un complemento necesario para, de la mano de la operación, lograr que el servicio de pagos inmediatos se brinde bajo estándares que promuevan la innovación y la aparición de nuevos casos de uso y en consecuencia generen escalabilidad del ecosistema.

¿Cuáles son los retos más importantes que enfrenta el proyecto al interior de la organización? (Por ejemplo, en temas de Cambio Organizacional, Nuevas Tecnologías, Talento Humano, Interfaces con Sistemas Existentes, entre otros).

La puesta en marcha del sistema de pagos inmediatos interoperados implica un cambio relevante en la forma en que el Banco de la República va a interactuar en el ecosistema de pagos de bajo valor. Como es de esperarse, el hecho de que el Banco sea ahora regulador implica una serie de ajustes organizacionales orientados a conllevar ambas funciones segregadas y a su vez alineadas al cumplimiento de los objetivos trazados.

Por otro lado, desde el punto de vista de la operación, el Banco será el proveedor del mecanismo para la liquidación de operaciones entre Entidades participantes, así como del directorio centralizado, ambos críticos para lograr la interoperabilidad plena. Este hecho obliga a generar capacidades al interior de la entidad además de ajustar y crear procesos orientados a favorecer la prestación del servicio. Además, la operación del sistema estará soportada en una solución tecnológica robusta que significará un ejercicio de capacitación y formación importante orientado a aprovechar todo el potencial de esta.

¿Cuál él es el impacto más importante que se espera tenga el proyecto en el ciudadano colombiano?

Una vez entre en funcionamiento el sistema de pagos inmediatos interoperados bajo los lineamientos de la regulación, lo cual se espera que ocurra en 2025, los usuarios finales contaran con una experiencia homogénea y podrán hacer uso de la interoperabilidad plena indiferente de la entidad en donde estos tengan su cuenta o billetera). De esta manera se espera que el proceso de adopción de las transferencias inmediatas como instrumento de pago crezca y motive a la industria a ofrecer nuevas funcionalidades y casos de uso, tal como ha ocurrido en países como Brasil e India.

¿Cuál él es el impacto más importante que se espera tenga el proyecto en la economía del País, tanto en su ámbito interno como a nivel internacional?

Nuestra expectativa es que el proyecto permita avanzar en la digitalización de los pagos de la economía, hecho que a su vez contribuye, de manera indirecta, a objetivos superiores de política pública como los de inclusión financiera, la reducción del uso del efectivo y la formalización.

¿Considerando que los cambios tecnológicos son cada vez más frecuentes y disruptivos, que estrategias se han considerado para garantizar la sostenibilidad y la evolución del sistema de pagos inmediatos?

Sin duda alguna uno de los elementos más importantes entorno a la sostenibilidad del sistema y a su resiliencia frente a cambios tecnológicos, está en el uso de estándares que van a ser indicados a través de la regulación. Hasta el momen-

to, los servicios de pagos en el país habían avanzado utilizando esquemas propietarios o de industria, los cuales hacían difícil su escalabilidad y restringían la aparición de servicios superpuestos.

La reciente regulación creo el Comité de Interoperabilidad de Pagos Inmediatos (CIPI) con el objetivo de fomentar un espacio de diálogo con la industria para la construcción de consensos entorno a los estándares, principios y parámetros que deben seguir cada uno de los actores del ecosistema de pagos inmediatos. De esta forma, esperamos que la convergencia a dichos estándares pueda darse de forma ordenada, facilitando la escalabilidad del sistema y, eventualmente, la interconexión con sistemas de otros países para cubrir, por ejemplo, pagos transfronterizos.

¿Considerando este proyecto como parte de un proceso de transformación digital en una organización, que aspectos importantes podría usted destacar para futuros proyectos en su entidad o en otras entidades?

El proyecto en mención ha motivado al Banco de la República a moverse a la frontera de la tecnología de pagos, lo que se refleja en acercarse a proveedores de primer nivel y a abrir discusiones de reorganización en favor de la innovación. Además, ha permitido una interacción activa con el sector privado. Durante la etapa de conceptualización de la arquitectura del sistema como de la regulación, el Foro de Sistemas de Pago fue definitivo pues se convirtió en un espacio clave para la construcción de consensos y la definición colegiada de las temáticas a tener en cuenta durante la ejecución del proyecto.

Para lograr avanzar se ha contado con un equipo de expertos locales e internacionales, para lo cual hemos tenido el patrocinio de distintos organismos multilaterales como el Programa de Cooperación Económica SECO de la Embajada Suiza, el Banco Interamericano de Desarrollo, el Banco Mundial y la Alianza Mejor que el Efectivo de Naciones Unidas. La interacción con los distintos equipos consultivos ha sido fundamental para recopilar en el diseño del proyecto, las mejores prácticas internacionales.

En suma, la metodología de trabajo implementada para este proyecto marcará un punto de referencia interesante en la planeación de los proyectos que el Banco de la República emprenda en el futuro.

XXIII Encuesta Nacional de Seguridad Informática

Valor y beneficio de la ciberseguridad.

DOI: 10.29236/sistemas.n169a4

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 2023, contó con la participación de 195 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.

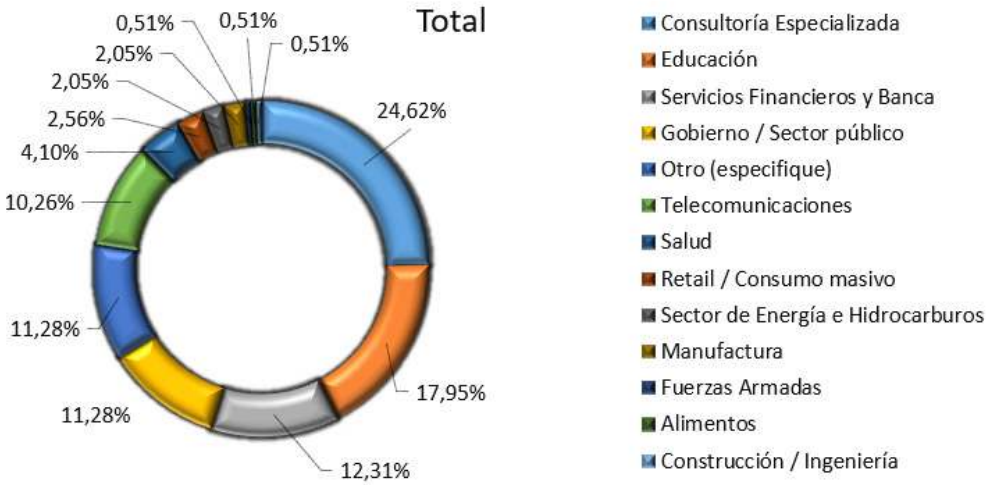
Temas emergentes: En esta sección se analizan varios aspectos, entre ellos: la percepción del futuro en materia de ciberseguridad; la vinculación de los directivos de la organización en la ciberseguridad empresarial, además de la responsabilidad y el papel del líder de seguridad en el desarrollo de la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

Hallazgos principales

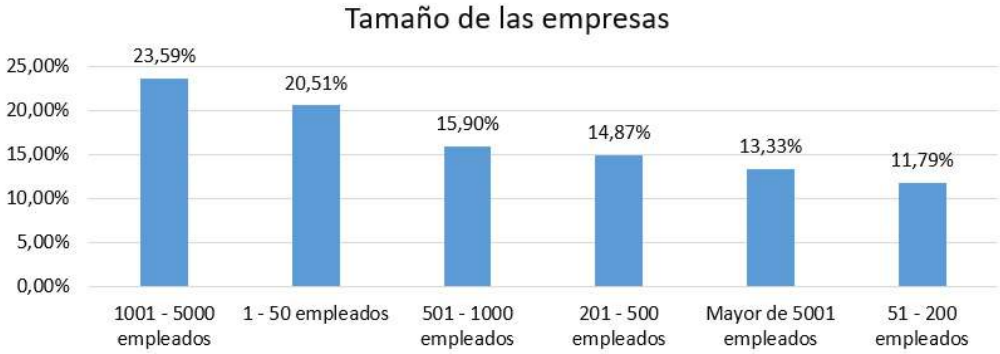
Demografía

Sectores participantes

La gráfica 1 refleja la participación de 13 sectores de la economía colombiana. Los tres segmentos con



Gráfica 1. Sectores participantes

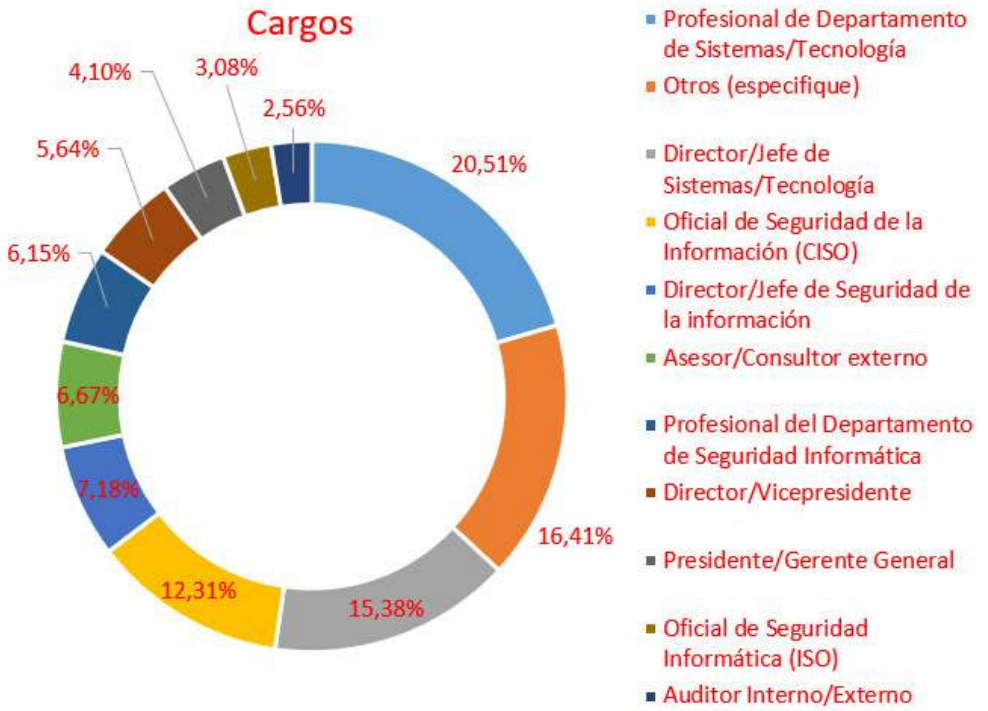


Gráfica 2. Tamaño de las empresas participantes

mayor participación de la encuesta para este año fueron Sector de Tecnología, Financieros, Educación y Consultoría especializada los más representativos en participación.

La gráfica 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

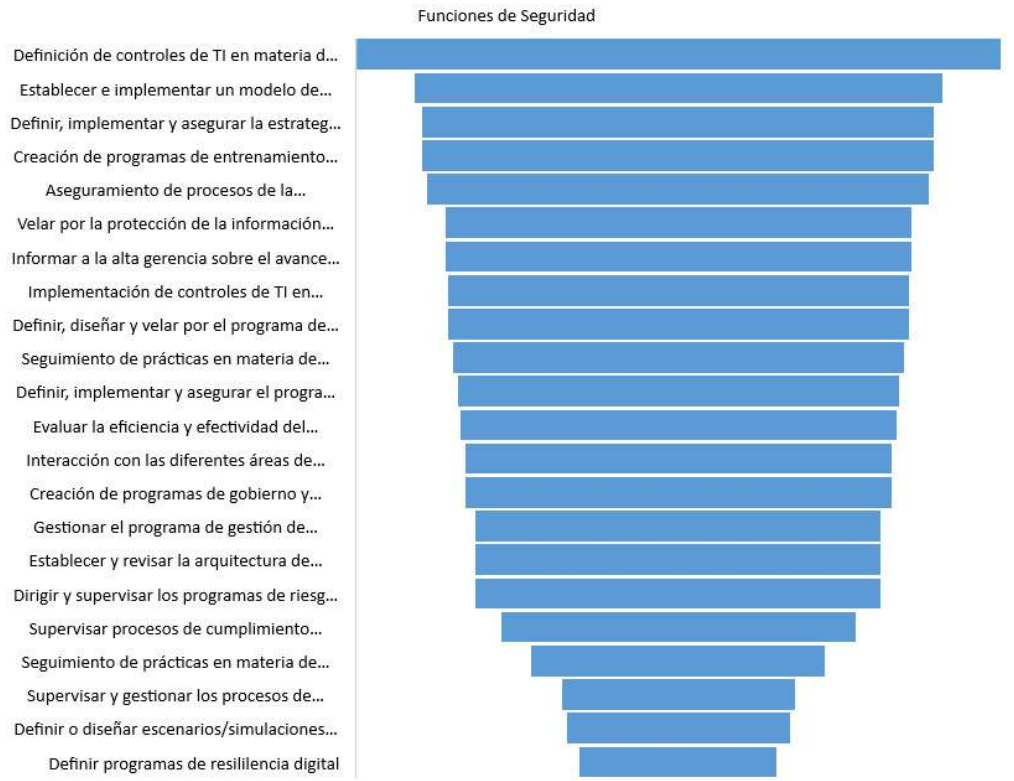


Gráfica 3. Cargos de los encuestados

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 ciberseguridad 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.



Gráfica 4. Funciones del responsable de seguridad

Gráfica 5. Dependencia del área de Seguridad

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 infor-

Gráfica 6. Roles de Seguridad

mación es el número 1, seguido de la posición CISO u Oficial de Seguridad de la Información y analista de seguridad informática.

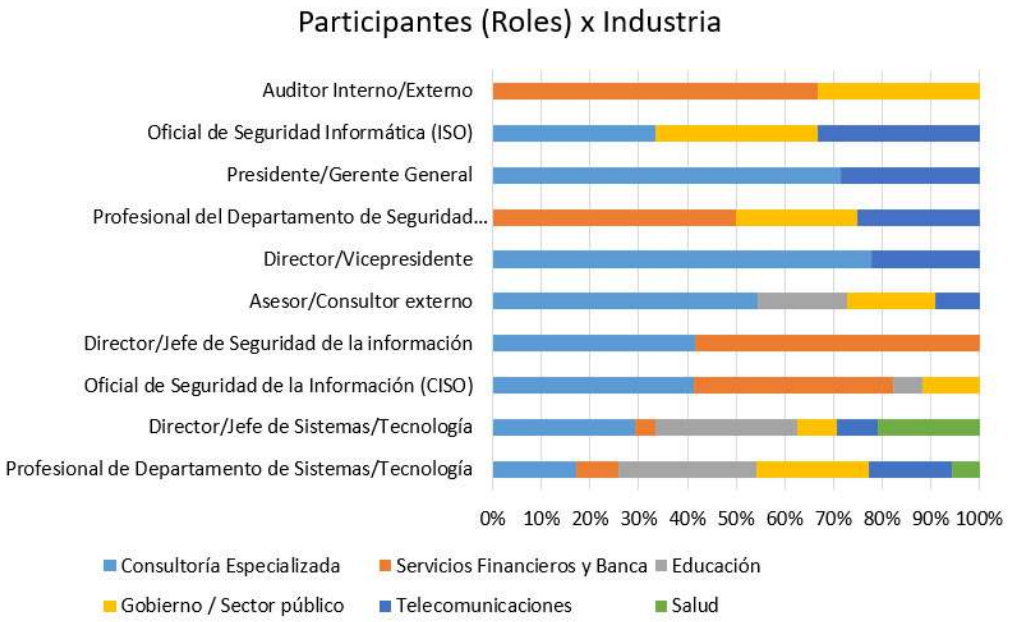
Consideraciones de los datos

Participación de la industria

Este año 2023, ha mantenido comparado con el 2022 una participación interesante de los profesionales de seguridad. Se sigue consolidando la encuesta de seguridad como un instrumento para entender la realidad nacional y en esa medida la participación de estos encuestados se mantiene.

Según las reuniones sostenidas en la agenda global del Foro Económico Mundial en Davos del 2023, se ha vuelto a manifestar que no importa el tamaño de las empresas, o el sector de industria, los riesgos cibernéticos afectan a las empresas y todas sin excepción están expuestas a lo inevitable, un ciberataque. Por tanto, la cooperación, colaboración y entendimiento de la realidad cibernética ya no es un lujo sino una necesidad que necesita de un ejercicios riguroso, constante y consistente, donde se estudie desde múltiples aristas como viene evolucionando el ecosistema digital y como el mismo adopta y fortalece sus esquemas de ciberseguridad en aras de desarrollar una mejor resiliencia.

Al revisar en la gráfica 7 la distribución de los cargos de los encuestados distribuidos en los sectores de



Gráfica 7. Roles x Sectores

la industria y los tamaños de las empresas, encontramos las siguientes consideraciones. En los sectores del Gobierno, Telecomunicaciones y Educación el rol que participa del instrumento es el profesional de las tecnologías de la información. En el sector de Salud participan más los directores de las áreas de tecnología, por su parte el sector financiero y el de consultoría es la figura de CISO y o directores de seguridad los que más participan.

Tendencia de participación que se ratifica al revisar reportes de industria como el informe anual de la Asociación de Control y Auditoría (ISACA) llamado "*State of Digital Trust 2023*" (ISACA, 2023) en donde el 26% de los participantes corresponden al sector financiero, 21% al sector de las tecnologías de la información y el 11% al sector del gobierno. Se puede concluir que estos instrumentos generan con el tiempo confianza de los participantes, puesto que ayudan a explorar con cada año de su realización la realidad del país y con ello ver las dinámicas y cambios en materia de seguridad digital en las empresas.

Roles, responsabilidades y funciones

Si bien es cierto que la función las dos funciones principales de los profesionales de seguridad se mantienen con el pasar del tiempo (definir controles de TI en materia de seguridad y establecer un modelo de políticas), existen pequeñas variaciones en las funciones.

Al revisar los datos por los diferentes sectores de la industria, si se pueden ver unas dinámicas interesantes propias de cada sector, entre los cuales se destacan:

1. A excepción del sector financiero, todos los sectores consideran como función principal que el profesional de seguridad se dedica a la "*Definición de controles de TI en materia de seguridad de la información*"; el sector gobierno es un caso especial pues en la primera posición comparte la función con la función "*Establecer e implementar un modelo de políticas en materia de seguridad de la información*"; contrario a todos los demás para el sector financiero la primera de las funciones es el "*Seguimiento de prácticas en materia de seguridad de la información*"; el sector de telecomunicaciones comparte el primer lugar con la función "*Velar por la protección de la información personal*".
2. En el caso de la segunda función más destacada hay variaciones interesantes, el sector de la consultoría considera que la "*Creación de programas de entrenamiento en materia de seguridad de la información*" ocupa la segunda posición, el sector educación considera a las funciones "*Aseguramiento de procesos de la organización y Definir, implementar y asegurar el programa*

de protección de datos personales de la empresa", que es razonable pues gran parte de la cantidad de datos que se manejan en estos sectores y una de sus funciones es preservar la privacidad, en donde el 44% de los profesionales y equipos de ciber/seguridad suministran información sobre la privacidad de los datos cuando esta es requerida (KPMG, 2023); el sector del gobierno la segunda función más importante la reparten entre "*Aseguramiento de procesos de la organización*"; el sector salud las variaciones entre las funciones son mínimas, pero la que resalta es "*Definir, implementar y asegurar la estrategia de ciberseguridad de la empresa";* el sector de telecomunicaciones considera que la función "Velar por la protección de la información personal", por último el sector financiero considera que la "*Definición de controles de TI en materia de seguridad de la información*" es su segunda función más importante.

3. La tercera función de importancia también tiene interesantes puntos de vistas, el sector de la consultoría considera que "*Definir, implementar y asegurar la estrategia de ciberseguridad de la empresa*"; el sector determina que la función en esta posición es "*Definir, implementar y asegurar el programa de protección de datos personales de la empresa*"; el sector del gobierno ve al "*Dirigir y supervisar los programas de riesgos de seguridad de la información de la organización*"; por su parte el sector de salud ve a la "*Implementación de controles de TI en materia de seguridad de la información";* mientras que el sector financiero considera al "*Establecer e implementar un modelo de políticas en materia de seguridad de la información*"; por último el sector de las telecomunicaciones considera que "*Definir, diseñar y velar por el programa de privacidad de la información de la organización*" que al igual que el sector salud, la información de sus clientes maneja información de datos personales que debe ser protegida, al revisar reportes de industria como (Proofpoint-Ponemon, 2023) e (ISACA, 2023) se ratifica que la protección de la privacidad es un fenómeno relevante para mejorar los ecosistemas digitales de las empresas.

Lo anterior muestra que cada sector de la industria está enfocando sus esfuerzos de acuerdo con sus niveles de madurez y la forma en cómo han evolucionado, ejemplo de esta afirmación es el caso del sector salud, que junto con el sector educación han sido los dos sectores que más han sido afectados durante el 2022 como lo mencionan informes de la industria (Verizon, 2023). La tabla 1, muestra la forma en como todas las funciones se visibilizan en los sectores principales.

Tabla 1. Distribución de responsabilidades por sectores

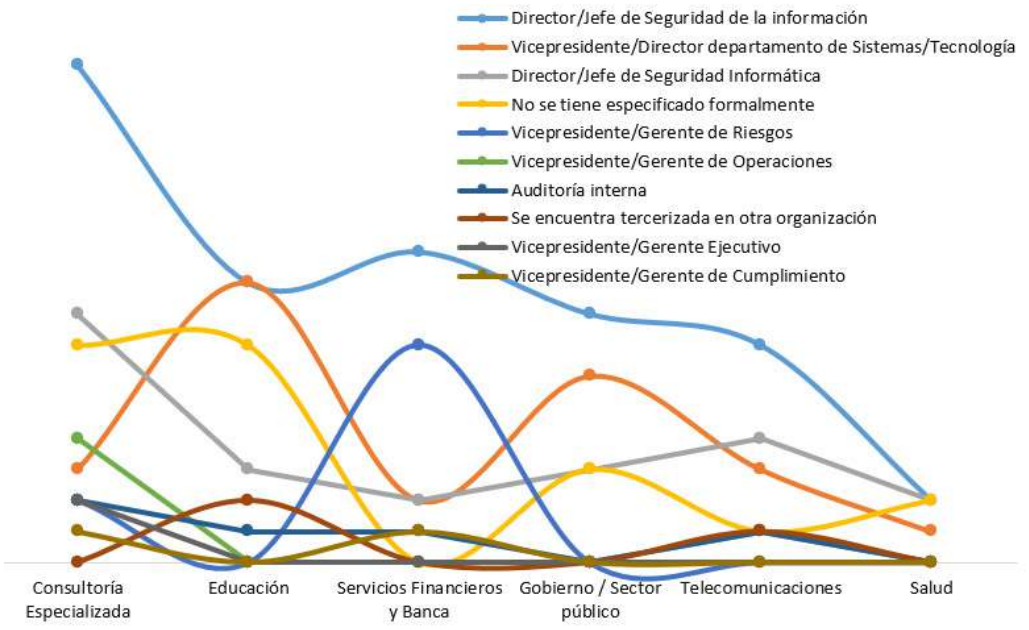
Valores	Consultoría Especializada	Educación	Gobierno / Sector público	Salud	Servicios Financieros y Banca	Telecomunicaciones
Definición de controles de TI en materia de seguridad de la información	17,44%	9,74%	6,15%	3,08%	8,72%	5,13 %
Establecer e implementar un modelo de políticas en materia de seguridad de la información	15,90%	6,67%	6,15%	2,05%	8,21%	3,08 %
Aseguramiento de procesos de la organización	13,85%	8,72%	5,13%	1,54%	8,21%	4,10 %
Definir, implementar y asegurar la estrategia de ciberseguridad de la empresa	16,41%	6,67%	3,59%	3,08%	7,18%	3,08 %
Creación de programas de entrenamiento en materia de seguridad de la información	16,92%	5,64%	3,59%	2,05%	7,69%	3,59 %
Definir, diseñar y velar por el programa de privacidad de la información de la organización	13,33%	7,18%	4,62%	2,56%	5,13%	4,62 %
Implementación de controles de TI en materia de seguridad de la información	12,82%	8,21%	4,62%	3,08%	4,10%	4,10 %
Velar por la protección de la información personal	11,79%	6,15%	4,10%	3,08%	6,15%	5,13 %
Definir, implementar y asegurar el programa de protección de datos personales de la empresa	10,77%	8,72%	4,62%	3,08%	5,13%	4,10 %
Seguimiento de prácticas en materia de seguridad de la información	13,33%	5,64%	3,08%	2,05%	9,23%	2,05 %
Informar a la alta gerencia sobre el avance del programa de seguridad de la información	13,33%	4,62%	3,08%	2,05%	7,69%	3,59 %
Evaluar la eficiencia y efectividad del modelo de seguridad de la información	13,85%	5,13%	4,10%	2,05%	6,15%	2,05 %
Dirigir y supervisar los programas de riesgos de seguridad de la información de la organización	13,33%	4,62%	5,13%	1,54%	7,18%	0,51 %
Creación de programas de gobierno y gestión en materia de seguridad de la información	14,87%	3,59%	2,05%	2,05%	6,67%	2,56 %
Establecer y revisar la arquitectura de seguridad de la información	11,79%	6,15%	2,05%	2,05%	7,18%	2,05 %
Interacción con las diferentes áreas de negocio	11,28%	4,10%	3,08%	2,05%	6,15%	4,10 %
Gestionar el programa de gestión de incidentes de seguridad de la información	11,79%	5,13%	4,10%	2,05%	6,15%	1,03 %
Supervisar procesos de cumplimiento regulatorio en tecnología de información	10,77%	3,59%	3,59%	2,56%	6,15%	2,05 %
Seguimiento de prácticas en materia de protección de la privacidad de la información personal	7,69%	5,64%	1,54%	1,03%	4,10%	3,08 %
Supervisar y gestionar los procesos de investigaciones forenses digitales	6,67%	3,59%	1,54%	1,54%	3,59%	1,03 %
Definir o diseñar escenarios/simulaciones/Playbooks en relación con ciberriesgos	4,62%	3,08%	1,54%	1,54%	3,59%	0,51 %
Definir programas de resiliencia digital	5,13%	3,08%	2,05%	1,03%	2,05%	0,51 %

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 8 muestra la distribución de los cargos en los distintos sectores de mayor representación, casos como el del sector educación que también hace mención que el área de seguridad depende directamente de las áreas de TI, y el sector salud que si



Gráfica 8. Sectores y roles

bien tiene director su segunda posición es ratificada la no existencia de un área para atender estos retos empresariales, muestra un poco la dinámica de madurez en los diferentes sectores. Los demás sectores a su ritmo van mostrando un área que tiene un director y que ejerce en propiedad en sus funciones.

Todos estos datos ratifican el crecimiento y aprendizajes que sigue teniendo el área de seguridad en las empresas, para la construcción de ecosistemas digitales confiables y por tanto posturas de seguridad acordes a la realidad y necesidad de las empresas. Este crecimiento es un soporte vital para la organización y para que paso a paso se siga interpretando a la seguridad como un instrumento que ayude al negocio. Directorios y Ejecutivos de la seguridad cada vez más tienen en su agenda y radar las amenazas cibernéticas (PwCb, 2023; NACD, 2023; Diligent Institute, 2023)

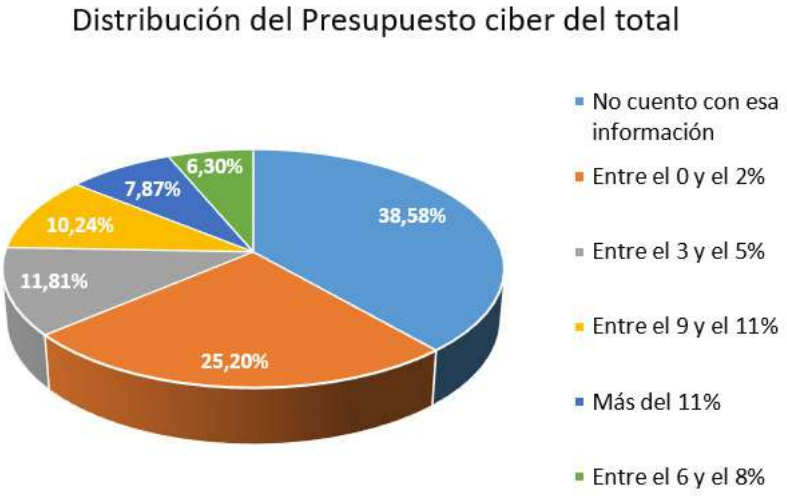
Mientras se siga avanzando en el desarrollo de la función de la seguridad en las organizaciones de Colombia como se viene dando, se seguirá mostrando unos aprendizajes que muy seguramente dejaran lecciones para optimizar y mejorar como igual se manifiesta en la tendencia mundial.

Presupuestos

Continúa la asignación de presupuestos para la ciberseguridad; en esta oportunidad el 73% manifiesta tener asignado un presupuesto de seguridad en la organización. Gráfica 9.

La gráfica 10 muestra el porcentaje que representa el presupuesto para la ciberseguridad del total del

Gráfica 9. Presupuesto de Seguridad

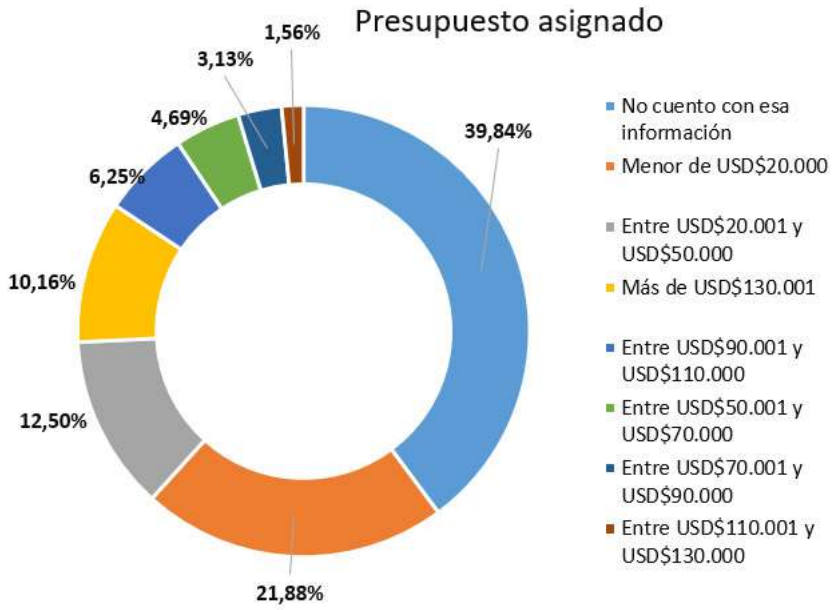


Gráfica 10. Porcentaje del presupuesto Global

presupuesto de la organización. Cerca del 64% de los encuestados lo conoce, mientras que el otro 38% 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 37%, mientras que el 22% están para los montos superiores al 5%. Entre el 0 y 2% representa un 25% mientras que entre 3 y el 5% representa el 12%, 8% es más del 11%, y entre el 9 y 11% es el 10%.

La gráfica 11 refleja los montos asignados en las organizaciones para la ciber-seguridad. Para este año cerca del 60% tiene un monto asignado para la seguridad; que aumenta, comparado con el año pasado cerca de un 13%, por su parte el 40% dice no conocer cuánto es el presupuesto asignado para la ciber-seguridad. Para este año cerca de un 22% dice que asigna menos de $US20.000 dólares americanos en sus presupuestos, seguido 13% que corresponde a la franja entre $US20.000 y $US-50.000; siguiente es el 10% que corresponde a los presupuestos por encima de $US130.000, el 6% asigna entre $US90.000 y $US-110.000, el 5% asigna entre $US-50.000 a $US70.000, 3% asigna entre $US70.000 a $US90.000 y 2% entre $US110.000 a $US-130.000 dólares americanos.

La gráfica 12 muestra la forma cómo se está invirtiendo el dinero en materia de ciberseguridad. El 48% invierte en la adquisición e implementación de tecnología de seguridad, el 39% invierte en renovación de licenciamiento, el 36% invierte en servicios de monitoreo y gestión, el 31% invierte en capacita-



Gráfica 11. Presupuesto de Seguridad

Gráfica 12. Inversión de Seguridad

ción del personal de seguridad y contratación de servicios de consultoría también tiene el 31%.

Consideraciones de los datos

Inversiones en ciberseguridad

Este año tiene consideraciones importantes que vale la pena resaltar, primero la forma en cómo se invierte el presupuesto por sectores de la industria y tamaño de las empresas; tenemos unas variedades de inversiones teniendo los siguientes elementos reflejados en la tabla 2.

Cuando se invierte más del 11% del presupuesto total de la organización sectores como el financiero y telecomunicaciones se resaltan más invirtiendo ambos en los ser-

Tabla 2. Inversiones de seguridad por sectores, presupuestos y montos

Distribución (Presupuesto - Franja) vs Sectores	Telecomunicaciones	Servicios Financieros y Banca	Salud	Gobierno / Sector público	Educación	Consultoría Especializada
Más del 11%						
Entre USD$50.001 y USD$70.000 Adquisición e implementación de tecnología de seguridad informática Renovación de licenciamiento y mantenimiento de hardware y software Servicios de monitoreo y gestión de seguridad con terceros				5,13% 5,88% 6,45%		
Entre USD$70.001 y USD$90.000 Adquisición e implementación de tecnología de seguridad informática Capacitación/Actualización del personal de seguridad de la información Renovación de licenciamiento y mantenimiento de hardware y software Servicios de monitoreo y gestión de seguridad con terceros		2,56% 4,35% 2,94% 3,23%				
Entre USD$90.001 y USD$110.000 Adquisición e implementación de tecnología de seguridad informática Renovación de licenciamiento y mantenimiento de hardware y software Servicios de monitoreo y gestión de seguridad con terceros						2,56% 2,94% 3,23%
Más de USD$130.001 Adquisición e implementación de tecnología de seguridad informática Capacitación/Actualización del personal de seguridad de la información	5,13% 4,35%	2,56% 4,35%				2,56% 4,35%

Contratación de servicios de asesoría/consultoría	4,55%	4,55%				
Renovación de licenciamiento y mantenimiento de hardware y software	5,88%	2,94%				
Servicios de monitoreo y gestión de seguridad con terceros	6,45%	3,23%				
Entre el 9 y el 11%						
Entre USD$110.001 y USD$130.000						
Renovación de licenciamiento y mantenimiento de hardware y software	2,94%					
Entre USD$20.001 y USD$50.000						
Adquisición e implementación de tecnología de seguridad informática						2,56%
Contratación de servicios de asesoría/consultoría						4,55%
Renovación de licenciamiento y mantenimiento de hardware y software						2,94%
Servicios de monitoreo y gestión de seguridad con terceros						3,23%
Entre USD$50.001 y USD$70.000						
Renovación de licenciamiento y mantenimiento de hardware y software						2,94%
Servicios de monitoreo y gestión de seguridad con terceros						3,23%
Entre USD$90.001 y USD$110.000						
Adquisición e implementación de tecnología de seguridad informática				2,56%		
Servicios de monitoreo y gestión de seguridad con terceros				3,23%		
Más de USD$130.001						
Adquisición e implementación de tecnología de seguridad informática					2,56%	
Capacitación/Actualización del personal de seguridad de la información					4,35%	
Contratación de servicios de asesoría/consultoría					4,55%	
Renovación de licenciamiento y mantenimiento de hardware y software					2,94%	
Servicios de monitoreo y gestión de seguridad con terceros					3,23%	
Menor de USD$20.000						
Adquisición e implementación de tecnología de seguridad informática						5,13%
Capacitación/Actualización del personal de seguridad de la información						8,70%
Contratación de servicios de asesoría/consultoría						4,55%
Renovación de licenciamiento y mantenimiento de hardware y software						2,94%
Servicios de monitoreo y gestión de seguridad con terceros						3,23%
Entre el 6 y el 8%						
Entre USD$20.001 y USD$50.000						
Adquisición e implementación de tecnología de seguridad informática	2,56%					5,13%
Capacitación/Actualización del personal de seguridad de la información	4,35%					
Contratación de servicios de asesoría/consultoría	4,55%					9,09%
Servicios de monitoreo y gestión de seguridad con terceros	3,23%					3,23%

Entre USD$70.001 y USD$90.000

Adquisición e implementación de tecnología de seguridad informática

Capacitación/Actualización del personal de seguridad de la información

Renovación de licenciamiento y mantenimiento de hardware y software

Servicios de monitoreo y gestión de seguridad con terceros

Entre USD$90.001 y USD$110.000

Adquisición e implementación de tecnología de seguridad informática

Contratación de servicios de asesoría/consultoría

Renovación de licenciamiento y mantenimiento de hardware y software

Servicios de monitoreo y gestión de seguridad con terceros

Menor de USD$20.000

Adquisición e implementación de tecnología de seguridad informática

Capacitación/Actualización del personal de seguridad de la información

Contratación de servicios de asesoría/consultoría

Renovación de licenciamiento y mantenimiento de hardware y software

Entre el 3 y el 5%

Entre USD$20.001 y USD$50.000

Adquisición e implementación de tecnología de seguridad informática

Capacitación/Actualización del personal de seguridad de la información

Contratación de servicios de asesoría/consultoría

Renovación de licenciamiento y mantenimiento de hardware y software

Servicios de monitoreo y gestión de seguridad con terceros

Entre USD$50.001 y USD$70.000

Renovación de licenciamiento y mantenimiento de hardware y software

Servicios de monitoreo y gestión de seguridad con terceros

Entre USD$70.001 y USD$90.000

Adquisición e implementación de tecnología de seguridad informática

Capacitación/Actualización del personal de seguridad de la información

Menor de USD$20.000

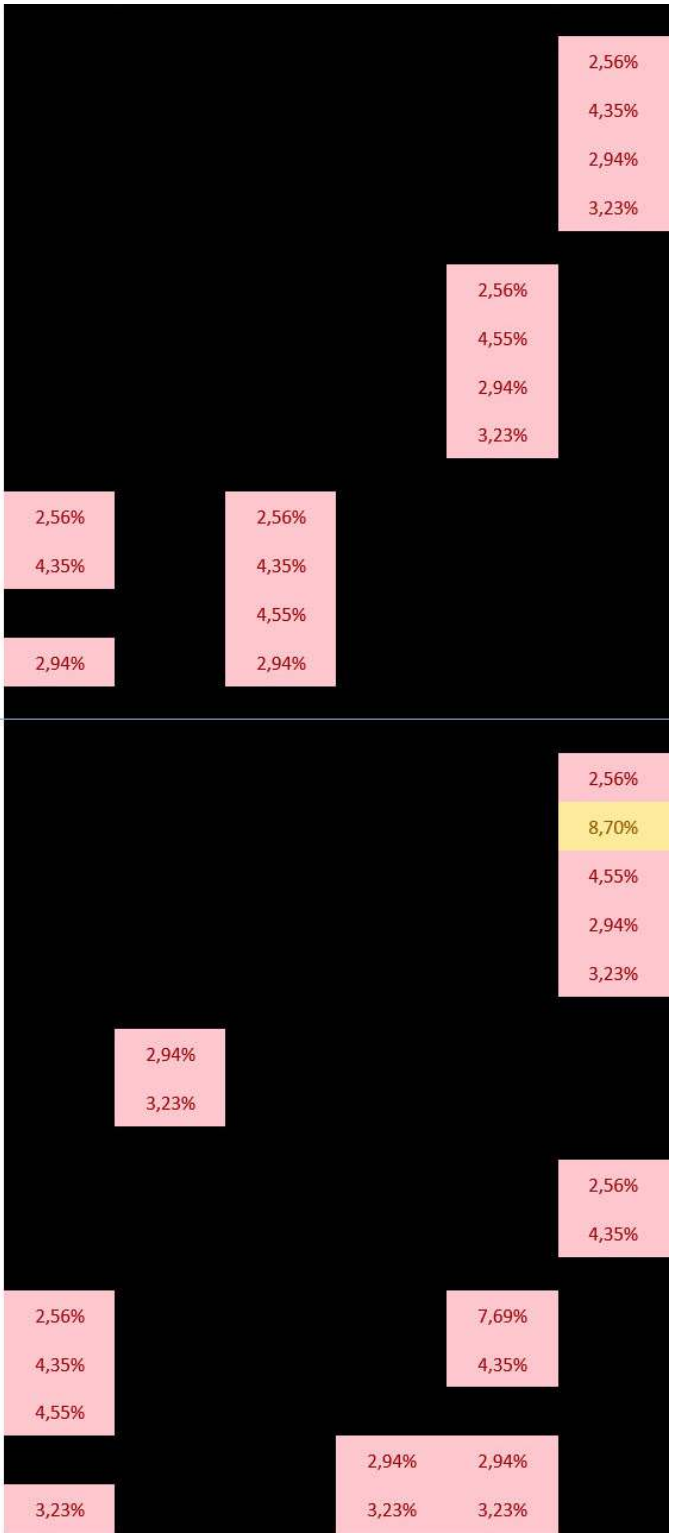
Adquisición e implementación de tecnología de seguridad informática

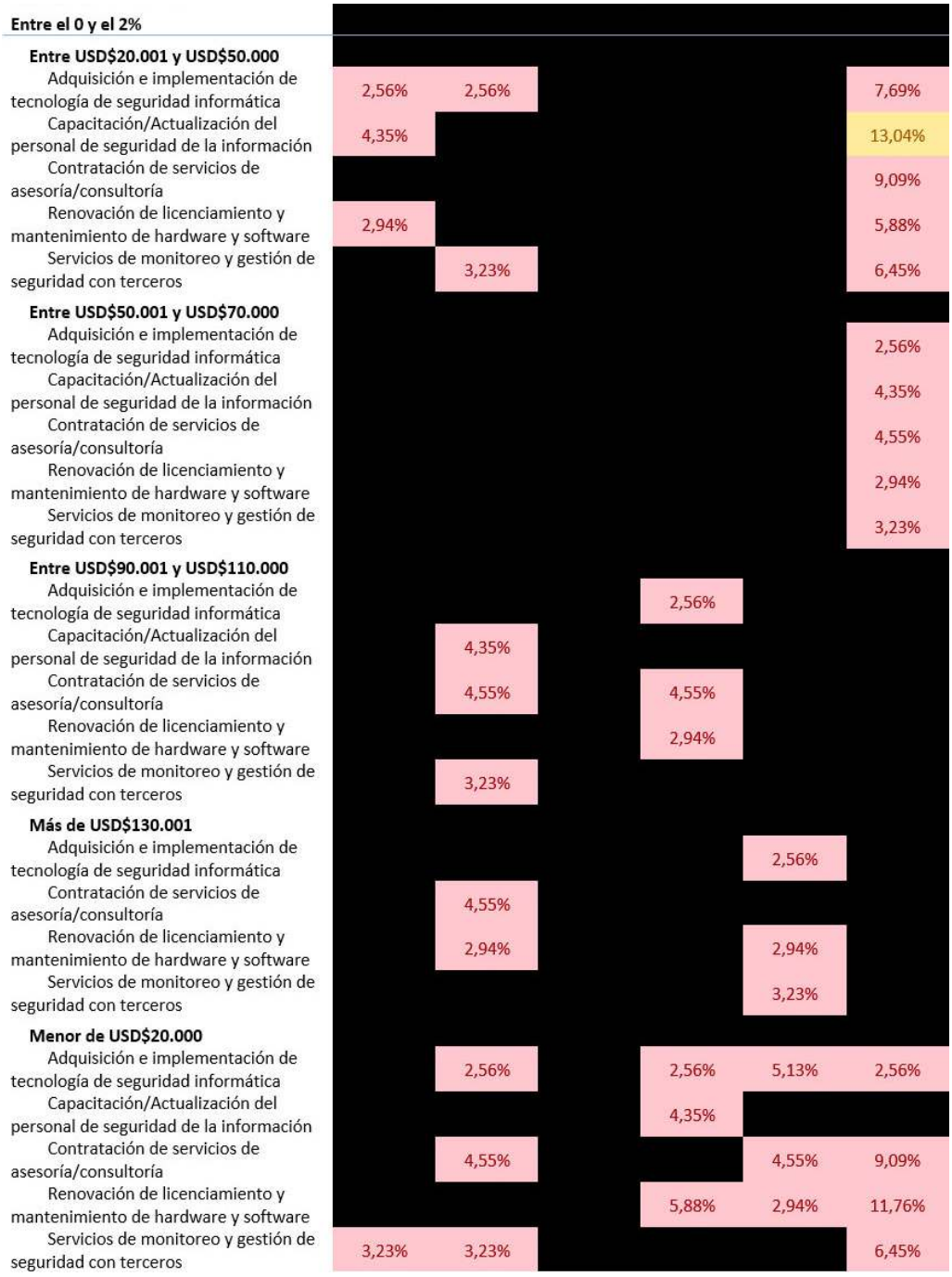
Capacitación/Actualización del personal de seguridad de la información

Contratación de servicios de asesoría/consultoría

Renovación de licenciamiento y mantenimiento de hardware y software

Servicios de monitoreo y gestión de seguridad con terceros





vicios de monitoreo y gestión de seguridad con terceros, sin embargo, el sector financiero solo invierte entre $US50.000 y $US70.000 dólares americanos mientras que el de las telecomunicaciones invierte más de $US 130.000 dólares americanos.

Cuando se invierte entre el 9 y el 11% del presupuesto global, el sector que resalta es el de la consultoría especializada que invierte menos de $US20.000 dólares en capacitación y/o actualización del personal de seguridad de la información.

Cuando se invierte entre el 6 y 8% del presupuesto global, el sector de la consultoría especializada nuevamente es el que invierte más en la franja de los $US20.000 a $US 50.000 dólares en servicios de contratación de servicios de asesoría/consultoría.

Entre el 3 y el 5 % del presupuesto global tiene un comportamiento similar, es el sector de consultoría especializada que invierte más en la franja de los $US20.000 a $US 50.000.

Por último, en la franja del 0 al 2% del presupuesto global es la capacitación del personal de seguridad el rubro de inversión más alto, que a su vez lo hace el sector de la consultoría especializada.

Hay consideraciones importantes en la tabla 3 que podría ser un resumen diciendo que cerca del 40% de los encuestados manifiestan no conocer el presupuesto que se asigna para la ciberseguridad, que, al explorar los datos, es indistinto del rol o cargo que desempeñe, esto es interesante porque sugiere que no son los CISOS o responsables de seguridad los que asignan o definen los presupuestos, sino

Tabla 3. Inversiones de seguridad por sectores

Sectores	No cuento con esa información	Menor de USD$20.000	Entre USD$20.001 y USD$50.000	Más de USD$130.001	Entre USD$50.001 y USD$70.000	Entre USD$90.001 y USD$110.000	Entre USD$70.001 y USD$90.000	Entre USD$110.001 y USD$130.000
Consultoría Especializada	8,00%	7,00%	8,00%	1,00%	2,00%	1,00%	3,00%	
Servicios Financieros y Banca	8,00%	1,00%	2,00%	2,00%	1,00%	2,00%	1,00%	
Telecomunicaciones	6,00%	5,00%	2,00%	3,00%				1,00%
Educación	8,00%	5,00%		2,00%		1,00%		
Gobierno / Sector público	7,00%	3,00%			2,00%	2,00%		
Salud	3,00%	1,00%		1,00%	1,00%			
Total, general	**40,00%**	**22,00%**	**12,00%**	**9,00%**	**6,00%**	**6,00%**	**4,00%**	**1,00%**

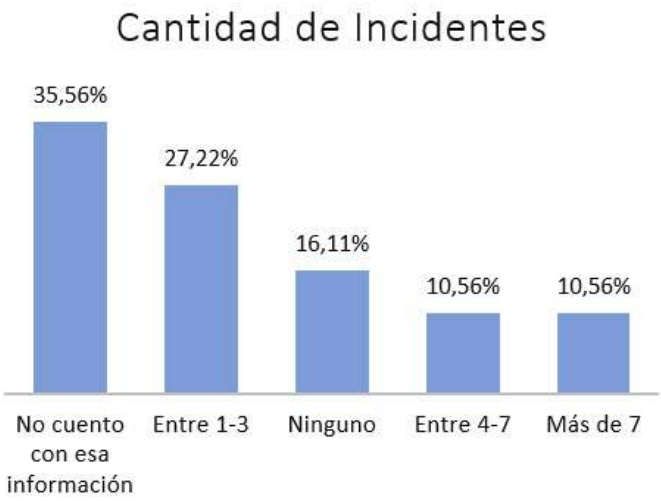
otras áreas en las mismas empresas. De los que indican conocerlo, el 22% advierte que sus presupuestos de seguridad están por debajo o igual a $US20.000 dólares, que puede ser un comportamiento normal frente a los vientos de contracción de mercados y posible recesión con la que comenzó el año 2023 (PwC, 2023; EY, 2023) y en esa misma línea el sector que más invierte en esa franja es el sector de la consultoría especializada. La segunda franja más usada en inversiones está entre $US20.000 y $US 50.000, que al igual que la anterior es el sector de la consultoría especializada, el que más se mueve en esta franja y le sigue la banda de inversión por encima de los $US 130.000 en el que el sector de las telecomunicaciones es el que se resalta.

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, 2023).

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

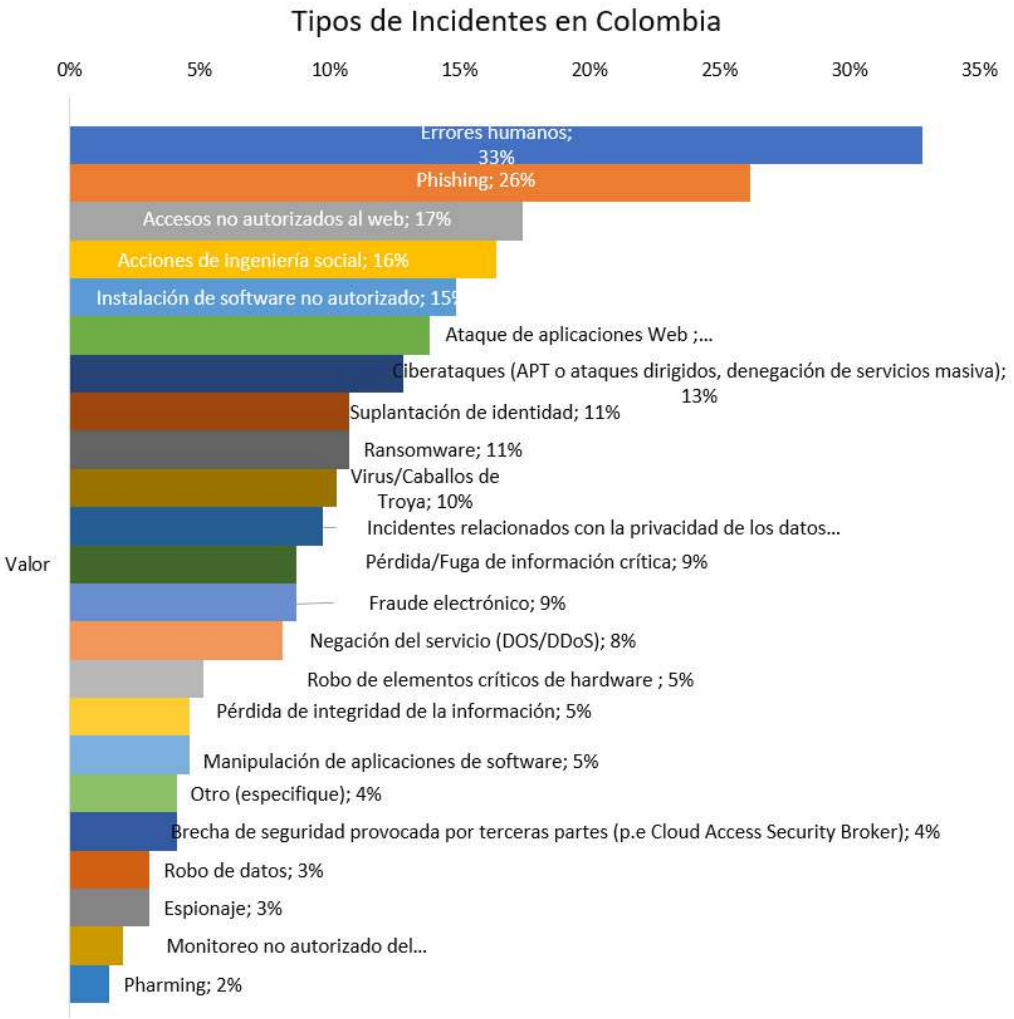
La gráfica 13 representa la cantidad de incidentes que para este



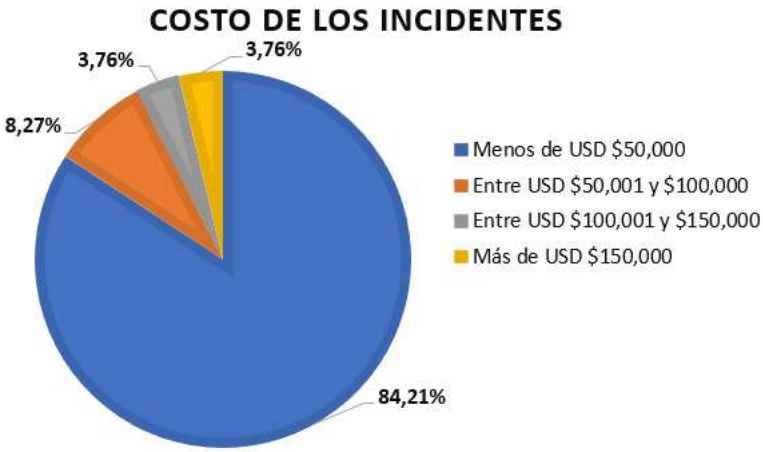
Gráfica 13. Cantidad de Incidentes

año los encuestados manifestaron que se presentaron. Para este año cerca del 48% de los encuestados manifiesta que ha estado en contacto con algún incidente de seguridad en su empresa, en comparación con el año inmediatamente anterior, donde el 56% lo ha manifestado. El 36% manifiesta no tener información al respecto de los incidentes en sus organizaciones, al revisar los detalles se encuentra que el 27% manifiesta haber experimentado entre 1 y 3 incidentes, tanto para los que expresan que han experimentado entre 4 y 7 incidentes, como los que han experimentado más de 7 incidentes el valor es cerno al 11%.

La gráfica 14 relaciona los tipos de incidentes que se presentaron en



Gráfica 14. Tipos de Incidentes de Seguridad



Gráfica 15. Costos de los Incidentes

las organizaciones, Errores humanos (33%), Phishing (26%) y accesos no autorizados al web (17%) 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 15 representa el costo promedio de los incidentes cibernéticos en las empresas colombianas, el 84% manifiesta que los costos estimados totales luego de sufrir un incidente están por debajo de los $US50.000 dólares americanos, entre $US50.000 y $US 100.000 solo el 8%, más de $US 150.000 el 4% y entre $US100.000 y $US150.000 dólares americanos el 4%

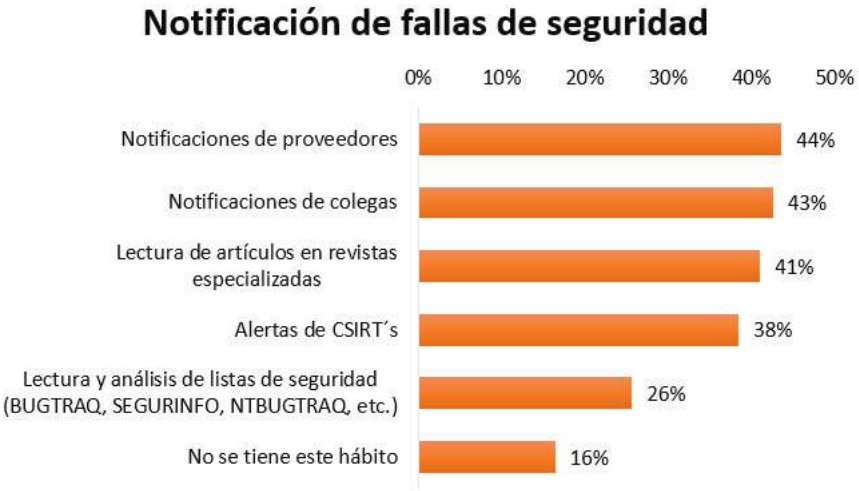
La gráfica 16, muestra ante quién se reportan los incidentes de seguridad. El 64% lo reporta directamente a los directivos de la organización, el 38% lo reporta al equipo de atención de incidentes (CSIRT), el 34% a las autoridades nacionales, el 32% a los asesores legales, el 17% a autoridades locales o regionales y solo el 5% manifiesta que no se denuncian. Para este año hubo más reporte hacia los directivos un aumento del 3% y una disminución del 4% de reportes ante los CSIRT, otro dato interesante es el aumento de más del 10% en incremento en reporte de incidentes a los asesores legales, y se mantiene en el 5% igual aquellos que no dicen nada o no notifican nada de sus incidentes.

La gráfica 17, muestra como los profesionales de ciberseguridad se mantienen informados sobre las vulnerabilidades y fallas de los sistemas. El 44% de los profesionales de seguridad se enteran a través de

Gráfica. 16 A quien se reportan los incidentes

sus proveedores en primera medida, seguido de la notificación de colegas con un 43%, la lectura de artículos especializados o revistas un 41% de las veces es usado para enterarse de las anomalías digitales, las alertas de un CSIRT el 38% de las veces el 26% de los casos es a través de listas de seguridad y solo el 16% no tiene ese hábito.

Comparado con el año pasado hay unos drásticos cambios; es la primera vez que los profesionales estrechan sus relaciones de confianza con sus aliados (proveedores) y son informados por estos sobre las anomalías digitales; el otro cambio drástico es el descenso vertiginoso de los CSIRT en este ejercicio.



Gráfica. 17 Notificación de incidentes

Contacto con autoridades	Porcentaje
No	44,03%
Si	55,97%

La tabla 4 se resalta que el 56% de las personas encuestadas si tienen contacto con las autoridades, mientras que el 44% no lo posee.

En cuanto la evidencia digital, los datos muestran que, 71% 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 28% está dividido en partes iguales para los que no saben y los que no son conscientes de la evidencia y su manejo como parte del proceso de incidentes.

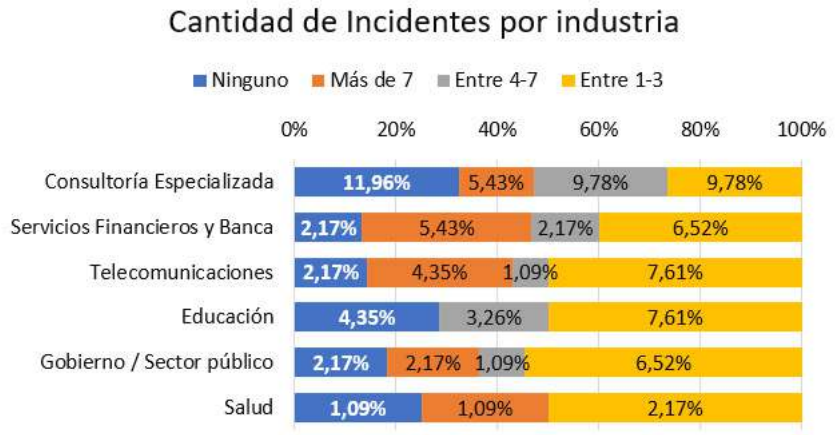
Al revisar qué tanto de esa consciencia se lleva a la práctica encontramos que el 46% manifiesta tener un procedimiento formal y establecido para la gestión de incidentes y un 54% no. Para este año se indago por la implementación de dicho procedimiento encontrando que solo el 65% de lo que lo tienen aprobado lo han implementado formalmente, los informales rondan el 17%, el 10% no lo han hecho y el 8% restante no sabe si eso se ha implementado.

Consideraciones de los datos

Frecuencias de los incidentes

Explorando la forma como experimentan en Colombia los diferentes sectores de la industria los distintos incidentes, la gráfica 18, muestra cómo los distintos sectores sufren las distintas franjas de incidentes.

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



Gráfica 18. Cantidad de Incidentes por sectores

mentan incidentes cibernéticos, tendencia que se confirma a través de reportes como (Verizon, 2023) (CyberEdge, 2023), (Cano & Almanza, 2021).

Llama la atención en el sector de la consultoría especializada, que su valor más alto esté relacionado con no manifestar incidentes, aspecto que puede tener dos lecturas, una pobre capacidad para gestionar y tratar incidentes (SecureWorks, 2023), o unas escalas inadecuadas en la clasificación y triage de los incidentes (CheckPoint, 2023), (Magnet, 2023).

Al revisar con detalle estos datos, la tabla 5, los muestra por sectores, tamaños de empresas y la cantidad de estos, de los cuales se puede decir.

Y en que invierten sus recursos financieros asignados de presupuesto a los desafíos que presenta la ciber-seguridad, la tabla 5, resalta la cantidad de incidentes que se presentan en los diferentes sectores de industria y adicional los relaciona por el tamaño de la empresa.

Al revisar la tabla, vemos el top 5 (Resaltado en rojo) que contiene lo siguiente son las empresas muy pequeñas del sector de la consultoría especializada las que manifiestan no tener incidentes, llama la atención que las empresas grandes (1001-5000) empleados del mismo sector manifiesten que no tienen incidentes, interesante ver que la proporción mayor de 4 incidentes hacia arriba en las empresas pequeñas sea en suma mucho

Tabla 5. Distribución de incidentes por sectores y tamaños

Sectores/Tamaños	Ninguno	Más de 7	Entre 4-7	Entre 1-3
Consultoría Especializada				
1 - 50 empleados	5,43%	3,26%	4,35%	2,17%
1001 - 5000 empleados	3,26%		1,09%	
201 - 500 empleados		1,09%		3,26%
501 - 1000 empleados			2,17%	2,17%
51 - 200 empleados	2,17%	1,09%	2,17%	1,09%
Mayor de 5001 empleados	1,09%			1,09%
Servicios Financieros y Banca				
1 - 50 empleados		1,09%		
1001 - 5000 empleados		1,09%		1,09%

201 - 500 empleados	1,09%	1,09%	1,09%	3,26%
501 - 1000 empleados	1,09%			
51 - 200 empleados			1,09%	1,09%
Mayor de 5001 empleados		2,17%		1,09%
Educación				
1001 - 5000 empleados			2,17%	2,17%
201 - 500 empleados	1,09%			1,09%
501 - 1000 empleados	1,09%			3,26%
51 - 200 empleados	1,09%			
Mayor de 5001 empleados	1,09%		1,09%	1,09%
Telecomunicaciones				
1 - 50 empleados	2,17%	2,17%		2,17%
1001 - 5000 empleados				2,17%
501 - 1000 empleados		1,09%	1,09%	1,09%
51 - 200 empleados		1,09%		1,09%
Mayor de 5001 empleados				1,09%
Gobierno / Sector público				
1001 - 5000 empleados		2,17%		2,17%
201 - 500 empleados				2,17%
501 - 1000 empleados	1,09%		1,09%	1,09%
51 - 200 empleados	1,09%			1,09%
Salud				
1001 - 5000 empleados		1,09%		1,09%
201 - 500 empleados	1,09%			
51 - 200 empleados				1,09%

mayor a las que dicen no tenerlos cerca del 8% en comparación con el 5%, el patrón de comportamiento en los sectores de la industria se mantiene donde es entre 1 a 3 incidentes es la constante y en las empresas entre 200 a 1000 de todos los sectores se manifiestan incidentes de toda naturaleza.

No todas las verticales empresariales en Colombia tiene los mismos tipos de incidentes; la tabla 6 muestra dos visiones. la primera vi-

sión resalta el top 3 de tipos de incidentes por sector, la segunda parte resalta el top 1 en materia del 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 ata-

Tabla 6. Tipos de incidentes x industria

	Visual por Sectores Empresariales (Top 3) lectura vertical						Visual por tipo de Incidentes (Top 1) lectura horizontal					
Tipos de Incidentes	**Telecomunicaciones**	**Servicios Financieros y Banca**	**Salud**	**Gobierno / Sector público**	**Educación**	**Consultoría Especializada**	**Telecomunicaciones**	**Servicios Financieros y Banca**	**Salud**	**Gobierno / Sector público**	**Educación**	**Consultoría Especializada**
Errores humanos	10%	13%	25%	17%	14%	17%	8%	14%	6%	11%	16%	34%
Phishing	8%	15%	13%	12%	10%	9%	8%	22%	4%	10%	14%	24%
Accesos no autorizados al web	13%	4%	6%	7%	13%	6%	18%	9%	3%	9%	26%	21%
Instalación de software no autorizado	6%	3%	13%	7%	7%	8%	10%	7%	7%	10%	17%	34%
Acciones de ingeniería social	6%	7%	13%	5%	6%	6%	9%	16%	6%	6%	13%	25%
Ataque de aplicaciones Web	8%	4%		7%	11%	5%	15%	11%		11%	30%	22%
Ciberataques (APT o ataques dirigidos, denegación de servicios masiva)	10%	3%		5%	3%	6%	20%	8%		8%	8%	32%
Suplantación de identidad	2%	8%	6%	2%	6%	4%	5%	29%	5%	5%	19%	24%
Virus/Caballos de Troya	2%	3%		7%	8%	5%	5%	10%		15%	30%	30%
Ransomware	6%	4%		5%	1%	6%	14%	14%		10%	5%	33%
Incidentes relacionados con la privacidad de los datos personales	2%	4%	6%	2%	7%	3%	5%	16%	5%	5%	26%	21%
Pérdida/Fuga de información crítica	6%	6%	6%	7%		3%	18%	24%	6%	18%		24%
Negación del servicio (DOS/DDoS)	6%	3%		2%	7%	3%	19%	13%		6%	31%	25%
Fraude electrónico	2%	6%		5%	1%	3%	6%	24%		12%	6%	24%
Robo de elementos críticos de hardware	2%	1%	6%	2%		4%	10%	10%	10%	10%		50%
Pérdida de integridad de la información		3%		2%	1%	4%		22%		11%	11%	56%
Manipulación de aplicaciones de software		4%		2%		2%		33%		11%		22%
Brecha de seguridad provocada por terceras partes (p.e Cloud Access Security Broker)	4%	3%			1%	1%	25%	25%			13%	13%
Espionaje	2%	1%	6%		1%	2%	17%	17%	17%		17%	33%
Robo de datos	2%	1%			1%	2%	17%	17%			17%	33%
Monitoreo no autorizado del tráfico		1%				2%		25%				75%
Pharming		3%			1%			67%			33%	

ques 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.
5. Al revisar sector por sector encontramos particularidades (Tabla 6 primera parte). Para el caso del sector de telecomunicaciones el incidente top 1, es acceso no autorizado al web, en el sector financiero es el Phishing, en los sectores de salud, gobierno, educación y consultoría especializada es el error humano el incidente número 1.
6. Al revisar la parte 2 de la tabla que está categorizada por la presencia del tipo de incidentes y su distribución en los distintos sectores, se encuentran cosas interesantes. En el sector salud, encontramos como los ataques de denegación de servicios y todas las afectaciones a las aplicaciones web y accesos no autorizados tiene fuerte presencia. El sector de la consultoría especializada menciona que todos los incidentes tienen presencia en su sector. El pharming, suplantación de identidad fraude electrónico y fuga de información incidentes que marcan presencia importante. El sector de telecomunicaciones muestra un interesante comportamiento pues son las brechas de seguridad de terceros particularmente lo que está asociado al cloud computing lo que se resalta como incidente importante.

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(a), 2023; FS-ISAC, 2023).

Para el caso del Phishing es uno de los fenómenos más estudiados y analizados por distintos especialistas de la industria, el reporte de Verizon (Verizon, 2023; FBI, 2023) manifiesta que el 74% de las brechas de seguridad donde se involucran datos, también tienen involucradas personas, en ese sentido la firma Knowbe4 resalta de los estudios de pruebas de phishing realizadas que más del 33% de las personas no entrenada no pasaran las pruebas de phishing (Knowbe4, 2023; Proofpoint(c), 2023). La fundación de investigación en seguridad informática revela que de 1466 dominios analizados entre abril y mayo del 2023 el 26% fueron phishing (Finsin, 2023). Barracuda networks en su informe resalta que el 50% de las empresas fueron víctimas de Spear Phishing, de la misma manera manifiesta que una empresa normal recibe 5 emails de Spear phishing muy personalizados por día

(Barracuda, 2023), (Barracuda(b), 2023). Zscaler en su reporte resalta que el incremento de los ataques de phishing desde el 2021 al 2022 creció cerca de un 47% (Zscaler, 2023). En el compendio de análisis de industria se resalta que los ataques de phishing que buscan credenciales crecen un 527% (Cofense, 2023).

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(d), 2023).

Para el caso de las fallas de aplicaciones y dada las tendencias globales o megatrends del Web 3.0 como una realidad innegable donde las APIs y las aplicaciones son la norma (HCLTech, 2023), lo cual también está aunado a la presencia del cloud computing como un apalancador de ambientes digitales en donde se expanden o extienden los riesgos de manera natural (ArticWolf, 2023). El 75% de los responsables de seguridad están algo preocupados por la cantidad de vulnerabilidades y amenazas por las aplicaciones en ambientes productivos (Dynatrace, 2022). El 32% de las aplicaciones han tenido ataques de DDos durante el 2022 en su último cuarto (Indusface, 2022). Solo el 2% confía en las estrategias de defensas para proteger sus aplicaciones y sobre todo en la nube (Opswat, 2023).

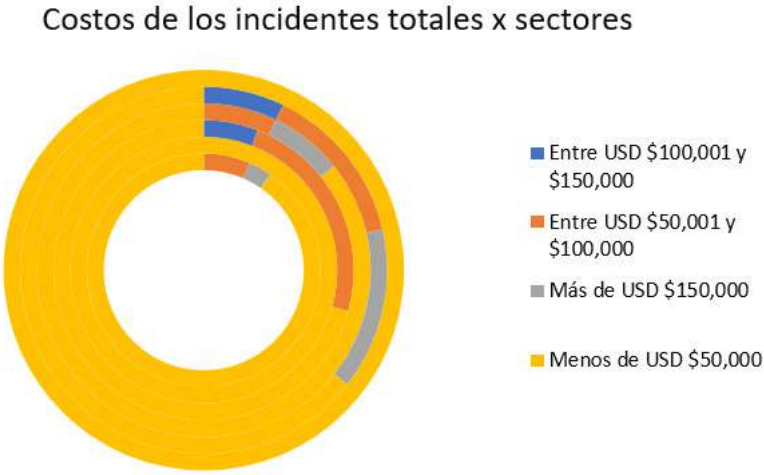
Muchos de los eventos del año 2022 (PwCc, 2022) han sido precedente para que el 2023 sea un año donde se tenga mayor atención a la presencia de los eventos cibernéticos que marcan a las organizaciones no solo a nivel internacional, sino nacional también.

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 19, representa los costos de los incidentes por sectores de industria, cada anillo es un sector de industria y en él se muestra la distribución de las franjas de valores económicos de los mismos.

Del cual se puede extraer lo siguiente:

1. Más del 90% de los costos asociados a un incidente cibernético están por debajo de los $US 50.000 dólares, una cifra no menor para el valor del peso colombiano, en una aproximado cercano en pesos de 200.000 millones de pesos colombianos haciendo el cálculo de una tasa representativa de 4.000 pesos.
2. A excepción del sector salud y educación, todos los demás sec-

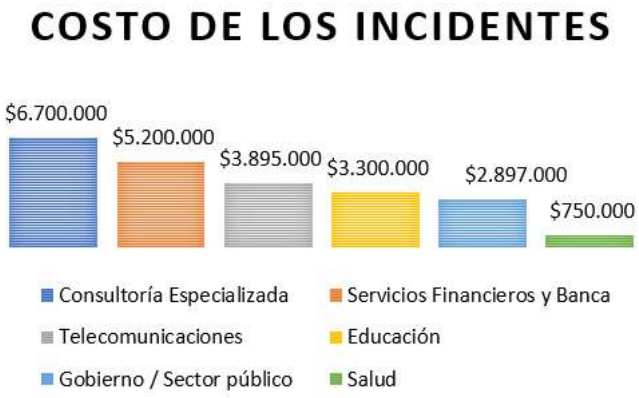


Gráfica 19. Costos de incidentes por industria

tores representativos (telecomunicaciones, financiero, gobierno y consultoría) tienen incidentes con costos en las demás bandas indagadas. Casos como el sector de telecomunicaciones donde tiene incidentes en todas las bandas.

3. Se resalta qué en comparación con los demás sectores, el sector financiero tiene menos incidentes de montos mayores de $US 50.000 dólares, comparado con los demás sectores representativos, mientras que el sector financiero solo tiene dos incidentes por encima de los $50.000 dólares, el sector de telecomunicaciones y gobierno tienen 5, y la consultoría especializada tiene 3.

Para este año analizando los datos recolectados, se ha determinado el



Gráfica 20. Costos de los incidentes x sectores de industria

costo total aproximado de los incidentes por sector de la industria, el cual se refleja en la gráfica 20. En ella se resalta que un promedio aproximado de los 22 tipos de incidentes que mide la encuesta le costó al sector de la consultoría especializada en dólares americanos cerca de $US 6.7 millones, al sector financiero le costó un estimado de 5.2 millones, al sector de las telecomunicaciones 3,9 millones de dólares al sector de educación 3,3 millones, al sector del gobierno sus costos pudieron llegar a cerca de 2,9 millones y por último al sector salud cerca de 750 mil dólares americanos.

La gráfica 21, 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 3,650.000, phishing seguido con 2.848.000 mil dólares, acceso no autorizado al web $US-1.850 millones.

Al revisar o decepcionar estos costos por sectores de la industria en los tipos de incidentes analizados, también se encuentran variaciones importantes, reflejadas en la tabla 7.

Gráfica 21. Costos totales por tipo de incidente

Tabla 7. Costos x tipo de incidentes en los sectores empresariales

Tipos de Incidentes	Telecomunicaciones	Servicios Financieros y Banca	Salud	Gobierno / Sector público	Educación	Consultoría Especializada
Errores humanos	$ 350.000	$ 600.000	$ 200.000	$ 450.000	$ 450.000	$ 1.100.000
Phishing	$ 349.000	$ 600.000	$ 50.000	$ 300.000	$ 300.000	$ 550.000
Accesos no autorizados al web	$ 350.000	$ 300.000	$ 50.000	$ 150.000	$ 400.000	$ 350.000
Acciones de ingeniería social	$ 150.000	$ 350.000	$ 100.000	$ 150.000	$ 200.000	$ 500.000
Ataque de aplicaciones Web	$ 350.000	$ 150.000	$ -	$ 200.000	$ 350.000	$ 350.000
Instalación de software no autorizado	$ 200.000	$ 150.000	$ 100.000	$ 200.000	$ 250.000	$ 500.000
Ciberataques (APT o ataques dirigidos, denegación de servicios	$ 399.000	$ 250.000	$ -	$ 199.000	$ 100.000	$ 450.000
Ransomware	$ 299.000	$ 300.000	$ -	$ 249.000	$ 50.000	$ 350.000
Suplantación de identidad	$ 150.000	$ 350.000	$ 50.000	$ 100.000	$ 200.000	$ 250.000
Pérdida/Fuga de información crítica	$ 300.000	$ 250.000	$ 50.000	$ 150.000	$ -	$ 300.000
Virus/Caballos de Troya	$ 50.000	$ 150.000	$ -	$ 249.000	$ 250.000	$ 300.000
Negación del servicio (DOS/DDoS)	$ 299.000	$ 100.000	$ -	$ 50.000	$ 250.000	$ 200.000
Incidentes relacionados con la privacidad de los datos personales	$ 50.000	$ 150.000	$ 50.000	$ 100.000	$ 250.000	$ 200.000
Fraude electrónico	$ 50.000	$ 250.000	$ -	$ 200.000	$ 50.000	$ 200.000
Robo de elementos críticos de	$ 149.000	$ 100.000	$ 50.000	$ 50.000	$ -	$ 250.000
Pérdida de integridad de la	$ -	$ 250.000	$ -	$ 50.000	$ -	$ 250.000
Brecha de seguridad provocada por terceras partes (p.e Cloud Access	$ 150.000	$ 150.000	$ -	$ -	$ 50.000	$ 100.000
Espionaje	$ 150.000	$ 100.000	$ 50.000	$ -	$ 50.000	$ 100.000
Robo de datos	$ 100.000	$ 100.000	$ -	$ -	$ 50.000	$ 150.000
Manipulación de aplicaciones de	$ -	$ 200.000	$ -	$ 50.000	$ -	$ 100.000
Pharming	$ -	$ 250.000	$ -	$ -	$ 50.000	$ -
Monitoreo no autorizado del tráfico	$ -	$ 100.000	$ -	$ -	$ -	$ 150.000

De la tabla anterior se pueden determinar los siguientes puntos:

1. Al sector de la consultoría especializada es al que más le cuesta los errores humanos, en relación con los demás sectores.
2. En el sector de las telecomunicaciones los ciberataques avanzados son los que más cuestan.
3. En el sector financiero se puede observar que son los clientes a quienes van mayormente dirigidos los ataques, phishing, ingeniería social y la identidad están dentro de los incidentes con mayores costos.
4. En el sector de gobierno el ransomware y el malware tradicional hace parte de la batería de incidentes que más se presentan.
5. En el sector de la educación el acceso no autorizado a sus aplicaciones web es el segundo incidente con mayores costos.

En el gráfico 23, 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 $200.000 dólares hasta $US 2.700.000 millones de dólares el costo en el que más oscila los incidentes 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 8), 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 36% más de probabilidad de que un incidente se presente, y exactamente un 24% 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 4 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

Distribución de los incidentes cibernéticos

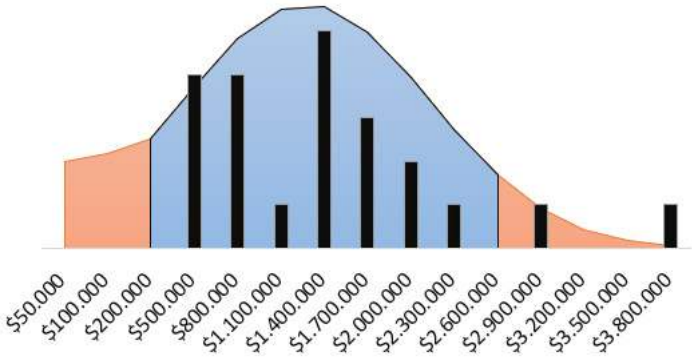


Tabla 8. Costos de los incidentes vs Inversiones vs Cantidad de Incidentes

Etiquetas de fila	Menos de USD $50,000	Entre USD $50,001 y $100,000	Entre USD $100,001 y $150,000	Más de USD $150,000
Entre el 0 y el 2%	**36,00%**	**2,00%**	**0,00%**	**0,00%**
Entre 1-3	24,00%	2,00%		
Entre 4-7	4,00%			
Más de 7	8,00%			
Entre el 3 y el 5%	**14,00%**	**2,00%**	**4,00%**	
Entre 1-3	8,00%	2,00%	4,00%	
Entre 4-7	2,00%			
Más de 7	4,00%			
Más del 11%	**6,00%**	**4,00%**	**4,00%**	**2,00%**
Entre 1-3			2,00%	2,00%
Entre 4-7	4,00%			
Más de 7	2,00%	4,00%	2,00%	
Entre el 9 y el 11%	**10,00%**	**2,00%**		**2,00%**
Entre 1-3	10,00%			
Entre 4-7				2,00%
Más de 7		2,00%		
Entre el 6 y el 8%	**8,00%**	**4,00%**		
Entre 1-3	2,00%			
Entre 4-7	2,00%	4,00%		
Más de 7	4,00%			
Total general	**74,00%**	**14,00%**	**8,00%**	**4,00%**

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 de aplicaciones se ven como un vector emergente y particularmente en el mundo de las API (Aplication Program Interfaces) el cual ha incrementado de 2021 a 2022 cerca de un 23% (Vmware, 2022; Imperva, 2022).

Los ataques de phishing, ingeniería social, en especial los de tipo Business Email Compromise es de los que más se usa (Secureworks, 2023), (Kroll, 2022), (Ironscale, 2022).

Los costos de los ciberataques crecen año tras año (Verizon, 2023; Sophos, 2023). 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 (Cybereason, 2022),

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 22, muestra la distribución del uso de las herramientas de seguridad, en ella se evidencia que

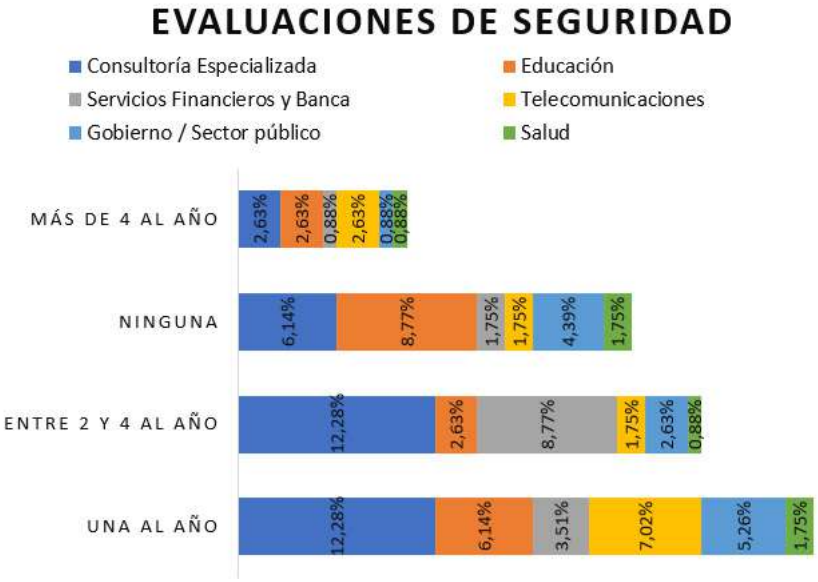
Gráfica 22: Herramientas de seguridad

el cifrado de datos, las VPNs, los sistemas de contraseñas, las soluciones antimalware y las firmas digitales, corresponden al top 5 de herramientas más usadas en las empresas de todos los tamaños y sectores de la industria nacional.

La gráfica 23 muestra el comportamiento de como las organizaciones en Colombia por industria realizan una evaluación de la postura de seguridad general. Se mantiene la tendencia con respecto al año inmediatamente anterior 36% dice que lo hace al menos una vez, entre 2 y 4 el 29% una disminución moderada con relación al año anterior un aumento importante en 6 puntos porcentuales que no se hizo siendo este año del 25% y un 11% lo hace más de 4 veces al año. Al revisar por sectores se observa como el sector de la consultoría especializada ocupa el primer lugar con excepción de ninguna donde es el sector de la educación el que tiene el primer puesto en no realizar este tipo de prácticas. El sector financiero definitivamente se consolida en manifestar que es de 2 a 4 evaluaciones de seguridad la que hace en un periodo de un año, llama la atención que el sector gobierno la segunda posición es el de ninguna que no es mucha la diferencia entre las dos posiciones.

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 9, la cual contiene la



Gráfica 23: Evaluaciones de Seguridad

Tabla 9 Herramientas usadas por sectores de la industria.

Mecanismos de seguridad	Consultoría Especializada	Educación	Gobierno / Sector público	Salud	Servicios Financieros y Banca	Telecomunicaciones
Cifrado de datos	39%	14%	7%	6%	19%	10%
VPN/IPSec	29%	14%	7%	6%	24%	7%
Sistemas de Contraseñas	30%	16%	11%	5%	12%	12%
Firmas digitales/certificados digi	32%	11%	11%	6%	20%	5%
Soluciones Anti-Malware	39%	9%	7%	3%	17%	9%
Web Application Firewalls (WAF	30%	11%	10%	3%	17%	7%
Firewalls tradicionales (Hardwar	33%	17%	9%	7%	12%	7%
Biométricos (huella digital, iris, e	27%	14%	9%	4%	20%	7%
Firewalls de nueva generación	26%	9%	9%	8%	22%	4%
Entrenamiento/Actualización de	41%	7%	1%	4%	18%	8%
Firewalls de Bases de Datos (DAF	24%	16%	3%	7%	22%	11%
IDS/IPS de nueva generación	33%	3%	9%	5%	24%	7%
Servicio de SOC	28%	7%	4%	0%	28%	8%
Soluciones de seguridad EDR (En	36%	4%	6%	5%	21%	5%
SIEM (Security Information Even	27%	3%	9%	0%	32%	5%
Herramientas Anti–DDoS	31%	7%	7%	3%	26%	6%
Sistemas de detección y/o preve	27%	6%	6%	6%	24%	6%
Proxies/Proxies inversos	39%	7%	3%	3%	16%	3%
Enfoque de seguridad Zero Trust	29%	4%	3%	3%	26%	6%
Ciberseguros	28%	3%	1%	7%	24%	14%
Cooperación/Intercambio de inf	30%	6%	0%	7%	22%	7%
Servicios de inteligencia de ame	29%	4%	1%	0%	25%	4%
ADS (Anomaly detection system	38%	4%	3%	5%	19%	5%
Soluciones de Seguridad con IA	41%	3%	1%	6%	12%	6%
Soluciones basadas en inteligen	35%	3%	3%	0%	18%	0%
Tercerización de la seguridad inf	38%	7%	1%	13%	13%	0%
Herramientas de validación de c	38%	1%	0%	8%	23%	0%
Soluciones de monitoreo de red	25%	1%	0%	0%	42%	8%
Otro (especifique)	38%	3%	4%	0%	0%	0%
Smart Cards	33%	1%	0%	0%	33%	0%

distribución por sectores de industria de los mecanismos de seguridad.

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

1. La sumatoria global muestra al cifrado de datos como el mecanismo número 1 de todos.
2. En el sector de la consultoría se ve al entrenamiento de los profesionales de seguridad, el uso de la IA y las soluciones Antimalware como los mecanismos tendencia en dicho sector.
3. En el sector de la educación y gobierno usan los mecanismos tradicionales como firewalls de redes y de bases de datos, así como los sistemas de contraseñas y firmas digitales como las herramientas más usadas.
4. En el sector salud la tercerización, herramientas de validación de requisitos regulatorios internacionales y los firewalls de nueva generación son observados como mecanismos a ser usados.
5. El sector financiero usa con frecuencia monitoreo de redes sociales, Smart cards y los Siem como herramientas útiles para manejar su seguridad
6. El sector de telecomunicaciones es un sector que usa los Ciberseguros, los sistemas de contraseñas y los firewalls de bases de datos.

En el estudio de IBM (IBM, 2023), se resalta que las empresas están tendiendo a usar herramientas de automatización para la seguridad, tales como herramientas de inteligencia artificial y máquinas de aprendizaje, movimiento que también se ve como tendencia de Colombia.

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

En relación con la protección de estaciones de trabajo el mismo informe resalta que las soluciones *antimalware*, cifrado de discos, antivirus avanzados basados en inteligencia artificial también están considerados.

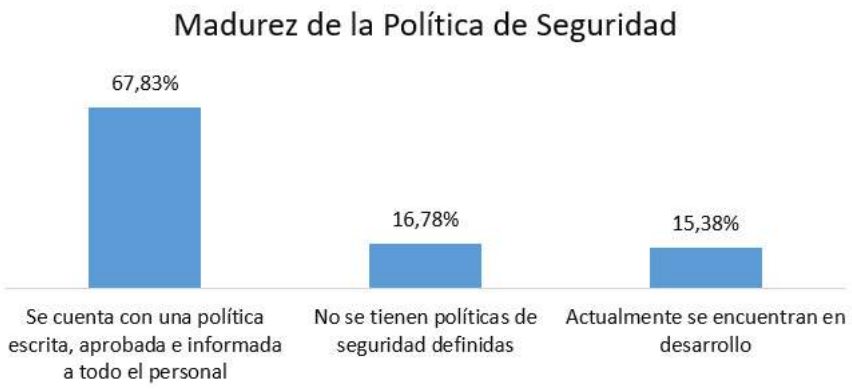
En cuanto a la protección de la capa de aplicaciones, los *Firewalls Web*, de bases de datos la protección de APIs son los controles que más se están usando y se tiene proyectado utilizar.

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 (Marsh, 2022).

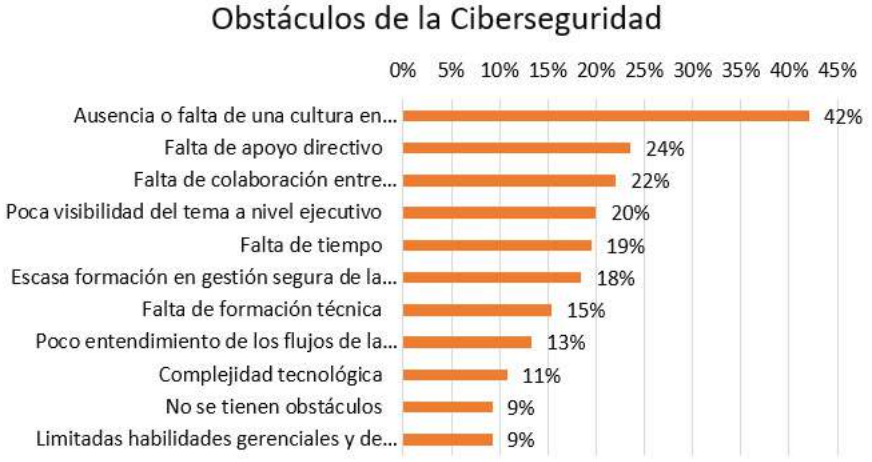
Políticas

La gráfica 24, refleja el estado de las políticas de seguridad en las organizaciones colombianas, el 68% de los encuestados manifiesta que tienen formalizada sus políticas de seguridad disminución de 4 puntos porcentuales frente al año 2022, el 15% actualmente en desarrollo y con un aumento del 9% frente al año anterior, el 16% señala no tener políticas de seguridad de la información.

La gráfica 25, 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 42%, la falta de apoyo directivo 24% y la falta de colaboración entre áreas 22% son los tres primeros lugares, cambios importantes para este año en los puestos 2 y 3 con relación al año anterior.



Gráfica: 24 Estado de las Políticas

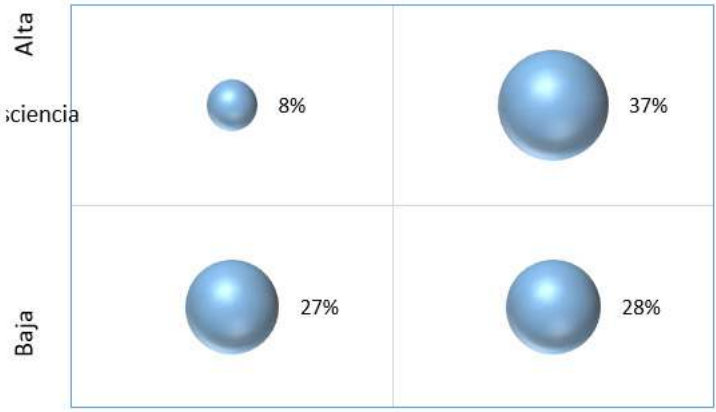


Gráfica 25 Obstáculos de la seguridad

La gráfica 26 refleja el nivel de consciencia y competencia de los directivos en materia de seguridad, encontrando que, la alta dirección con un 37% toma decisiones en materia de ciberseguridad, 28% atiende las recomendaciones de sus profesionales, 27% no participa en la toma de decisiones y no se involucra, y el 8% delega y espera informa de avances.

La gestión de riesgos de seguridad es un elemento esencial, en esa línea el 75% de los encuestados tiene un proceso de gestión de riesgos y solo 25% no lo posee.

En la gráfica 27, se resalta cada cuanto son ejecutados dichos ejercicios, el 56% manifiesta que al menos la ejecuta 1 vez al año, el 20% más de dos y solo dos el 24%. Es-



Gráfica 26: Consciencia de los directivos

Gráfica 27 Ejecución de Evaluaciones de riesgo

tos 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 realizada la gestión de riesgos. El principal motivo que resaltan los participantes está relacionado con no tener un proceso formal de gestión de riesgos (31%), disminución con relación al año anterior en 6 puntos porcentuales, seguido por un lado del desconocimiento del tema 23% y que ya está incluido en el proceso de gestión de riesgo empresarial 23%, la falta de presupuesto 11% y por último el no tener asociados riesgos con el tratamiento de la información 11%.

La tabla 10 muestra las metodologías de gestión de riesgos usadas por los participantes del estudio. En primer lugar, está ISO 27005 como la más usada con el 27%, seguido de ISO 31000 25%, 14% menciona no tener una metodología.

La Gráfica 28 muestra la forma en como las organizaciones hacen las asociaciones entre incidentes de seguridad y el riesgo. El 57% asocia los incidentes de seguridad con riesgos de ciberseguridad, el 48% los asocia con riesgos operacionales, el 36% los asocia con riesgos reputacionales, el 35% con riesgos legales, el 32% con riegos económicos, el 26% los asocia a riesgos transversales.

La tabla 11 muestra la distribución del uso de los distintos marcos de trabajo (*frameworks*) aplicados en las organizaciones colombianas: ISO/IEC 27001, NIST, ITIL y COBIT son los más usados.

Tabla 10. Metodologías para la gestión de riesgos

Metodologías	%
ISO 27005	27%
ISO 31000	25%
No se cuenta con metodología	14%
Magerit	9%
SARO	9%
GRC (Governance, Risk & Compliance)	8%
ERM(Enterprise Risk Management)	5%
Octave	4%
AS/NZ 4360	1%

Gráfica 28: Tipos de Riesgos

Tabla 11

ISO 27001	52%
Guías del NIST	22%
ITIL	18%
COBIT	13%
Ninguna	9%
PCI-DSS	9%
Guías de la ENISA	5%
ISM3 - Information Security Management Maturity Model	2%

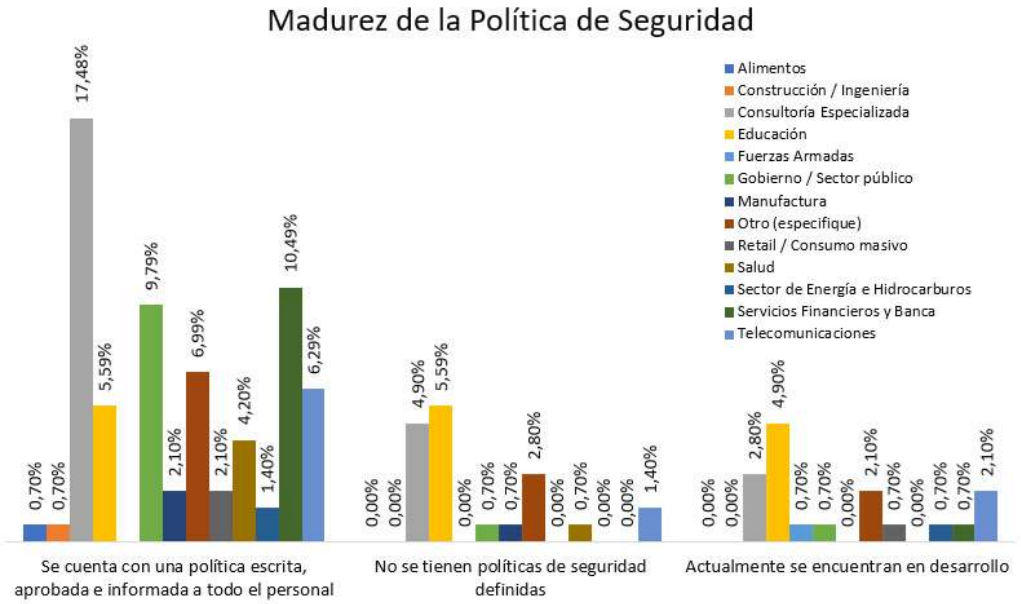
En cuanto a las regulaciones que las organizaciones deben cumplir, el caso colombiano menciona que, el 48% de los participantes manifiesta que sí existen regulaciones que son aplicables a sus modelos de negocio, el 38% considera que no está sujeto a cumplir ningún marco regulatorio o normativos, el 7% debe cumplir con marcos regulatorios internacionales y solo el 7% menciona a otros elementos de regulación.

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 (Accenture, 2023).

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 29, 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. El sector de la consultoría especializada manifiesta con un 17,5% tener aprobada una política, el sector de educación es el sector con mayor valor 5,59% comparado con los otros sectores en no tener una política, el sector de la educación en términos de comparaciones con los demás sectores es el que tiene el valor más alto 4,90% en manifestar que está en desarrollo su política de seguridad, dicho de otra manera, el sector de la educación reconoce que tiene una deficiencia al no tener una política de seguridad formalizada, sin

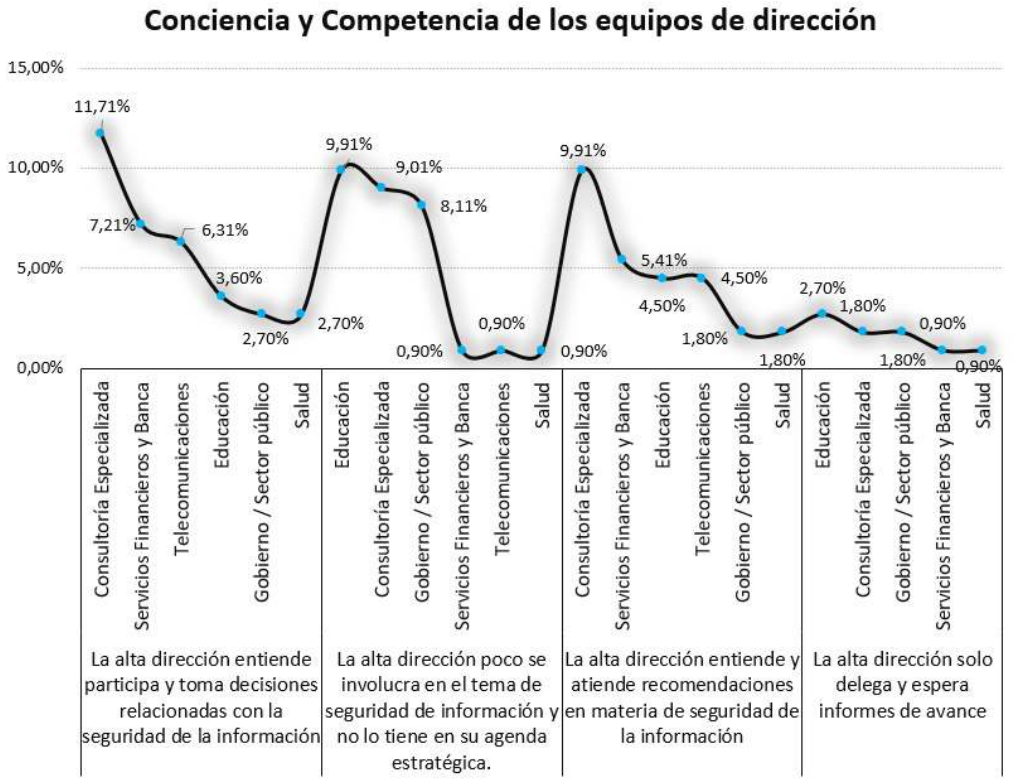


Gráfica 29. Madurez de la política de seguridad por sectores de industria

embargo, está hoy haciendo esfuerzos por desarrollarla y disminuir la brecha de gestión, dato no menor, dado que junto con el sector salud, son los sectores más apetecidos por los adversarios digitales como lo manifiestan reportes de industria (Verizon, 2023), (IBMb, 2023). Otro dato importante e interesante de análisis es que el sector financiero manifiesta no tiene en esta muestra de datos empresas que no tengan política de seguridad, o la tiene muy formalizada, o la está desarrollando.

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, 2023), 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 están centradas en que sus directivos tengan un contacto directo con la ciberseguridad (NACD, 2023), 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



Gráfica 30. Juntas directivas x sectores

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 se tiene la gráfica 30.

Las juntas directivas que se involucran y toman decisiones en el mundo de la ciberseguridad, primeramente, están en el sector de la consultoría especializada y el sector financiero, mismo comportamiento que tiene estos cuerpos directivos que con menos madurez al menos atienden las recomendaciones de seguridad, la variación radica en la tercera posición donde el sector salud atiende más que el sector de telecomunicaciones.

Los cuerpos directivos del sector educación, consultoría especializada caso especial de empresas pequeñas y el sector de gobierno muestran un comportamiento de poco interés en participar o atender recomendaciones de seguridad

Los equipos directivos que solo delegan y esperan algún tipo de informe de avance de estos temas, el sector de educación, consultoría empresas pequeñas de menos de 50 empleados tienen este comportamiento y el sector del gobierno.

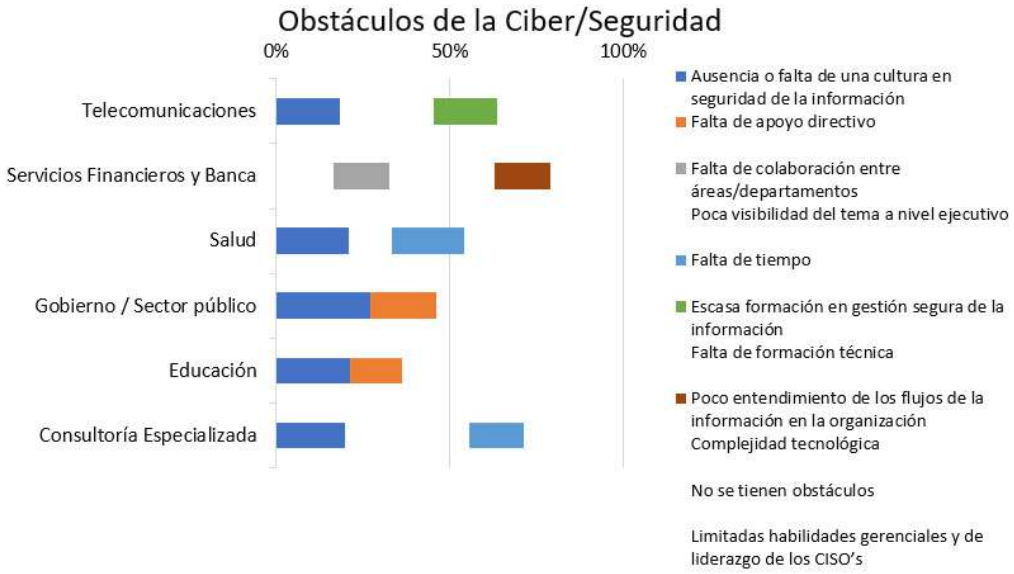
Esto resalta la idea de que la madurez de las organizaciones se ve reflejada desde la posición que decide asumir la dirección en relación con la ciberseguridad, cuando los líderes de riesgo y de seguridad vuelven a la seguridad un asunto de los negocios, se crea un compromiso en la dirección y cuerpos directivos no solo se involucran en ellos (Accenture, 2023).

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 (Nuspire, 2023), son parte de los que pueden existir para el Líder de Seguridad Digital de las empresas colombianas.

En la gráfica 31, se expresa cuáles son los obstáculos más representativos que los distintos sectores de la industria ha experimentado.

De la gráfica y los datos recolectados se pueden afirmar lo siguiente:

1. La cultura de seguridad es un factor diferencia en todos los sectores y es un gran obstáculo para que la postura de seguridad permee la organización.
2. Cada sector tiene un sentir con particularidades de como los



Gráfica 31. Obstáculos de la Seguridad por sectores

obstáculos hacen que los programas de seguridad no fluyan de la manera más adecuada posible.

3. Por ejemplo, el sector de telecomunicaciones resalta que uno de sus factores claves tiene que ver con las capacidades humanas y habilidades gerenciales de sus CISOs.
4. El sector financiero resalta los pocos entendimientos de los flujos de información es un factor que definitivamente hace fuerte presencia.
5. La falta de tiempo es el factor relevante en el sector salud y consultoría especializada, el cual inquieta pues muestra que no es la seguridad vista como un asunto de negocio, sino como un reto del momento en el que se requiera.
6. El sector gobierno ha considerado que el poco interés que este tema tiene tanto en el nivel ejecutivo como el apoyo que a este tema se le debe dar, como el obstáculo importante a considerar.
7. El apoyo de la dirección es otro de los impedimentos para que la ciber-seguridad fluya en las organizaciones.

Lo cierto de todos los datos y la gráfica 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 orien-

tar 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, 2023).

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).

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 de la consultoría especializada el que hace uso de todas las frecuencias de realización de la evaluación de riesgos
2. El sector de Consultoría especializada y gobierno realiza dos evaluaciones de riesgo al año con mayor porcentaje
3. El sector de educación usa una al año como su forma de explorar los riesgos.
4. En el sector salud se mantiene el desconocimiento del tema como la principal causa por la que estos ejercicios no se hacen en las empresas, entidades y/o organizaciones
5. En el sector de la Educación si bien se dice que se hace una vez, al indagar en dichos sectores por que no se hace, la manifestación está relacionada a que no existe un proceso formal de gestión de riesgos.
6. En cuanto a metodología del marco ISO tanto 27005 y 31000 son las metodologías más usadas en todos los sectores, sin embargo, el sector de la educación llama la atención porque en este sector no tener una metodología formal para gestionar los riesgos es el valor más alto de todos los sectores de la industria analizados.
7. 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 (AON,2023).

Capital intelectual

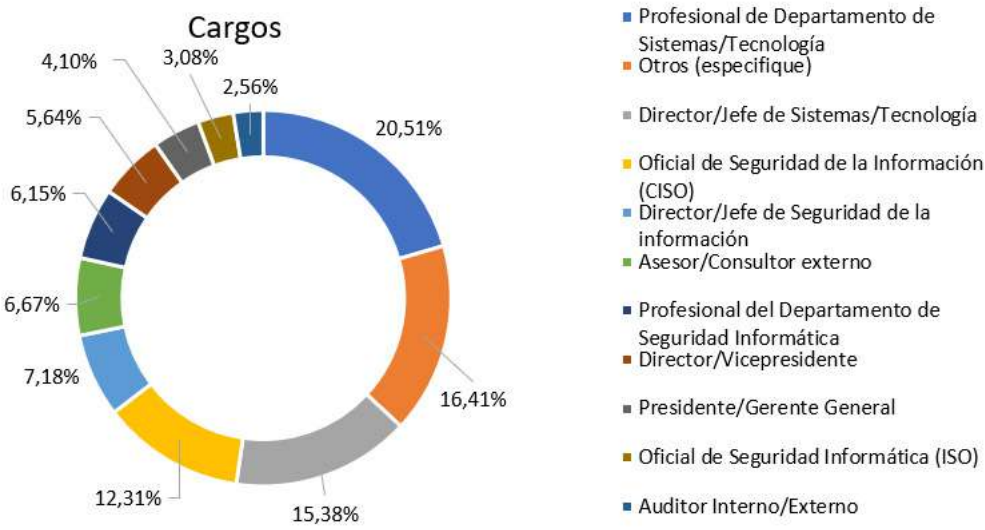
La gráfica 32 muestra los participantes de la encuesta de seguridad, en las cuales se puede ver que los profesionales de tecnología, de seguridad son los que más participan, el caso de otros está representado entre otros a docentes de las áreas de seguridad, especialistas de ciberseguridad que no se identifican con los roles propuestos.

Son múltiples y variadas las funciones del profesional de seguridad en las empresas de Colombia, la gráfica 33 muestra las múltiples funciones que hoy desempeña el profesional.

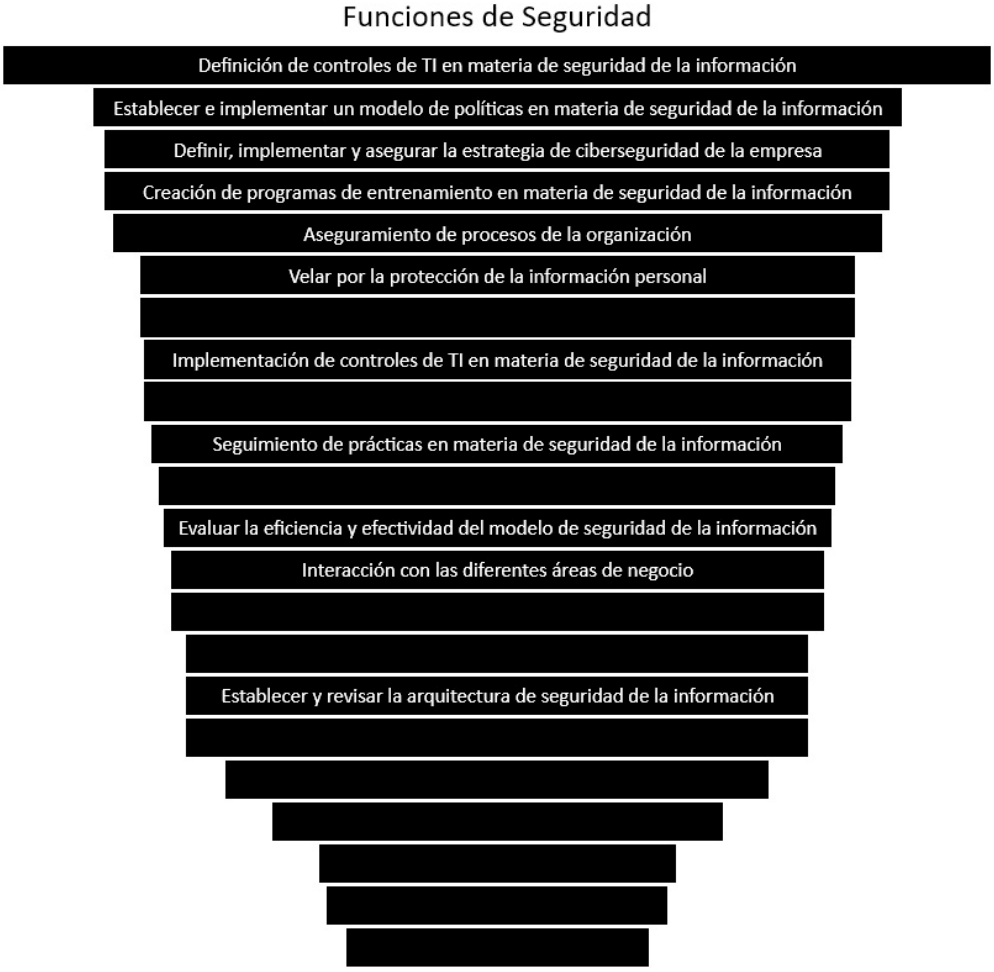
Las tres primeras funciones tienen que ver con, Definición de controles de TI en materia de seguridad de la información 65%, Establecer e implementar un modelo de políticas en materia de seguridad de la información 53%, Definir, implementar y asegurar la estrategia de ciberseguridad de la empresa 52%.

La gráfica 34 muestra la dependencia del área de seguridad en las empresas.

La gráfica 35 muestra los distintos roles que son usados en las empresas de la realidad colombiana.



Gráfica 32. Cargo de los participantes de la encuesta



Gráfica 33. Funciones del profesional de seguridad

Los tres roles más comunes, el analista de seguridad de la información 43%, el Oficial de Seguridad de la Información 37% y el analista de seguridad informática 33%.

La gráfica 36, muestra el tamaño de las áreas de seguridad, llama que el segundo valor de mayor importancia es ninguno con el 16,15%, el tamaño definitivamente consolidado es de 1 a 5 profesionales conformando un área de seguridad con el 58,46%.

Consideraciones de los datos

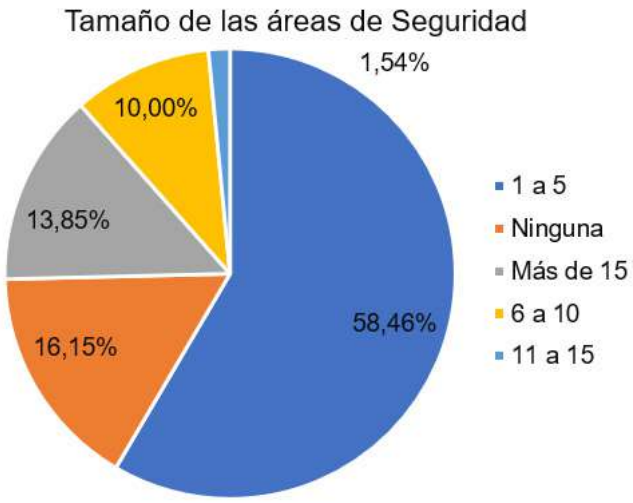
Quien es el profesional de seguridad

En Colombia el profesional de seguridad es un perfil, diverso y con muchas capacidades. La encuesta nacional de seguridad tiene parti-

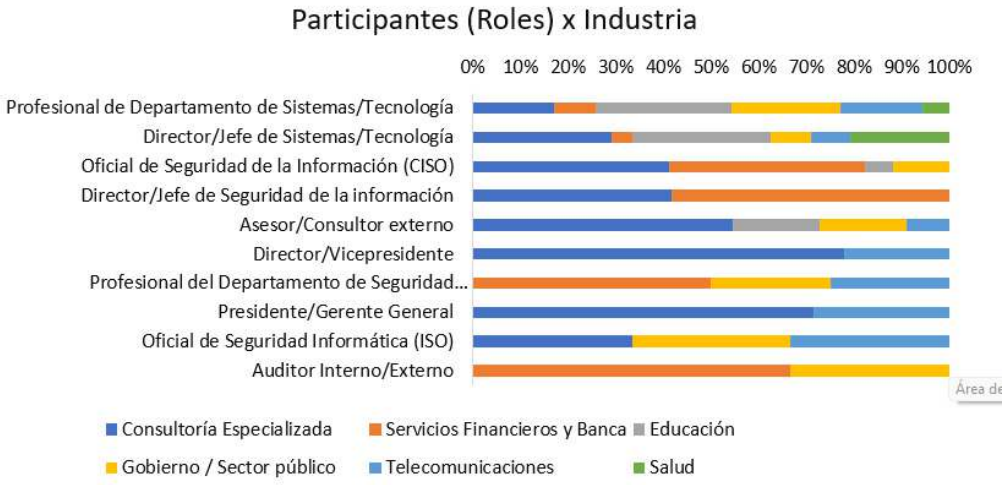
Gráfica 34. Dependencia de la Seguridad

Gráfica 35. Roles de Seguridad

cipación de múltiples sectores de industria y profesionales de las áreas afines. En la gráfica 36, vemos la distribución de profesionales por sector de industria, encontrando que el sector educación, telecomunicaciones y gobierno tiene una alta participación los profesionales de TI en el diligenciamiento de la encuesta, en el sector de la consultoría especializada y el sector salud, son los directores de tec-



Gráfica 36. Tamaño del área de Seguridad

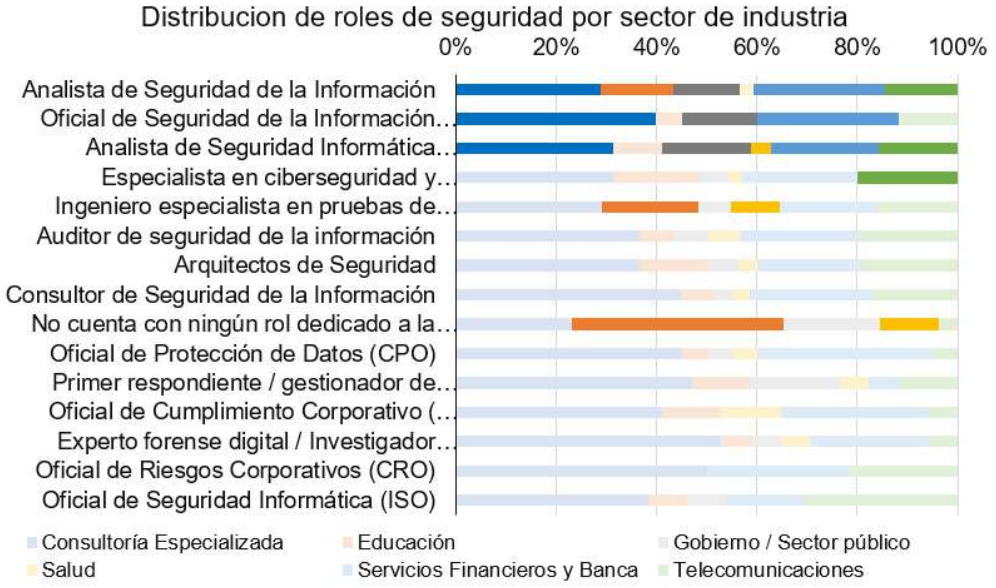


Gráfica 36. Participantes de la encuesta (Roles)

nologías los que más diligencian el instrumento, los Cisos y directores de seguridad del sector financiero y la consultoría especializada son seguidamente los que más participan.

Las diferentes industrias tienen tipos de roles y es lo que hace que se deban revisar roles, funciones e industrias.

La gráfica 37, muestra como las diferentes industrias determinan los roles que conforman sus áreas de seguridad, y esto claramente influye en la cantidad de funciones y responsabilidades del área de se-



Gráfica 37. Distribución de roles de seguridad por sector de industria

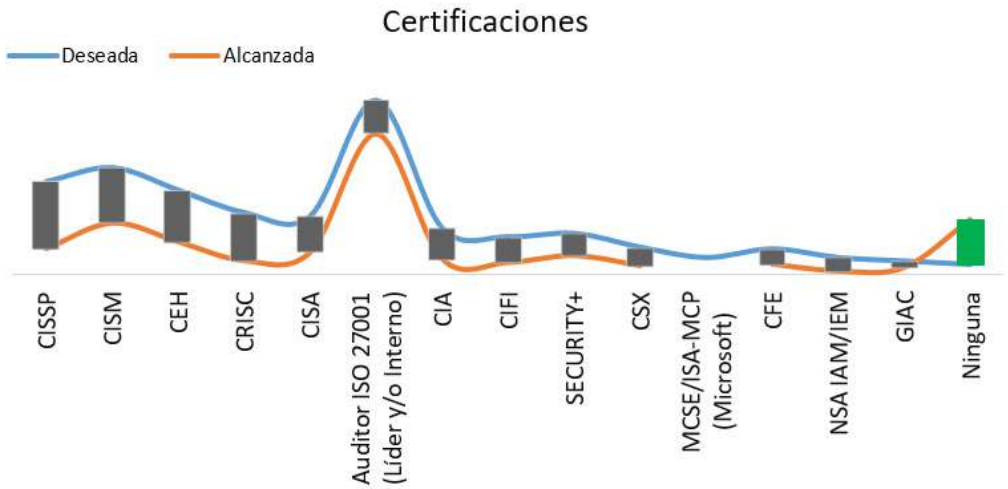
guridad, así como su nivel de entrega de información.

Este gráfico, determina cuáles son los tres roles más usados en los sectores más representativos de la industria en Colombia, diciendo el analista de seguridad de la información, el CISO Oficial de Seguridad de la Información, y el analista de seguridad informática son los roles primarios que existen, muy formalmente definido el rol del CISO está en el sector de la consultoría especializada, el financiero y el gobierno en ese orden de importancia.

El analista de seguridad informática está mayormente formalizado o es el rol principal en la consultoría especializada, que en los servicios financieros que en el sector financiero.

En el sector de las telecomunicaciones lo más común es encontrar analista de seguridad de la información como primer rol identificado.

Sectores que preocupan son el sector salud y educación, los cuales manifiestan como su valor más representativo, el hecho de que la función de seguridad no está y no ha dedicado ningún talento humano a esta función, lo que indicará o que no se desarrollan todas las funciones de seguridad o en su defecto las comparten específicamente con el área de tecnología.



Gráfica 38 Certificaciones de los profesionales de seguridad

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, 2023; Fortinet, 2023). La gráfica 38, precisamente refleja y se conecta con las tendencias internacionales.

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 CISM y CISSP respectivamente, sin embargo, al revisar lo que el profesional de seguridad desea lograr, se invierten los papeles y encontramos que la certificación de CISSP es la que más se busca en el contexto nacional seguido de CISM, y CEH respectivamente.

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 tran-

quilidad y bienestar (Deepinstinct, 2023).

¿Qué hace comúnmente?

Son diversas las actividades que hacen los profesionales de seguridad, y que dependen en gran medida de la madurez, formación del área de seguridad en las empresas, así como el sector (ArticWolf, 2023).

Para los sectores más importantes de la industria colombiana, definitivamente el área de seguridad y sus profesionales están centrados en la Definición de controles de TI en materia de seguridad de la información, sin embargo, al revisar las siguientes funciones si hay cambios interesantes por sector de la industria.

Sector financiero, en este sector las tres funciones principales son, Seguimiento de prácticas en materia de seguridad de la información, Definición de controles de TI en materia de seguridad de la información, Establecer e implementar un modelo de políticas en materia de seguridad de la información, Aseguramiento de procesos de la organización.

Consultoría especializada, sus principales actividades están centradas en, Definición de controles de TI en materia de seguridad de la información, Creación de programas de entrenamiento en materia de seguridad de la información, Definir, implementar y asegurar la estrategia de ciberseguridad de la empresa.

Gobierno / Sector público, sus actividades principales son: Definición de controles de TI en materia de seguridad de la información, Creación de programas de entrenamiento en materia de seguridad de la información, Definir, implementar y asegurar la estrategia de ciberseguridad de la empresa y Dirigir y supervisar los programas de riesgos de seguridad de la información de la organización. Existen dos funciones que comparten los mismos valores.

Telecomunicaciones, las áreas de seguridad se centran en Definición de controles de TI en materia de seguridad de la información, Velar por la protección de la información personal, Definir, diseñar y velar por el programa de privacidad de la información de la organización.

Educación, sus áreas de seguridad se centran en, Definición de controles de TI en materia de seguridad de la información, Aseguramiento de procesos de la organización, Definir, implementar y asegurar el programa de protección de datos personales de la empresa.

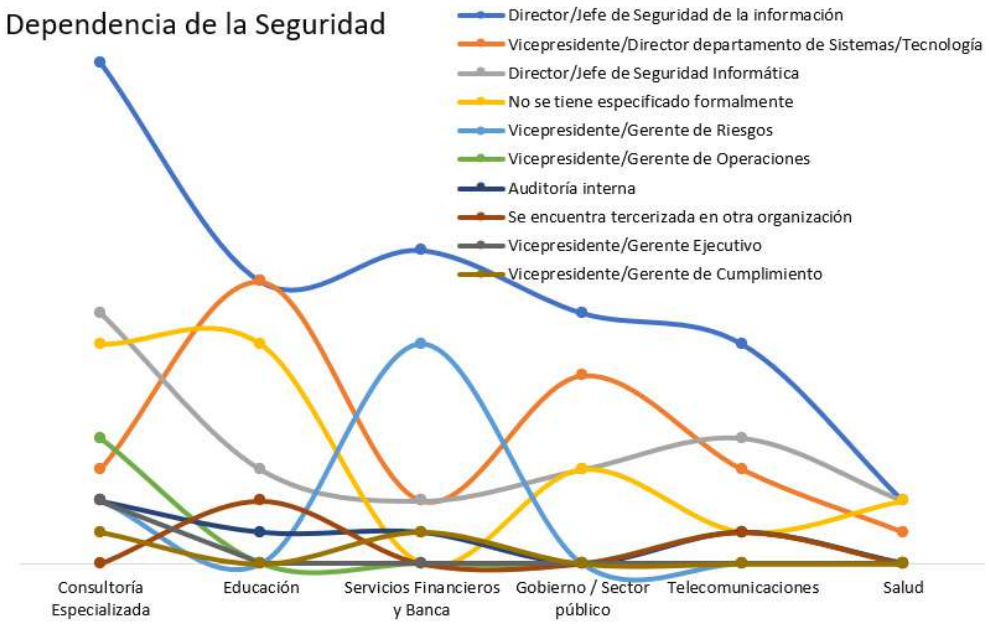
Salud, las actividades de seguridad en las que se centran sus equipos son, Definición de controles de TI en materia de seguridad de la información, Definir, implementar y asegurar la estrategia de ciberseguri-

dad de la empresa, Velar por la protección de la información personal, Definir, implementar y asegurar el programa de protección de datos personales de la empresa.

La tabla 12, es el detalle de todas las actividades y funciones del área de seguridad.

En cuanto a la dependencia de la seguridad, los diferentes sectores de la industria tienen posiciones interesantes, la gráfica 39, se puede observar que, el sector de la consultoría especializada tienen junto al sector financiero un área de seguridad posicionada y claramente definida de quien depende toda la función de seguridad, llama la atención que en estos mismos sectores la dirección de TI no tiene ninguna relación con la dependencia de seguridad, lo cual muestra y refleja una madurez en la función, el sector financiero adicional a lo anterior también muestra que la seguridad de la información puede estar dependiendo de una vicepresidencia de riesgo, comportamiento único en los sectores de la industria de Colombia.

Situaciones inquietantes, el sector salud es el único sector que muestra que no se tiene formalmente definida la función y la dependencia de la seguridad, deja al descubierto



Gráfica 39. Dependencia de la Seguridad por sectores

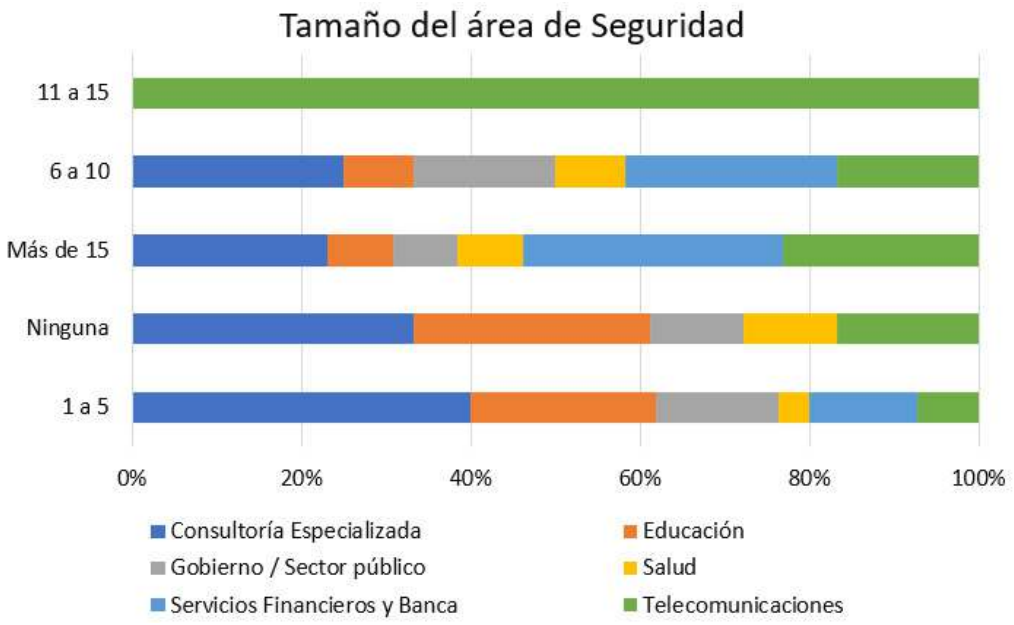
Tabla 12. Distribución de funciones del profesional de seguridad por sectores

Criterios	Consultoría Especializada	Educación	Gobierno / Sector público	Salud	Servicios Financieros y Banca	Telecomunicaciones
Definición de controles de TI en materia de seguridad de la información	17,44%	9,74%	6,15%	3,08%	8,72%	5,13%
Establecer e implementar un modelo de políticas en materia de seguridad de la información	15,90%	6,67%	6,15%	2,05%	8,21%	3,08%
Aseguramiento de procesos de la organización	13,85%	8,72%	5,13%	1,54%	8,21%	4,10%
Definir, implementar y asegurar la estrategia de ciberseguridad de la empresa	16,41%	6,67%	3,59%	3,08%	7,18%	3,08%
Creación de programas de entrenamiento en materia de seguridad de la información	16,92%	5,64%	3,59%	2,05%	7,69%	3,59%
Definir, diseñar y velar por el programa de privacidad de la información de la organización	13,33%	7,18%	4,62%	2,56%	5,13%	4,62%
Implementación de controles de TI en materia de seguridad de la información	12,82%	8,21%	4,62%	3,08%	4,10%	4,10%
Velar por la protección de la información personal	11,79%	6,15%	4,10%	3,08%	6,15%	5,13%
Definir, implementar y asegurar el programa de protección de datos personales de la empresa	10,77%	8,72%	4,62%	3,08%	5,13%	4,10%
Seguimiento de prácticas en materia de seguridad de la información	13,33%	5,64%	3,08%	2,05%	9,23%	2,05%
Informar a la alta gerencia sobre el avance del programa de seguridad de la información	13,33%	4,62%	3,08%	2,05%	7,69%	3,59%
Evaluar la eficiencia y efectividad del modelo de seguridad de la información	13,85%	5,13%	4,10%	2,05%	6,15%	2,05%

Dirigir y supervisar los programas de riesgos de seguridad de la información de la organización	13,33%	4,62%	5,13%	1,54%	7,18%	0,51%
Creación de programas de gobierno y gestión en materia de seguridad de la información	14,87%	3,59%	2,05%	2,05%	6,67%	2,56%
Establecer y revisar la arquitectura de seguridad de la información	11,79%	6,15%	2,05%	2,05%	7,18%	2,05%
Interacción con las diferentes áreas de negocio	11,28%	4,10%	3,08%	2,05%	6,15%	4,10%
Gestionar el programa de gestión de incidentes de seguridad de la información	11,79%	5,13%	4,10%	2,05%	6,15%	1,03%
Supervisar procesos de cumplimiento regulatorio en tecnología de información	10,77%	3,59%	3,59%	2,56%	6,15%	2,05%
Seguimiento de prácticas en materia de protección de la privacidad de la información personal	7,69%	5,64%	1,54%	1,03%	4,10%	3,08%
Supervisar y gestionar los procesos de investigaciones forenses digitales	6,67%	3,59%	1,54%	1,54%	3,59%	1,03%
Definir o diseñar escenarios/simulaciones/Playbooks en relación con ciberriesgos	4,62%	3,08%	1,54%	1,54%	3,59%	0,51%
Definir programas de resiliencia digital	5,13%	3,08%	2,05%	1,03%	2,05%	0,51%

las grandes falencias y claramente se conecta con las tendencias internacionales de ser uno de los sectores que más requiere de atención por el interés del adversario, así como la necesidad de fortalecer la función de seguridad (Proofpoint-Ponemon, 2023). De la misma manera inquietante que sectores como la educación, y el sector gobierno tengan este mismo comportamiento de no tener definida una línea de dependencia y que claramente hace que gobernar la seguridad y definir roles y responsabilidades sea mucho más complejo de realizar (Accenture, 2023)

Las áreas de seguridad en los distintos sectores de la industria en sus tamaños determinan el hacer y actuar del profesional de seguridad y sobre todo quien, sectores como las telecomunicaciones es el único sector que manifestó tener un área de seguridad entre 11 y 15 personas, mientras que los demás sectores de la industria tienen variedad



Gráfica 40. Tamaño del área de seguridad x sector de industria

en los tamaños de las áreas de seguridad. La gráfica 40, es una representación del tamaño de las áreas de seguridad distinguidas por los sectores de la industria.

Definitivamente se consolidad que un área de seguridad en Colombia tiene un tamaño hasta máximo 5 personas, sin decir que los demás tamaños no sean representativos, áreas de seguridad grandes, más de 15 personas las lidera el sector financiero, áreas entre 6 y 10 personas las lideran el sector de la consultoría especializada y el sector financiero, el sector de la consultoría especializada lidera en las áreas de 1 a 5 personas, y sorprende que el mismo sector sea el líder de las empresas que manifiestan no tener áreas de seguridad, seguido del sector educación.

En esa misma medida los tamaños de las áreas determinan los quehaceres de estas, mientras que las áreas pequeñas (1-5) profesionales de seguridad que en su mayoría son analista de seguridad de la información, de seguridad informática y coordinador de seguridad (CISO), se dedican a asegurar procesos, verificar eficacia y gestionar los incidentes. Las áreas medianas (6 a 15), que tienen un líder de seguridad con funciones ejecutivas al que se le llama CISO en algunos casos, tienen como funciones primarias hacer un seguimiento de las prácticas de seguridad, guiar a la empresa en aprender de sus incidentes a través de los procesos forenses y mejorar las capacidades cibernéticas de las empresas a través del diseño de playbooks en relación con el ciberriesgo. Por otro

lado, las áreas grandes (Más de 15), las cuales están conformadas por uno o varios líderes de seguridad con funciones específicas, arquitectos de seguridad y los roles de analistas muy bien definidos, se dedican principalmente a simular al adversario en relación con riesgo cibernético, mejorar las capacidades de la empresa en relación con la resiliencia empresarial y aprender de los incidentes a través de los procesos forense, que pueden ser evidenciados en la tabla 13. Sorprende que las áreas que manifiestan no tener una estructura definida para atender las funciones de seguridad, si realiza algunas actividades y las principales están todas centradas proteger de alguna manera la información y dedicarse cumplir con los requerimientos de cumplimiento de protección de datos bajo el contexto de la regulación colombiana.

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 (Proofpointb, 2023), 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.

La gráfica 41, muestra precisamente que tipo de información entrega en el CISO en la empresa. Cabe destacar que cada sector de la industria tiene unos matices importantes en la forma como es percibido el rol y cómo evalúan su valor.

Gráfica 41. Información que entrega el CISO por sector de la industria

Tabla 13. Funciones de seguridad por tamaño del área de seguridad

Funciones	Ninguna	Más de 15	6 a 10	11 a 15	1 a 5
Velar por la protección de la información personal	17,39%	17,39%	15,22%		50,00%
Aseguramiento de procesos de la organización	8,89%	15,56%	8,89%	2,22%	64,44%
Supervisar y gestionar los procesos de investigaciones forenses digitales		25,00%	20,83%		54,17%
Supervisar procesos de cumplimiento regulatorio en tecnología de información	10,26%	17,95%	12,82%		58,97%
Seguimiento de prácticas en materia de seguridad de la información	9,43%	18,87%	16,98%		54,72%
Seguimiento de prácticas en materia de protección de la privacidad de la información personal	6,45%	19,35%	12,90%		61,29%
Interacción con las diferentes áreas de negocio	12,50%	22,50%	15,00%		50,00%
Informar a la alta gerencia sobre el avance del programa de seguridad de la información	7,84%	17,65%	13,73%		60,78%
Implementación de controles de TI en materia de seguridad de la información	15,09%	18,87%	9,43%		56,60%
Gestionar el programa de gestión de incidentes de seguridad de la información	4,55%	18,18%	13,64%		63,64%
Evaluar la eficiencia y efectividad del modelo de seguridad de la información	9,09%	15,91%	11,36%		63,64%
Establecer y revisar la arquitectura de seguridad de la información	12,82%	23,08%	7,69%		56,41%
Establecer e implementar un modelo de políticas en materia de seguridad de la información	12,28%	14,04%	12,28%		61,40%
Dirigir y supervisar los programas de riesgos de seguridad de la información de la organización	9,76%	17,07%	9,76%		63,41%
Definir programas de resiliencia digital	15,00%	25,00%	15,00%		45,00%
Definir, implementar y asegurar la estrategia de ciberseguridad de la empresa	10,71%	16,07%	16,07%		57,14%
Definir, diseñar y velar por el programa de privacidad de la información de la organización	16,00%	12,00%	12,00%		60,00%
Definición de controles de TI en materia de seguridad de la información	15,15%	15,15%	10,61%	1,52%	57,58%
Creación de programas de entrenamiento en materia de seguridad de la información	12,73%	20,00%	12,73%		54,55%
Definir o diseñar escenarios/simulaciones/Playbooks en relación con ciberriesgos	9,09%	31,82%	18,18%		40,91%
Creación de programas de gobierno y gestión en materia de seguridad de la información	4,17%	20,83%	12,50%		62,50%
Definir, implementar y asegurar el programa de protección de datos personales de la empresa	16,00%	14,00%	14,00%		56,00%

En el sector de la consultoría especializada, el gobierno y el sector financiero, lo que más se valora es que el CISO, entrega información relacionada con la gestión de la seguridad para la toma de acción, por encima de los demás criterios. Una particularidad en el sector de la consultoría especializada es que el CISO también entrega información relacionada con los riesgos de seguridad y ciberseguridad para la toma de decisiones.

En el sector de la educación se reconoce que no existe esta figura, si bien es cierto que desarrollan algunas funciones con relación a la seguridad no existe un rol líder que se encargue de orientar a la empresa en ese sentido, lo cual claramente refleja un bajo nivel de gobierno de la seguridad.

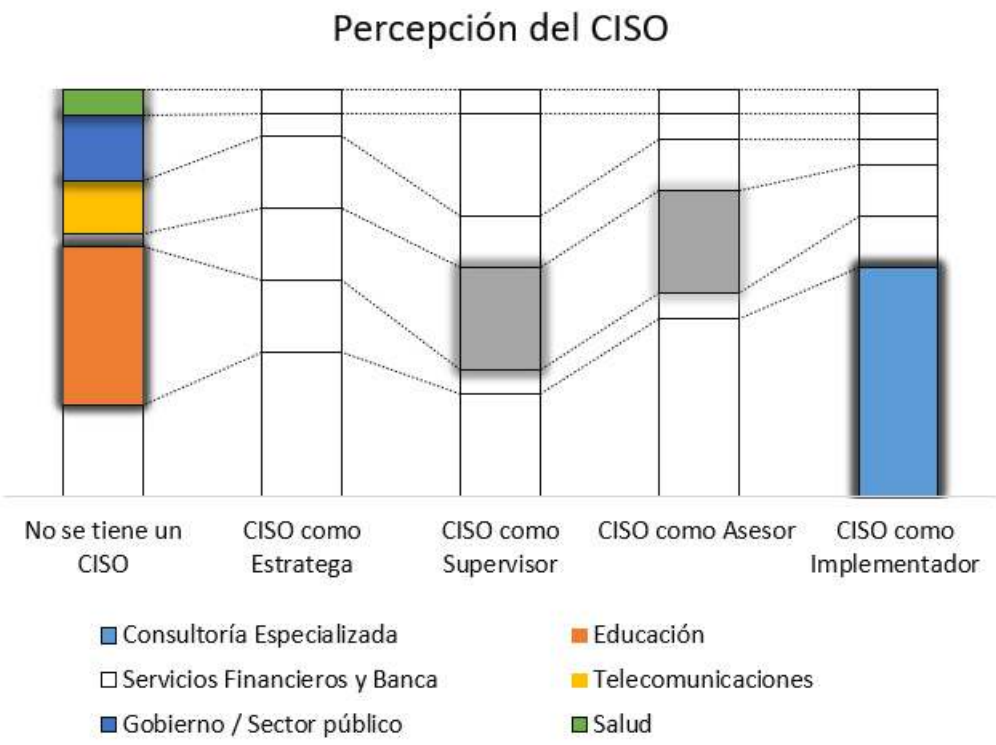
En el sector de la salud y de telecomunicaciones, lo que entrega el CISO como información en el caso de las empresas que tienen este cargo definido, entrega solo información de las posibles brechas de seguridad, esto se puede leer como una actividad reactiva que denota la emergencia manifiesta de desarrollar esta posición, frente a un constante asedio del adversario en el sector (Proofpoint-Ponemon, 2023).

Todas las organizaciones de una u otra manera perciben al CISO (Proofpoint, 2023), 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 42, 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 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, al revisar con las funciones del área, entonces claramente 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 una vista encontrada, por un lado lo ven como un supervisor una lectura viable toda vez que es un sector de la industria con una regulación amplia que debe velar por el cumplimiento de muchas medidas de control frente a los marcos regulatorios nacionales e internacionales, y en segundo lugar como un asesor que está soportado en la idea que en-



Gráfica 42. Percepción del CISO por industria

trega información de la gestión de riesgos y cuyas áreas de seguridad ya están desarrollando y viendo a la seguridad como una función que apoya a la resiliencia operacional del negocio.

Esto muestra que las empresas colombianas tienen unas grandes oportunidades para fortalecer el rol, darle un nivel de relevancia como ejecutivo y hacer que esta relación prospere, madure y contribuya al desarrollo de los modelos de negocio (Chelly, M. et all, 2023).

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 51%, la educación formal 41%, seguido de los cursos cortos con un 26%, la gráfica 43 muestra esta tendencia.

Sin embargo, el CISO en cada sector de la industria si muestra unos interesantes patrones de formación.

Los Cisos en el sector de la consultoría prefieren los cursos de formación ejecutiva con un 55% de las veces por encima de todos los demás, los pocos Cisos que existen en el sector salud prefieren con un 22% los diplomados, los Cisos del sector gobierno prefieren la educa-

Gráfica 43. Preferencia de formación del CISO

ción formal, claramente aprovechando los convenios y oportunidades que ofrece el estado en la formación en el mundo de las Tics, los profesionales de seguridad que se identifican como Cisos pese a que no estén definidos como tal, prefieren el mundo de las certificaciones. En el sector financiero la situación es diferente los Cisos en este sector por la importancia y relevancia prefieren las charlas especializadas y claramente los eventos de gran tamaño en ciberseguridad son de sus preferidos, por último y no menos importante los Cisos del sector de las telecomunicaciones prefieren los cursos cortos. La tabla 13 describe este comportamiento.

Siendo el CISO 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, sus capacidades estratégicas se colocan en primer lugar con un 41%; un 36% las capacidades intelectuales; un 26% las capacidades humanas; y, por último, la experiencia profesional con un 25%.

Es de anotar que las dinámicas de las empresas y los sectores de la industria colombiana hacen que se tengan algunos matices interesantes de estos datos, representados en la gráfica 44.

El sector de la consultoría en términos generales ve que las capacidades estratégicas son aquellas que deben ser mejoradas por los Cisos, razonable si analizamos que son áreas de seguridad más maduras que necesitan ya de un ejecutivo que pueda liderar y comunicar de una mejor manera la seguri-

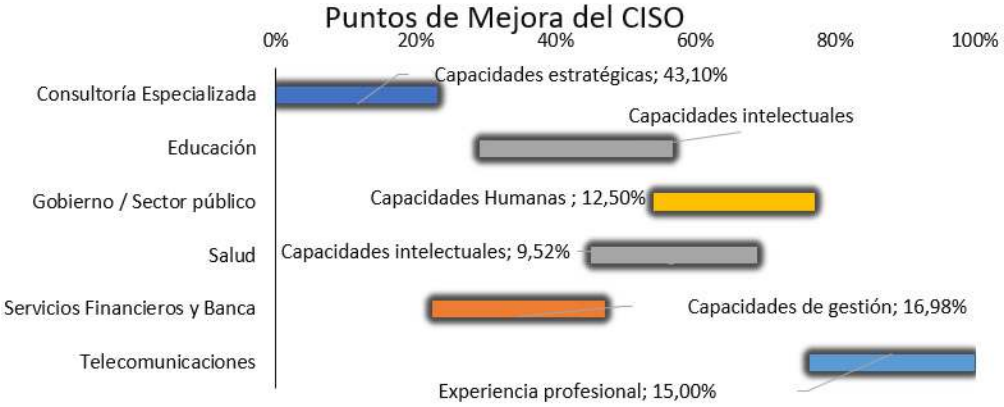
Tabla 14. Preferencia de formación de los Cisos por sectores de industria

Tipo de Formación	Consultoría Especializada	Educación	Gobierno / Sector público	Salud	Servicios Financieros y Banca	Telecomunicaciones
Educación formal universitaria	37,10%	17,74%	14,52%	3,23%	14,52%	12,90%
Charlas especializadas	42,86%	11,43%	11,43%	2,86%	20,00%	11,43%
Programas de formación ejecutiva	54,84%	9,68%	6,45%	3,23%	16,13%	9,68%
Cursos cortos	44,12%	8,82%	11,76%	5,88%	11,76%	17,65%
Certificaciones	38,46%	15,38%	12,82%	7,69%	15,38%	10,26%
Diplomados	42,42%	21,21%	9,09%	6,06%	15,15%	6,06%

dad como lo demanda la organización.

En el sector de la educación y salud, se necesita que el CISO mejore sus capacidades intelectuales que están asociadas a la actualización de sus conocimientos, toda vez que en este sector es probable que los profesionales de TI estén haciendo las transiciones al mundo de la seguridad y por tanto la actualización es importante.

El sector público, considera que las capacidades humanas de los Cisos son algo muy importante y que debe mejorar, es entendible puesto que en este sector el CISO es visto como un supervisor que puede ser interpretado como una persona rígida y poco flexible que puede



Gráfica 44. Puntos de mejora del CISO

estar necesitando mejorar su nivel de relacionamiento para que sus iniciativas pasen de un deber hacer como mensaje a uno de poder hacer para generar valor.

El sector financiero, considera que las capacidades de gestión son importantes y sobre todo que en este sector se debe enriquecer mucho el lenguaje del profesional al hablar de los riesgos bien sea porque requiera para tener diálogos abiertos con los líderes financieros y gerentes de las empresas (Balbix, 2023).

En el sector de las telecomunicaciones la experiencia de los Cisos es lo que se debe mejorar de tal manera que le ayude a sobre llevar los distintos retos que el sector posee, esto es un ejercicio que puede tener sus riesgos porque al buscar personas con mucha experiencia se puede incurrir en el riesgo de acrecentar la brecha de talento de la que hoy se habla en el mercado de la ciberseguridad (ISACA, 2023).

Temas emergentes

La gráfica 45 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, 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

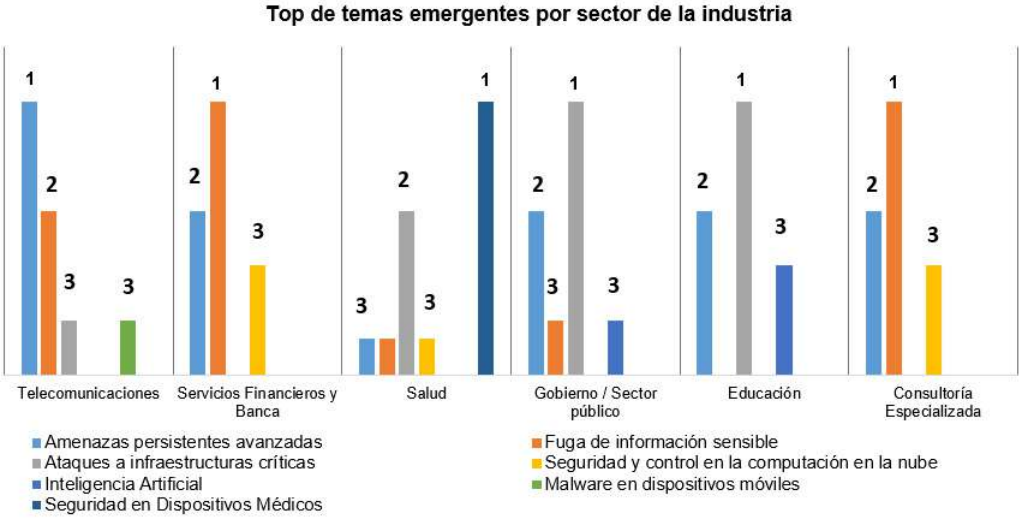
Gráfica 45. Temas emergentes

los profesionales de seguridad. Parámetros que coinciden con algunos de los asuntos que despiertan la atención de la agenda de los ejecutivos de seguridad en este 2023 y los que se verán en el 2024 (IBMc, 2023; Gartner, 2023; Forrester, 2022).

Consideraciones de los datos

Para todos los sectores de la industria se encuentran matices interesantes que direccionan claramente los esfuerzos y orientaciones del profesional y las áreas de seguridad, lo cual obviamente lleva a ver sectores con niveles de esfuerzo, madurez y realidades algo distantes. La gráfica 46 muestra los patrones de interés de los distintos sectores de la industria en relación con los temas emergentes.

De ella se puede decir, el sector de las telecomunicaciones ve a las amenazas persistentes, la fuga de información, el malware de dispositivos móviles y los ataques a infraestructuras críticas como sus mayores temas emergentes. El sector financiero por otro lado, ve a la fuga de información, las amenazas persistentes avanzadas y seguridad y control en la computación en la nube como sus temas a ser monitoreados y considerarlos emergentes. El sector de la salud ve la seguridad en los dispositivos médicos como su tema más relevante en segundo lugar los ataques de infraestructuras críticas y en tercer lugar se comparten el puesto la seguridad y control en la computación en la nube y las amenazas persistentes avanzadas. El sector del gobierno ve a los ataques de infraes-



Gráfica 46. Distribución de temas emergentes por sectores de la industria

tructuras críticas, las amenazas persistentes, fuga de información e inteligencia artificial como elementos claves que deben ser observados. El sector de la educación los ataques de infraestructuras críticas, amenazas persistentes y la inteligencia artificial como sus elementos relevantes. Por último la consultoría especializada ve a al fuga de información sensible, las amenazas persistentes y a la seguridad y control en la nube como un elemento emergente y de interés.

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).

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

Crear valor en un contexto digital, implica crear nuevos y novedosos esfuerzos por desarrollar programas de ciberseguridad que atiendan a las necesidades de las 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 (WEFb, 2023). Otro de los temas que trae gran atención a la mesa es el tema de los equipos de ciberseguridad (Stottandmay, 2023). Los ciberriesgos y la ciberresiliencia en general están en la agenda de todos los CEO de las organizaciones de todo el mundo y eso no es una sorpresa, realmente es una constante de los últimos años (Istari, 2023). Las tensiones geopolíticas, la reciente guerra en Ucrania, y los conflictos posteriores que se divisaran en el espacio digital son parte de lo que se visualiza no solo para el largo, también en el corto plazo (WEFb, 2023). 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 (Mandiant, 2023).

Las ciberoperaciones están a la orden del día, y con el conflicto en el cual se encuentra el mundo aún más. Es por ello, que se verán mayores movimientos por parte de gobiernos y naciones en el manejo de sus operaciones cibernéticas, de tal manera que debe haber un especial cuidado del ecosistema en el que se desenvuelven no solo las naciones, sino las organizaciones (Mandiantb, 2023). Definitivamente los riesgos que se presentan e incrementan por las cadenas de suministro serán otro de los juegos a atender en un espacio de trabajo cada vez más complejo, no solo para las organizaciones financieras, en todos los sectores de la industria la tensión y presión es importante pues no trabajar con los terceros y no hacerlos parte de un modelo integrado de protección puede traer consecuencias desafortunadas (Giarrusso, M., Nyholm, N., & Seth, K., 2023).

Claramente la pandemia dio una nueva visión al mundo digital, sin embargo, también ha mostrado por un lado el aumento sostenido de los riesgos, ha visibilizado aún más la capacidad del adversario por hacer daño, así mismo ha acelerado el

desarrollo de las capacidades organizacionales tanto para asegurar y proteger, como para anticipar y defenderse de un adversario cada vez más dotado (Trendmicro, 2023).

En esta nueva era los ejecutivos de seguridad se enfrentan de una manera más directa a otros escenarios dinámicos que demandan reacciones rápidas y prospectivas arriesgadas. Estos implican desarrollar espacios para anticiparse y observar los entornos cambiantes y superpuestos, en procura de la protección de la información y los nuevos activos digitales. Por tanto, esta nueva realidad hace que los líderes de seguridad necesiten evolucionar, no solo por desarrollar nuevas habilidades, a su vez capacidades y competencias que los posibiliten para enfrentar los desafíos actuales. Los Líderes de seguridad seguirán siendo líderes de niveles medios (Heidrick, 2023; Proofprintb, 2023; Coalfire, 2023), que deben poder actualizar el conjunto de herramientas como la comunicación para que puedan interactuar con mayor determinación en los equipos de trabajo.

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. 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.
2. Las áreas de seguridad siguen ganando terreno, espacio, posición, poder e influencia, todos los sectores de la industria a su ritmo lo ven y siguen aprendiendo, a lo mejor no con la velocidad que debería ser, pero al menos los marcadores e indicadores muestran progreso en todos ellos.
3. Las compañías de gran tamaño, con más de 1000 empleados, son las que tienen mayor claridad en torno a un área independiente y a un director de seguridad. En tales empresas grandes, el área de seguridad depende de las direcciones como la de gestión de riesgos. Es interesante observar entre las organizaciones de todos los tamaños, el bajo porcentaje que no tiene un cargo o responsabilidades definidas.
4. La voz del CISO continúa su proceso de afianzamiento den-

tro de las organizaciones, cada vez se ven más plazas creadas de profesionales de seguridad como CISOs, directores/gerentes de seguridad en las organizaciones, estos movimientos demandan la creación de nuevas y actualizadas conjunto de competencias, capacidades y habilidades que le permitan desarrollar mejor sus nuevas funciones. La formación, crecimiento y aprendizaje del CISO, sigue estando presente, no se puede sustraer su esfuerzo por seguir asimilando lo que significa la función, el rol y sobre todo la adaptabilidad en un entorno tan cambiante como el actual.

5. La práctica básica, como la gestión de riesgos, el uso de marcos de referencia, son una realidad en Colombia, su afianzamiento es requerido, para que el fundamento de la ciberseguridad esté acorde con las necesidades de las empresas, y así poder avanzar en el desarrollo de capacidades que lleven a las organizaciones a un estado de ciberresiliencia que soporte las operaciones del negocio.
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).

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

Accenture. (2023). How cybersecurity boosts enterprise reinvention to drive business resilience. https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-State-Cybersecurity.pdf

AON, (2023). How cyber risk touches nearly all aspects of business risk. https://www.aon.com/2023-cyber-resilience-report/risk/how-cyber-risk-touches-nearly-all-aspects-of-business-risk/

ArcticWolf. (2023). The state of cybersecurity: 2023 trends report. https://arcticwolf.com/resource/aw/the-state-of-cybersecurity-2023-trends-report

Balbix. (2023). Anuj Magazine. Cyber risk in CFO lingo: CISOs need a financial vocabulary. https://www.balbix.com/blog/cyber-risk-in-cfo-lingo-cisos-need-a-financial-vocabulary/

Barracuda. (2023). 2023 spear-phising trends. https://www.barracuda.com/reports/spear-phishing-trends-2023

Barracuda(b). (2023). 2023 email security trends. https://www.barracuda.com/reports/email-security-trends-report-2023

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

CheckPoint. (2023) Global analysis. https://go.checkpoint.com/2023-cyber-security-report/chapter-04.php

Chelly, M. L., Tan, S., & Tran, H. (2023). Building a Cyber Resilient Business: A cyber handbook for executives and boards. Packt Publishing.

Coalfire. (2023). The state of CISO influence 2023. https://www.coalfire.com/insights/resources/reports/the-state-of-ciso-influence-2023

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

Cofense (2023). from https://cofense.com/lp/q1-cofense-phishing-intelligence-report/

CyberEdge Group. (2023). Cyberthreat Defense Report. https://cyber-edge.com/cdr/

Cybereason. (2022). Ransomware the true cost to business 2022. https://www.cybereason.com/ransomware-the-true-cost-to-business-2022

Davis. D. (2021). 5 Models for the Post-Pandemic Workplace. HBR. https://hbr.org/2021/06/5-models-for-the-post-pandemic-workplace

Diligent Institute. 2023. What Directors Think 2023. Diligent Institute. https://www.diligentinstitute.com/research/what-directors-think-2023/

Deloitte (2021). Building The Resilient Organization. https://www2.deloitte.com/content/dam/insights/articles/US114083_Global-resilience-and-disruption/2021-Resilience-Report.pdf

Deepinstinct. (2023). Voice of SecOps V4. https://info.deepinstinct.com/voice-of-secops-v4-2023

Dynatrace. (2022). Observability and security are key to closing vulnerability gaps. https://www.dynatrace.com/news/press-release/global-ciso-research-2022/

ECIIA. (2023). Risk in Focus 2024: Hot topics for internal auditors. https://www.eciia.eu/2023/09/risk-in-focus-2024-hot-topic-for-internal-auditors/

EY. (2023). If AI holds the answers, are CEOs asking the right strategic questions? https://www.ey.com/en_gl/ceo/ceo-outlook-global-report

Forrester. (2022). Forrester's 2023 predictions indicate a bumpy road ahead for CISOs. VentureBeat. https://venturebeat.com/security/forrester-2023-predictions-indicate-a-bumpy-road-ahead-for-cisos/

Gartner. (2023). Top 10 Strategic Predictions for 2023 and beyond. (n.d.). Gartner. https://www.gartner.com/en/articles/gartner-top-10-strategic-predictions-for-2023-and-beyond

FBI. (2023). Internet crime report 2022. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

FINSIN. (2023). Reporte (bi)mensual de Phishing Abril y Mayo 2023. FINSIN. https://finsin.cl/2023/06/13/reporte-bimensual-de-phishing-abril-y-mayo-2023/

Fortinet. (2023). Cybersecurity Skills Gap. https://www.fortinet.com/content/dam/fortinet/assets/reports/2023-cybersecurity-skills-gap-report.pdf

FS-ISAC. (2023). Navigating Cyber2023. https://www.fsisac.com/navigatingcyber2023

Giarrusso, M., Nyholm, N., & Seth, K. (2023). 2023 EY Global Third-Party Risk Management Survey. https://www.ey.com/en_gl/risk/2023-ey-global-third-party-risk-management-survey

Heidrick. 2023 global chief information security officer (CISO) survey. https://www.heidrick.com/en/insights/cybersecurity/2023-global-chief-information-security-officer-survey

HCLTech. (2023). Tech Trends 2023 – Business and Industry Edition. https://www.hcltech.com/sites/default/files/document/open/TechTrends2023_Business-and-Industry-edition-FV.pdf

IBM. (2023). Chief Executive Officer Study: Decision-making in the age of AI. https://www.ibm.com/thought-leadership/institute-business-value/c-suite-study/ceo

IBM(b). (2023). Cost of a Data Breach Report 2023. https://www.ibm.com/downloads/cas/E3G5JMBP

IBM(c). (2023). IBM institute for business value | research brief. Ibm.com. Retrieved October 17, 2023, from https://www.ibm.com/downloads/cas/JLKJK1ZP

Indusface. (2022). The state of application security 2022. https://www.indusface.com/resources/research-reports/the-state-of-application-security-q4-2022/

Imperva. (2022). Quantifying the cost of API insecurity. https://www.imperva.com/resources/resource-library/reports/quantifying-the-cost-of-api-insecurity/

Ironscale. (2022). How much does phishing cost businesses? https://secure.ironscales.com/the-business-cost-of-phishing/report-download

ISACA. (2023). State of Cybersecurity 2023, Global Update on Workforce Efforts, Resources and Cyberoperations. https://www.isaca.org/state-of-cybersecurity-2023

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

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

KPMG. (2023). Cybersecurity considerations 2023. https://kpmg.com/xx/en/home/insights/2023/02/cybersecurity-considerations-2023.html

KnowBe4. (2023). TYP phishing by industry benchmarking. https://www.knowbe4.com/typ-phishing-by-industry-benchmarking

Kroll. (2023). Cyber Risk and CFOs. https://www.kroll.com/-/media/kroll-images/pdfs/cyber-risk-cfos-report.pdf

Magnet. (2023). 2023 State of Enterprise Digital Forensics and Incident Response. https://www.magnetforensics.com/resources/2023-state-of-enterprise-digital-forensics-and-incident-response/

Mandiant (2023). M-Trends 2023. https://www.mandiant.com/m-trends

Mandiant(b). (2023). | Mandiant Cyber Security Forecast 2023. https://www.mandiant.com/resources/reports/mandiant-cyber-security-forecast-2023

Marsh. (2022). Cyber resilience: 12 key controls to strengthen your security. https://www.marsh.com/us/services/cyber-risk/insights/cyber-resilience-twelve-key-controls-to-strengthen-your-security.html

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

Martinez, J. (2022). La información es inútil sin conocimiento. https://www.linkedin.com/pulse/la-informaci%25C3%25B3n-es-in%25C3%25BAtil-sin-conocimiento-javier-mart%25C3%25ADnez-aldanondo/?trackingId=%2F8Kotk%2BATGGJnh%2FuRNG70Q%3D%3D

Minterellison. (2023). Perspectives on Cyber Risk 2023: the real cost of a data breach – Insight. https://www.minterellison.com/articles/

perspectives-on-cyber-risk-2023-the-real-cost-of-a-data-breach

NACD. (2022). 2022 GOVERNANCE OUTLOOK. https://boardleadership.nacdonline.org/rs/815-YTL-682/images/2022_Governance_Outlook.pdf

Nuspire. (2023). Second annual CISO research report on challenges and buying trends: A focus on optimization. https://5182296.fs1.hubspotusercontentna1.net/hubfs/5182296/Analyst%20research/Nuspire_Annual%20CISO%20Report_25May23.pdf

OPSWAT. (2023). 2023 state of web application security. https://www.opswat.com/resources/reports/2023-state-of-web-application-security

PwC. (2023). Cyber threats 2022: A year in retrospect. https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect.html

PwC(b). 2023. Winning today's race while running tomorrow's. PwC. https://www.pwc.com/gx/en/issues/c-suite-insights/ceo-survey-2023.html

PwC(c) (2022). 2022 Global Risk Survey Embracing risk in the face of disruption. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/assets/pwc-global-risk-survey-report-2022-main.pdf

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

Proofpoint(a). (2023). 2023 Human Factor. https://www.proofpoint.com/uk/resources/threat-reports/human-factor

Proofpoint(b). (2023). 2023 Voice of the CISO REPORT. Global Insights Into CISO Challenges, Expectations and Priorities. https://www.proofpoint.com/sites/default/files/white-papers/pfpt-us-wp-voice-of-the-CISO-report.pdf

Proofpoint(c). (2023). 2023 State of the Phish. https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

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

Secureworks. (2023). Learning from incident response: 2022 year in review. https://www.secureworks.com/resources/rp-irs-learning-from-incident-response-team-2022-year-in-review

Sophos. (2023). El estado del ransomware 2023. https://assets.sophos.com/X24WTUEQ/at/jr9ftt3m4qmzbw86m8wgq5f/sophos-state-of-ransomware-2023-wpes.pdf

Stottandmay. (2023). Cyber Security in Focus 2023. https://resources.stottandmay.com/hubfs/Research/2023_Cyber%20Security%20in%20Focus_Web.pdf

TrendMicro. (2023). Future/tense: Trend micro security predictions 2023. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2023

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

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

Verizon (2023). Data Breach Investigation Report. https://www.verizon.com/business/resources/T5b/reports/2023-data-breach-investigations-report-dbir.pdf

Vmware. (2022). Global Incident Response Threat Report. https://www.vmware.com/content/dam/learn/en/amer/fy23/pdf/1553238_Global_Incident_Response_Threat_Report_Weathering_The_Storm.pdf

WEF - World Economic Forum (2023) Global Risk Report 2023. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

WEF(b) - World Economic Forum (2023) Global Cybersecurity Outlook. Meeting of experts. https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

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

Zscaler. (2023). Informe sobre el estado del phishing de Zscaler ThreatLabz https://info.zscaler.com/resources-industry-reports-threatlabz-phishing-report-es

***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.*

¿Transformación o confusión digital?

DOI: 10.29236/sistemas.n169a5

Este encuentro es un espacio para reflexionar sobre los retos que enfrentan las organizaciones en procura de adaptarse a los cambios en sus ecosistemas digitales, y sobre cómo poner en marcha estrategias para adoptar transformaciones digitales en su interior.

Sara Gallardo M.

Fueron convocados tres especialistas en estos asuntos con quienes se dio comienzo al debate bajo la moderación Emir Pernet y María Mercedes Corral, quienes formularon la primera inquietud, acompañados de Jeimy J. Cano M., director de la revista.

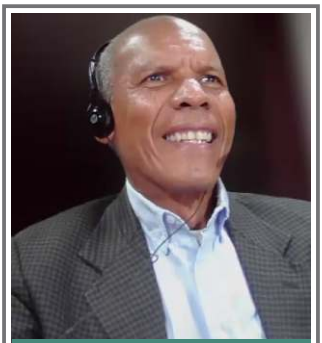
¿Cuáles son los principales aspectos por considerar en un proceso de transformación digital en una organización y en cuál aspecto considera usted que no se puede equivocar?

Bogdan Djoric
myCloudDoor Colombia
Director para Colombia

Oscar Wilde, escritor genial que me fascina, afirmaba que la experiencia es el nombre que le damos a nuestros errores, porque todos nos

equivocamos. Pero hay un aspecto en el que no podemos fallar en la transformación digital, que es crear y exigir la cultura de cambio en la organización, algo que no es simple. Los seres humanos somos individuos que por naturaleza de nuestra especie nos resistimos al cambio y en las organizaciones pasa lo mismo. Así que el problema es ¿cómo crear y mantener una cultura que impulse el cambio? Es un asunto de liderazgo dentro de la empresa y se trata de contar con talento dispuesto a enfrentarlo y propiciarlo. Hay una frase de Lou Gerstner que él usó para narrar cómo tomó el control de IBM, estableció una nueva misión, logró una transformación competitiva y cultural y superó la crisis que sufría la empresa que lideró: “Como líder, si uno quiere cambio, debe empoderar a los líderes del cambio y desempoderar a los líderes del status quo”. Si no lo hace, en esa mezcla no ocurren cosas buenas, se produce conflicto, frustración y como resultado los líderes del cambio se desgastan y se van. Por eso, hay que “tener coraje” y desde el CEO debe existir y promoverse una cultura de liderazgo orientada a la transformación constante.


María Mercedes Corral


Emir Pernet


Bogdan Djoric


Luis Puerto Y.


Alberto Cueto

Luis Puerto Y.
U. Externado de Colombia
Director Transformación Digital

Mi experiencia abarca la colaboración integral con personas, procesos y tecnologías, enfocándome especialmente en la gestión de datos, un elemento clave en cada uno de estos aspectos. Quiero enfatizar este punto debido a un desafío recurrente que he observado: nuestros líderes, a pesar de su capacidad, a menudo luchan con la rápida evolución del panorama tecnológico. Esta velocidad de cambio resulta en estrategias que, apenas son formuladas, parecen desfasadas frente a modelos establecidos, generando incertidumbre sobre la dirección a seguir. La pregunta persistente es si avanzar, detenernos o reajustar.

Este dilema se agudiza cuando se enfrenta a procesos organizacionales que son inherentemente rígidos y resistentes al cambio. La transformación exitosa, por lo tanto, requiere una integración profunda con la cultura organizacional, la cual debe evolucionar en respuesta a la estrategia adoptada. Este proceso debe ser inclusivo, abarcando desde quienes ejecutan tareas operativas hasta aquellos en puestos de liderazgo, asegurando su convicción y compromiso.

Finalmente, la claridad en la estrategia es fundamental; sin ella, nos enfrentamos al riesgo de un fracaso significativo. Solo con una estrategia bien definida podemos esperar progresar de manera efectiva.

Bogdan Djoric
Opino que cultura y estrategia son inseparables, así como los comportamientos de las personas en los cuales todo se refleja.

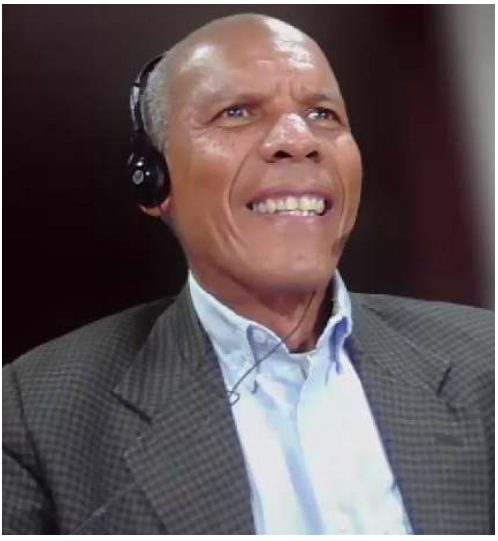
La transformación digital es un tema que se discute desde hace mucho, pero ¿qué pretende una empresa al llevarla a cabo? ¿Qué persigue? Persigue sobrevivir, y las empresas que sobreviven hoy en día son las que adoptan nuevas tecnologías y saben crear nuevos modelos de negocio usando esas nuevas tecnologías. Estoy de acuerdo con Luis en que la estrategia debe ser muy adaptable. Eso conlleva una cultura corporativa que debe estar muy clara para todos.

Hoy en día la inteligencia artificial es una de las tecnologías esen-

ciales, si se puede denominar así, y será como en la famosa teoría de Darwin: el que mejor se adapta sobrevive, el que no, se extingue.

Emir Pernet

De cara al líder ¿cuál sería el perfil de ese líder transformacional? ¿Cuáles son las características que debe tener y que va uno a potenciar?



Bogdan Djoric

Para crear ese perfil de líder transformacional, dispongo de varios ingredientes y confío en que todos los que estamos aquí podemos conseguirlo. El líder debe ser una persona que se acomode al cambio con soltura, que no le asuste el riesgo y que admita la posibilidad de fallar. Ese perfil es importante. También debe ser un aprendiz, alguien que promueva el aprendizaje constante. Eso es algo que he aprendido de la empresa Amazon. Ellos afirman que necesitamos "learners" y que todos sus empleados son "líderes", sin importar su nivel. Además, debe ser un apasionado de los datos, que sepa utilizar todas las herramientas existentes para sacar valor de ellos. Los que saben hacer eso son los que prosperan. Y por último, debe ser un líder empático, una buena persona, que motive a los demás. Estos son los rasgos que quiero en un líder: audacia, adaptación, aprendizaje, análisis y empatía.

Luis Puerto Y.

En los pilares de cualquier estrategia, es crucial definir y entender claramente el rumbo del sector matizado con el enfoque del líder y la empresa. Los elementos básicos, como la planeación, objetivos estratégicos e indicadores, son esenciales para guiar el cambio. Lograr esto requiere salir del entorno habitual y observar el entorno. En educación, por ejemplo, es frecuente el aislamiento puede llevar a una percepción engañosa de perfección, lo cual es dañino para la estrategia. Ser empático es fundamental, especialmente al conocer las necesidades de clientes como docentes y estudiantes. Comprender si las estrategias funcionan implica involucrarse directamente en sus procesos. No se trata solo de un pensamiento teórico elevado; es crucial rodearse de personas que aporten conocimiento y salir del status quo para entender la realidad. En un mundo interconectado, los eventos externos impactan a todos los sectores, no solo al propio.

Jeimy J. Cano M.

Abrazar y pactar con el incierto, para resumir lo aquí planteado. Mediante prototipos y simulaciones. ¡Necesitamos hacer cosas distintas!

Bogdan Djoric

Me gustaría comentar algo que me pareció interesante y que tiene que ver con el reto de tener una estrategia, una arquitectura y un objetivo definidos, cuando todo cambia tan rápido que en uno o dos años, estos objetivos ya son irrelevantes. Y esa es la incertidumbre que nos plantea el futuro. Según el Presidente Eisenhower, "los planes son inútiles, pero planificar es indispensable". Aunque los planes tengan una duración corta, hay que elaborarlos, pero saber a la vez que no se cumplirán a rajatabla.

En el libro "Sapiens", el autor se pregunta cuál es el mayor descubrimiento de la humanidad. Y se responde que el mayor descubrimiento es la ignorancia. Tenemos que convivir con que no sabemos. En la Edad Media, las Sagradas Escrituras eran la única fuente de conocimiento y no había que indagar nada más. Al descubrir la ignorancia, entramos en la senda del progreso. Y hoy en día, la ignorancia sigue mucha.

Alberto Cueto

Consultor

El líder debe tener muy clara cuál es la visión estratégica de la organización, como ya se mencionó, entendiendo los objetivos a lograr en el corto, mediano y largo plazo, y para cada uno de ellos el papel que la tecnología puede desempeñar. Aunque la tecnología es un catalizador de la transformación y operación de todas las empresas, no en todas funciona igual, y no todas las tecnologías son igualmente aplicables en cualquier empresa. Lo anterior, trabajado conjuntamente con la transformación, cambio, cultural que la organización requiere. Si las personas no están involucradas, de forma positiva e inclusiva, la transformación digital será difícil de lograr; este es un punto en que no puede haber equivocaciones.

La estrategia de gestión del cambio es otro tema crítico a trabajar por el líder, porque es importante alinear los intereses de las personas con los de la organización, en un ambiente propicio para el cambio. Es

indispensable identificar los primeros líderes del cambio, apoyarse en ellos, y lograr que la organización poco a poco se permee y contagie del cambio en marcha, motivados por la inclusión, la necesidad de pertenecer a ese cambio, y de disfrutar los beneficios del cambio que se deber ir materializando de manera paulatina pero continua. Los detractores del cambio normalmente salen de manera natural de la organización, porque acaban sintiéndose incómodos y extraños a los procesos pues les “duele”. Y para que las cosas fluyan es necesario involucrar a las personas adecuadas que pueden convertir el proceso de cambio de la cultura organizacional en éxito.

Emir Pernet

Precisamente, en torno la estrategia formulamos la siguiente pregunta. ¿Cuáles indicadores le comparten a la alta gerencia sobre el avance en la transformación digital de su empresa? ¿Tienen una hoja de ruta? ¿Está concertada con los ejecutivos de primer nivel?

Luis Puerto Y.

Tradicionalmente no nos enfocamos en monitorear indicadores o cuadros de mando de manera rigurosa, hay un aspecto que se ha vuelto crucial con el tiempo - y en nuestra institución, esto se ha observado a lo largo de ocho años. Nos hemos dado cuenta de que nuestros estudiantes, principalmente Millennials y Centennials, valoran enormemente la satisfacción del cliente. Esta percepción ha guiado nuestra estrategia, llevándonos a preguntarnos constantemente: '¿Cómo lograr la satisfacción del cliente?' Esta pregunta se ha convertido en un indicador esencial para medir nuestro progreso en la transformación digital. Aunque no seguimos una hoja de ruta tradicional, la satisfacción del estudiante, que refleja nuestro éxito en adaptarnos a sus necesidades y expectativas cambiantes, es compartida y reconocida por la alta gerencia y los ejecutivos de primer nivel.

Bogdan Djoric

El tema no es sencillo, sabemos que en las empresas y juntas directivas, donde están los accionistas y propietarios, los estados financieros son la prioridad. Esos son los indicadores que ellos vigilan. ¿Cómo se vinculan con la

transformación digital? Eso supone un costo y una migración a la nube, una experimentación y unos resultados que pueden ser más o menos rentables, pero que exigen de profesionales, talento, fallos y paciencia. Es un desafío constante que tiene la gerencia, los líderes, de persuadir a la empresa de que hay que invertir. Un libro interesante sobre cómo se implementaron los objetivos OKR en Google es "Mide lo que importa", donde se ofrecen orientaciones de diversa índole. Al final, las empresas son sistemas donde hay entradas y salidas, y para obtener la salida o el resultado deseado, necesitamos incidir en la entrada.

Estoy totalmente de acuerdo en que es necesario crear indicadores de futuro y una cultura integral alrededor de estos temas.

Emir Pernet

¿Qué elementos concretos y verificables les indican a ustedes que han alcanzado una transformación digital exitosa y cuáles serían los dos principales indicadores con los que se calificaría exitoso su proceso?

Alberto Cueto

El proceso de transformación digital debe conducir a una forma distinta de ver las cosas. Los objetivos de la organización se deben estar logrando, pero sin perder del foco al cliente o usuario, y sin descuidar las personas al interior de la organización. En este orden de ideas, los elementos podrían ser: satisfacción del usuario, además de un pensamiento transformacional continuo de las personas, hacia la satisfacción del usuario dentro de los objetivos organizacionales. El cambiar, para beneficio de la organización y del usuario, debe ser un proceso natural.

Bogdan Djoric

Los indicadores o "sensores", me gustó que se les llamara así porque son el pulso de la empresa, son muy importantes. Pero también hay que medir a las personas, los procesos y la tecnología. ¿Cuáles serían los dos indicadores más importantes? Creo que cada organización tiene que determinar qué es lo que quiere medir y depende de su negocio y sus metas. Por ejemplo, si medimos los errores "buenos" y son muchos, eso significa que lo estamos intentando. Pretender ser una organización perfecta en la que no hay errores es irreal.

Luis Puerto Y.

En nuestro proceso de transformación digital en el sector educativo, hemos identificado elementos clave que nos indican el éxito de nuestras iniciativas. Primero, la colaboración interuniversitaria para identificar indicadores comunes que nos indique como estamos frente al sector es significativo y nos ofrece un marco de referencia de cómo mejorar. A diferencia de otros sectores donde la competencia es primordial, en el ámbito educativo, especialmente entre las universida-

des iberoamericanas, hemos observado una tendencia creciente hacia la colaboración y la unión de esfuerzos. Este fenómeno no solo refleja un cambio en la cultura organizacional, sino también una adaptación exitosa a las nuevas dinámicas digitales.

Segundo, otro indicador esencial es el grado de integración y adopción de tecnologías digitales en nuestros procesos educativos. Esto no solo incluye la implementación de herramientas tecnológicas en la enseñanza y el aprendizaje, sino también la forma en que estas herramientas mejoran la experiencia educativa de los estudiantes y profesores. La medición del éxito en este ámbito se refleja en el aumento de la eficiencia operativa, la mejora en la calidad de la enseñanza y la satisfacción de los usuarios finales.

Emir Pernet

¿Cuáles considera usted que son los principales roles de los stakeholders en el proceso de transformación digital de una organización?

Alberto Cueto

Cada stakeholder tiene intereses personales particulares y únicos, legítimos, por los cuales estará luchando: poder, remuneración, reconocimiento, aprendizaje, ambiente social, crecimiento, por mencionar apenas algunos motivadores. Sin embargo, todos los stakeholders deben, desde su posición, trabajar para lograr el objetivo común, sin necesariamente renunciar a sus propios objetivos.

Stakeholders hay de distintas índoles. i) los patrocinadores, deben dar la orientación de los objetivos a lograr, a corto, mediano y largo plazo. Pero, sobre todo, con los objetivos establecidos, deben apoyar todo el proceso de cambio, especialmente en los elementos más complejos como es el cambio cultural, liderando con el ejemplo. La organización debe ser un lugar seguro donde se pueda aprender y equivocar, proponer y criticar. ii) los mandos medios, tienen el verdadero poder de lograr u obstaculizar el cambio.

Ellos deben estar alineados con la estrategia, y para ello deben ejercer un liderazgo positivo, permanente, para lograr el cambio. Es importante identificar los distintos tipos de motivación de los colaboradores, de tal manera que logre de cada uno de ellos lo mejor. iii) los colaboradores, alinear sus intereses con los de la empresa, dentro del ambiente seguro que se mencionó, fomentado por los patrocinadores y mandos medios, pero también conscientes de que la transformación sale de cada uno de ellos y no solo de los líderes organizacionales. En muchas situaciones los patrocinadores y mandos medios deben ser solo los instrumentos que permitan materializar las iniciativas que surjan de los colaboradores. iv) Los proveedores y contratistas, actuando como socios

comerciales y tecnológicos, dentro de un objetivo común. Por su posición, pueden tener un conocimiento especializado que no tiene la empresa, y que puede ser un gran catalizador para lograr la transformación.

Luis Puerto Y.
En el contexto de la transformación digital, los stakeholders juegan roles cruciales y diversificados. Para empezar, figuras como el Consejo Directivo y el Rector en una universidad son fundamentales. Estos líderes no solo deben tener una visión clara de las estrategias digitales, sino también la habilidad para comunicarlas efectivamente a toda la organización. Su rol implica no solo la formulación de la visión, sino también asegurar que esta se alinee con los objetivos de la organización.

Más allá de la alta dirección, otros stakeholders como los docentes, los estudiantes y el personal administrativo son igualmente importantes. Los estudiantes, como usuarios finales de estas transformaciones, son agentes clave en retroalimentar sobre la eficacia de las nuevas herramientas y prácticas implementadas. Su participación y feedback son cruciales para el éxito continuo de la transformación digital.

El proceso de transformación digital, cada stakeholder, desde la alta dirección hasta los usuarios finales, tiene un rol distintivo y complementario. La colaboración y comunicación efectiva entre estos grupos es esencial para asegurar que la transformación digital sea integral y alineada con la misión y visión de la organización.

Bogdan Djoric
El tema de los empleados es muy importante, es un factor clave. El CIO, líder de tecnología de una organización, se enfrenta a mucha complejidad hoy en día. Por un lado, tiene una tecnología que se queda vieja y obsoleta y no dispone del tiempo, el dinero ni el personal para mantenerla actualizada. Por otro lado, tiene el negocio que le demanda la transformación y su rápida ejecución. Además, tiene la exigencia de ser experto en ciberseguridad, las amenazas son cada vez más complejas, la inteligencia artificial juega un papel importante en ese campo; así como el talento.

Jeimy J. Cano M.
En el mundo hoy las juntas directivas y los equipos ejecutivos deben estar atentos a los desarrollos y retos globales. En este sentido, el escenario actual lo podríamos definir como cinco “p”s: polarización, populismo, postverdad, policrisis y permacrisis.

Emir Pernet
¿Cómo proceder si uno de sus aliados o socios tecnológicos estratégicos que soporta su ecosistema es víctima de un ciberataque con efectos en las iniciativas de su proceso de transformación digital?

Alberto Cueto

Ante todo, con tranquilidad y solidaridad. La organización debe haber trabajado la ciberseguridad integralmente, atendiendo los distintos frentes que ella requiere, incluyendo sus aliados y socios estratégicos. Para ello debe contar con planes de contingencia, teniendo claro qué hacer en distintos escenarios, incluyendo la falla de uno de sus aliados tecnológicos. En la medida en que dichos planes existan, y se tengan claras las acciones a seguir, será más sencillo salir de la crisis, porque se pensó y diseñó cuando la cabeza estaba fría y en sosiego, y no en medio de la crisis donde todo puede empeorarse por no actuar con serenidad.

Luis Puerto Y.

Primero, es esencial tener protocolos establecidos para responder a tales incidentes. Trabajamos activamente en desarrollar y fortalecer dichos protocolos, identificando áreas de mejora en nuestra preparación y respuesta a incidentes de seguridad.

Además, es crucial revisar y fortalecer nuestras políticas de gestión de riesgos y ciberseguridad. Esto implica asegurarnos de que nuestros socios tecnológicos como manos extendidas de nuestra operación cumplan con estándares rigurosos de ciberseguridad y realicen auditorías y evaluaciones periódicas. En caso de detectar deficiencias, tomamos medidas proactivas para mitigar los riesgos, incluyendo la revisión de contratos, la implementación de controles adicionales o la búsqueda de alternativas más seguras.

Finalmente, la comunicación abierta y transparente con los stakeholders es fundamental. En situaciones de ciberataques, mantener informados a nuestros colaboradores, empleados y usuarios sobre los impactos y las medidas tomadas es clave para mantener la confianza y la estabilidad en nuestro ecosistema digital.

Bogdan Djoric

Es un tema muy importante, yo no me considero un experto en seguridad, pero sí he aprendido mucho sobre ello, sobre todo de la gente especializada, de tener un buen equipo y de aliarme bien. Uno debe ser proactivo. Hay que autoevaluarse continuamente para ver dónde está la brecha y qué se puede

hacer para prevenir antes de que ocurra. ¿Qué pasa si hay un ciberataque? La ciberseguridad es un tema de negocio, si ocurre algo el que sufre es el negocio, si hay un costo reputacional es del negocio. Por eso hay que implicarlo mucho en estos asuntos.

Jeimy J. Cano M.
Una cosa importante adicional a lo que señala Luis es a propósito del reciente ciberataque de IFX que tuvo toda la visibilidad a nivel nacional. El problema de fondo es la cadena de suministro en dónde se ubica el tercero. No es lo mismo continuidad que resiliencia. Mientras la continuidad primero debe parar y luego reactivar, la resiliencia exige continuar operando a pesar de un evento exitoso.

Emir Pernet
¿Cuál es el mayor reto y la mayor oportunidad que encuentras en los procesos de transformación digital?

Alberto Cueto
Considero que el mayor reto, y al mismo tiempo la mayor oportunidad, es el cambio cultural, la incorporación efectiva de las personas en el cambio que requiere la transformación digital, lo cual requiere, como mencioné antes, una gestión de cambio efectiva. El cambio de *mindset* de todos los stakeholders, comenzando por los patrocinadores, siguiendo por los mandos medios, los socios o aliados comerciales y tecnológicos, y terminando (pero sin considerarlo una tarea menor) con los colaboradores, de tal manera que todos incorporen en su día a día, en su pensamiento, y sobre todo, en sus acciones, los ajustes requeridos para que la transformación digital trabaja en favor de la estrategia organizacional, del cliente o usuario, y de todas las personas involucradas.

Es un reto, porque el cambio cultural y de comportamiento es dificil y requiere tiempo y dedicación; es una oportunidad, porque permite que tanto la organización, como las personas detrás de la misma, crezcan personal y profesionalmente, si se hace adecuadamente.

Luis Puerto Y.
En mi perspectiva, el mayor reto en la transformación digital radica en la capacitación y el desarrollo de habilidades tecnológicas. La rápida evolución de la tecnología y las cambiantes necesidades del mercado requieren que tanto los empleados como la dirección estén constantemente actualizados y competentes en nuevas herramientas y metodologías. Este desafío se amplifica en entornos como el educativo, donde la brecha entre las habilidades existentes y las requeridas puede ser significativa.

Por otro lado, la mayor oportunidad que veo en la transformación digital es la posibilidad de democratizar el acceso a la educación. Las tecnologías digitales nos permiten supe-

rar barreras geográficas y económicas, brindando acceso a una educación de calidad a un espectro mucho más amplio de estudiantes. Este acceso ampliado no solo beneficia a los individuos, sino que es escalable a nivel país.

Bogdan Djoric

El desafío es afrontar todas las complejidades que se han mencionado. El gran desafío es navegar con todo esto. Seguramente la inteligencia artificial será un factor clave y diferencial en el futuro, ¡que está a la vuelta de la esquina!

Jeimy J. Cano M.

Estamos siempre expuestos a "olas indomables[1]", es decir a cambios radicales inesperados, por tanto el reto está en surfear, no podemos dominar la ola, pero si podemos montarnos en ellas para ver las oportunidades posibles y esto exige, entender aquellas tendencias que convergen de formas imprevistas.

[1] Brill, J. (2021). *Rogue Waves. Future-proof your business to survive & profit from radical change*. New York, USA: Mcgraw Hill.

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

Las juntas directivas y el riesgo cibernético

DOI: 10.29236/sistemas.n169a6

Fundamentos, áreas de riesgo y el proceso de duelo.

Resumen
En un escenario de tiempos posmodernos animados por complejidad, inestabilidad, inciertos y caos, los directorios de las empresas deben encontrar nuevas formas de mantener una vista actualizada sobre las diferentes tendencias y tensiones que marcan el ritmo de la dinámica internacional. En este sentido, el riesgo cibernético como responsabilidad ejecutiva surge como un nuevo reto sistémico que exige reconocer que no se conocen todos los riesgos y abrirse al proceso de construir nuevas reflexiones situadas en la promesa de valor de la organización, y desde allí avanzar en la gestión y gobierno de los ciberriesgos, como un compromiso corporativo con los diferentes grupos de interés para mantener una postura vigilante que habilite una organización más resiliente frente a amenazas cibernéticas. Este artículo, plantea algunas ideas básicas de esta relación naciente entre las juntas directivas y el ciberriesgo, como una excusa académica y práctica para acompañar a los directores en este reto inherente al desarrollo de los negocios en el contexto digital actual y futuro.

Palabras claves
Juntas directivas, Riesgo cibernético, Promesa de valor, Ciberataques, Duelo

Introducción

Los tiempos de inestabilidad y controversia que vive la humanidad establecen y definen nuevos desafíos para las organizaciones. Particularmente establecen retos novedosos para las juntas directivas, las cuales deben orientar y acompañar a la organización para establecer los nuevos rumbos estratégicos en medio de las tensiones, la incertidumbre y el caos propio de una realidad en tiempos posnormales (Sardar, 2010): con mayores complejidades sociales y organizativas a nivel político, económico, social, tecnológico, ambiental y legal.

En este sentido, los ejecutivos actuales deberán mantener una vista en la realidad actual, mientras exploran y actualizan el panorama de retos y riesgos de la empresa, el cual cambia de forma frecuente e inesperada, haciendo que los mejores pronósticos y ejercicios de actualización de sus mapas de ruta, queden obsoletos y muchas veces no respondan a las exigentes contradicciones y novedades del entorno.

Por tanto, no es la metodología que se use para mantenerse sintonizado con los cambios relevantes para el negocio, sino cómo la organización es lo suficientemente flexible y resiliente para aprender rápidamente y adaptarse a las transformaciones aceleradas del entorno. En consecuencia, los ejecutivos de primer nivel deben mantener calibrados sus sensores de la dinámica empresarial y retar sus saberes previos, para salirse de la zona cómoda de los riesgos conocidos y empezar a caminar y descubrir el desafío de tomar decisiones en medio de riesgos emergentes y algunas veces desconocidos (Agua, 2023).

En esta línea, recientemente los cuerpos directivos colegiados, denominados Juntas Directivas o Directorios, han recibido la noticia que ahora son responsables de la vigilancia y monitoreo de los riesgos cibernéticos. Un riesgo novedoso y distinto del riesgo de tecnología de información, que tratan de interpretar como algo tecnológico y cuya gestión le corresponde a los “técnicos”, sin percatarse que es un riesgo que atraviesa la esencia del negocio (interconexiones e interacciones de iniciativas digitales en todas las áreas de la empresa y sus clientes) y que requiere una visión sistémica e interdisciplinar para su adecuado tratamiento (Brinson & Briggs, 2023).

Así las cosas, es necesario visualizar este nuevo escenario de tensiones que genera el riesgo cibernético en las juntas directivas, para establecer orientaciones, alternativas y propuestas que permitan apoyar y acompañar a este cuerpo colegiado en su proceso de comprensión, apropiación y aceptación

de esta nueva responsabilidad (¿o no tan nueva?) con el fin de mejorar el nivel de madurez en la gestión y gobierno de los ciberriesgos, que habiliten a las empresas actuales para desplegar iniciativas innovadoras en sus procesos de transformación digital que cambien la forma de hacer las cosas y concreten nuevas experiencias en sus clientes (Cano, 2023).

En este sentido, este artículo inicia con una revisión de los fundamentos de las juntas directivas y su relación con el riesgo cibernético, para luego entrar en detalle en aquellas temáticas internacionales que son relevantes para dicho riesgo en las organizaciones. Seguidamente se explora el proceso de duelo que surge en estos cuerpos colegiados con ocasión de la responsabilidad que se les asigna a pesar de su poca experiencia y la negativa natural que surge, así como algunas ideas concretas para acompañarlos en este proceso. Finalmente se concluye con breves reflexiones que re-dondean las ideas planteadas a lo largo de este documento.

Fundamentos de las Juntas Directivas y el ciberriesgo

Las juntas directivas como cuerpos colegiados representan los órganos de gobierno naturales de las empresas (Calleja & Rovira, 2015).

Sus retos y responsabilidades implican condiciones particulares de sus participantes, que es necesario comprender y analizar con el fin de establecer puentes efectivos que permitan conversar y conectar en términos de sus intereses, exigencias y relaciones para hacer realidad la visión de una organización.

Por tanto, las juntas directivas cada vez más están expuestas a juicios de responsabilidad frente a eventos cibernéticos adversos que comprometan las operaciones de las organizaciones donde ellas operan, así como la promesa de valor para sus clientes. En este sentido, estos cuerpos colegiados deben desarrollar acciones concretas que les permitan mantener la confiabilidad, la vigilancia y la resiliencia de la organización en el contexto digital, como fundamento de su “debido cuidado” y demostración de su actuación deliberada y consciente frente a la inevitabilidad de la falla (Oktem, Pederson & Sallet, 2023).

En este escenario, los miembros de la junta deben asegurar que sus actuaciones son coherentes con esta realidad y dar cuenta de sus acciones respecto de estos eventos, para movilizar las acciones requeridas para proteger los intereses de la empresa y el cuidado de la imagen corporativa. Por consiguiente, cada miembro de la junta debe asegurar el cumplimiento de al menos cinco deberes (Frappolli, 2015, pp. 316-317) frente a la dinámica de las tensiones que provoca un ciberataque y las exigencias que la ciberseguridad demanda tanto para la organización como para sus ejecutivos de primer nivel:

- *Deber de cuidado*. Cada miembro de la junta debe mantenerse informado de los eventos y noticias relevantes sobre ciberseguridad o ciberataques, con el propósito de asegurar un tono adecuado de las discusiones en el contexto de los objetivos y estrategias de la organización.

- *Deber de lealtad*. Cada miembro de la junta no debe tener negocios o participar en negocios que compitan con la organización para la cual sirve, y más aún, comunicar situaciones adversas que conozca, las cuales afecten las condiciones de seguridad y control que tenga la empresa de la que es miembro en su directorio ejecutivo.

- *Deber de divulgación* (transparencia). Los miembros de la junta están obligados a revelar los hechos que son relevantes para los grupos de interés de la empresa para la cual trabajan. En particular, establecen el mecanismo y la estrategia que permiten dar cuenta de eventos desafortunados en ciberseguridad, con impactos en alguno de sus grupos de interés.

- *Deber de obediencia*. Los miembros de la junta deben ceñir sus actuaciones a la Constitución y la ley, así como frente a los fundamentos del gobierno corporativo. En otras palabras, asegurar las prácticas y los estándares requeridos para aumentar la resistencia de la empresa frente a ciberataques, así como motivar y apoyar comportamientos adecuados en el tratamiento de la información de la compañía.

- *Deber de verificación*. Los miembros de la junta deben contar con mecanismos para validar las acciones que sobre el tema de ciberseguridad se llevan a cabo en la empresa, motivar los planes de mejora que sean del caso y asegurar los recursos necesarios para incorporar las buenas prácticas en normativas, personas, procesos y tecnología.

Las juntas directivas y las áreas de riesgo cibernético

Los directorios comienzan a mantener en su radar las implicaciones y efectos nocivos de la materialización de los ataques cibernéticos. Las noticias permanentes de los impactos de los ciberataques en todo tipo de industria, así como las sanciones que revelan por cuenta de estos eventos, cada vez llaman la atención, no sólo por las posibles demandas o acciones legales que se puedan derivar, sino por el nivel de exposición que tiene la empresa a esta nueva realidad, que puede llevarla incluso a desaparecer del negocio (Myles, 2023).

En línea con lo anterior, la junta directiva debe mantener una visual de áreas clave susceptibles a los

riesgos cibernéticos, que puede concretar consecuencias adversas graves para dinámica empresarial. Las áreas donde se debe mantener el foco vigilante y sobremanera resiliente se ubican en:

- *Tensiones geopolíticas y cibernéticas globales y locales* - Para ello el equipo ejecutivo debe mantener y actualizar un diseño base de amenaza, que se traduzca en un análisis de escenarios posibles y probables de alto impacto.

- *Tratamiento de datos* – En esta temática el cuerpo colegiado debe asegurar un adecuado uso y explotación de datos con una visual de seguridad, privacidad y ética por defecto y desde el diseño.

- *Terceros de confianza* – La junta directiva deber conocer y asegurar la cadena de suministro y su relación con los objetivos del negocio para hacerla flexible, adaptable y resiliente frente a ciberataques.

- *Transformación digital* – El directorio debe definir y actualizar el apetito de riesgo corporativo frente a las iniciativas digitales estratégicas de la organización, para asegurar las capacidades cibernéticas necesarias para defender la promesa de valor de la empresa.

- *Cumplimiento normativo* – Los directores son particularmente sensibles al tema legal y normativo, por tanto deberán asegurar el cumplimiento de las exigencias de los reguladores locales e internacionales.

- *Brechas y vulnerabilidades* – Los miembros de junta deben comprender que no existe riesgo cero ni seguridad ciento por ciento. Por tanto, deben mantener una postura y protocolos concretos para atender una crisis cibernética, lo que exige desarrollar, ejecutar y aprender de simulaciones y ejercicios que revelen puntos ciegos en el modelo de seguridad y control de la organización.

Si bien pueden existir otras áreas que requieren atención frente al riesgo cibernético, las mencionadas previamente recogen las expectativas más sensibles y visibles de las organizaciones actuales, así como los efectos más adversos que pueden enfrentar las empresas y sus ejecutivos de primer nivel.

Por consiguiente, los equipos ejecutivos se sienten en una encrucijada que les genera tensiones y sentimientos encontrados, que se traducen en emociones y posturas que terminan generando rechazo y negación en la atención del riesgo cibernético y sus implicaciones empresariales.

Las junta directivas y el proceso de duelo frente a la responsabilidad del riesgo cibernético

Con el advenimiento de la formalización de las nuevas reglas de la Comisión del Mercado de Valores Norteamericano (SEC) sobre la ciberseguridad para las organizaciones que cotizan en bolsa donde entre otras normas se tienen: (Toscano, 2023)

- Notificar los incidentes de ciberseguridad importantes en un plazo de cuatro días laborables a partir de su detección y proporcionar actualizaciones periódicas sobre los incidentes de ciberseguridad notificados anteriormente.

- Divulgar las políticas y procedimientos mediante los cuales la organización identifica y gestiona los riesgos de ciberseguridad.

- Revelar cómo se consideran los riesgos cibernéticos como parte de la estrategia empresarial, la planificación financiera y la asignación de capital de la organización.

- Detallar la supervisión del riesgo cibernético por parte del consejo de administración, así como el papel de la dirección -y su experiencia- en la evaluación y gestión del riesgo cibernético y en la aplicación de políticas y procedimientos de ciberseguridad,las juntas directivas han entrado en tensiones y controversias comoquiera que estas nuevas responsabilidades (que no son tan nuevas) generan dinámicas distintas y exigencias que los cuerpos colegiados directivos no tienen en la actualidad, pues consideran que los temas de ciberseguridad son temas técnicos y procedimentales que no son de su nivel.

En este sentido, se podría decir que estos equipos viven un duelo, una pérdida irreparable que por exigencias de los supervisores deben ahora incorporar, muy a pesar de su negativa y posiblemente poca experiencia en el tratamiento de este tipo de riesgo de negocio en el contexto digital (Gorge, 2021).

De acuerdo con la psicología, "*la pérdida de cualquier objeto de apego provoca un duelo, si bien la intensidad y las características de éste pueden variar en gran medida en función del grado de vinculación emocional o de la propia naturaleza de la pérdida. Las pérdidas no siempre son físicas, sino que también pueden tener un carácter abstracto*" (Martin, 2019).

En este sentido, los directorios ejecutivos pierden la comodidad de su dinámica actual y conocida, para ser lanzados a entender, atender y asegurar un riesgo del cual poco se conoce y del cual poseen poca in-

formación, generando incertidumbre, dudas y miedos.

Para apoyar a los ejecutivos en su proceso de duelo, la literatura plantea dos alternativas para concretar el proceso cognitivo propio del estrés que esta nueva responsabilidad genera y las tensiones que puede suscitar en el ejercicio mismo de su función ejecutiva y directiva.

Lazarus y Folkman (1986) establecen dos modos de afrontamiento de la situación:

- *Dirigidos a la emoción* – regular las respuestas emocionales que surgen por causa del problema.

- *Dirigidos al problema* - buscar soluciones que reduzcan o desaparezcan el problema basado en un proceso analítico dirigido principalmente al entorno.

Una primera connotación del proceso de duelo de los directores frente al riesgo cibernético, el cual se percibe como una amenaza personal a su labor y posición ejecutiva, son las emociones que por lo general se producen entre las cuales se encuentran: *ansiedad*, *confusión* y *enojo*, las cuales surgen, entre otras, por la falta de conocimiento, información y manejo de una temática que resulta novedosa y que puede generarle afectaciones a su imagen, posición y capital político dentro y fuera de la organización.

Los ejecutivos de ciberseguridad frente este primer momento deben, con apoyo de un consultor externo, construir un entorno psicológicamente seguro, donde los directivos puedan liberarse de estas emociones y encontrar un escenario para poder preguntar sin temores, sin restricciones y de forma abierta, para conocer, explorar y aprender el tema, de tal forma que se liberen de sus propios miedos y se abran a construir en conjunto su propia versión de la temática situada en la realidad de la organización.

La segunda connotación para el tratamiento del duelo de los miembros de junta es trabajar dirigido al problema y los impactos que genera el asumir la responsabilidad del riesgo cibernético como son: *las sanciones*, *la pérdida de reputación* y *la pérdida de su posición*, las cuales se presentan por los efectos que se producen por cuenta de la materialización de un ciberataque, que termine no sólo afectando la dinámica de la empresa, sino comprometiendo datos sensibles y personales que generen grandes afectaciones a la corporación que sea referida a la falta de adecuada supervisión de dicho riesgo por cuenta de los miembros de junta.

Frente a esta forma de afrontamiento, los ejecutivos de ciberseguridad tienen una mayor participación comoquiera que demanda un proceso de compartir y conversar con los miembros de junta sobre los hechos y datos disponibles

en la compañía frente al tratamiento del riesgo cibernético. Esto es, construir, conversar y aprobar el nivel de apetito de riesgo de la empresa frente a dicho riesgos, desarrollar y desplegar el marco de debido cuidado necesario y establecer los acuerdos de nivel de protección que deberán ser supervisados de forma periódica e independiente, de tal manera que se interroguen todo el tiempo las capacidades de defensa y anticipación de la organización, así como la prácticas de protección y aseguramiento que tiene en la actualidad.

Reflexiones finales

El riesgo cibernético llegó a las organizaciones para generar incomodidad, incierto e inestabilidad, como una oportunidad para movilizar a las empresas de su zona cómoda y reconocer la nueva dinámica digital e interconectada de la sociedad y el mundo en general. Es el reconocimiento de los ecosistemas digitales de negocio tanto interno como externos para motivar transformaciones que cambien la dinámica de una industria y habiliten a las compañías para renovar y concretar ventajas competitivas en medio de zonas de inestabilidad y cambios permanentes (Woerner, Weill & Sebastian, 2022).

En este nuevo contexto, las juntas directivas deben actualizar su carta de navegación vigente y tradicional, basada en ejercicios de planeación estratégica y pronósticos de mercados en su sector de negocio, para reconocer una realidad cambiante, dinámica y exigente, que demanda una estrategia digital de las empresas, no sólo para acelerar sus iniciativas estratégicas, sino para tomar riesgos calculados que permitan cautivar a sus clientes y movilizar nuevas formas de monetizar el uso y explotación de los datos, consciente de la responsabilidad digital que implica ahora navegar en un entorno digital novedoso y particularmente volátil (Wucker, 2021).

Así las cosas, el riesgo cibernético se asoma y sitúa en la dinámica de la organización como un elemento intrínseco a su modelo de generación de valor, que es necesario comprender, atender y vigilar, comoquiera que se convierte en la piedra angular de las iniciativas que se van a desplegar en sus clientes, donde la confianza digital se revela como el referente natural de la relación de las compañías con sus consumidores. En este escenario, las juntas directivas deben conectar con esta nueva realidad, para asistir la empresa en el reto de aprovechar la oportunidad de una sociedad más digital e interconectadas (Brill, 2021).

El riesgo cibernético debe ser a las juntas directivas, como la promesa de valor de las empresas es a sus clientes. Esto es, una responsabilidad que se asume como parte natural e integral del compromiso del comprender, acompañar y responder a las expectativas y retos de los

consumidores cautivados por la manera que se provee de hacer las cosas de forma distinta. Por tanto, mientras se avanza en la solución del proceso de duelo de las juntas directivas frente a la responsabilidad del riesgo cibernético, es necesario avanzar en crear encuentros más constructivos y pedagógicos basados en un proceso cognitivo situado, para fundar las bases de un diálogo informado que haga del riesgo cibernético un reto para construir sinergias y no un juego de tensiones políticas.

Referencias

Agua, P. (2023). A Framework For Risk Governance. European Business Review. https://www.europeanbusinessreview.com/a-framework-for-risk-governance/

Brill, J. (2021). Rogue Waves. Future-proof your business to survive & profit from radical change. New York, USA: Mcgraw Hill

Brinson, R. & Briggs, R. (2023). Effective board governance of cyber security – A source of competitive advantage. Savanti Insight. https://info.savanti.co.uk/hubfs/Savanti%20Insight%20%20Effective%20Board%20Governance%20Of%20Cyber%20Security.pdf

Calleja, L. & Rovira, M. (2015). Gobierno institucional. La dirección colegiada. Navarra, España: EUNSA.

Cano, J. (2023). Maturity Model for Boards of Directors in Cyber Risk Governance. A Conceptual and Practical Proposal. En: Rocha, Á., Fajardo-Toro, C.H., Riola, J.M. (eds) Developments and Advances in Defense and Security. Smart Innovation, Systems and Technologies. Vol 328. 39–510. Springer, Singapore. https://doi.org/10.1007/978-981-19-7689-6_4

Frappolli, M. (2015). Managing cyber risk. Malvern, Pennsylvania. USA: American Institute for Chartered Property Casualty Underwriters.

Gorge, M. (2021). The cyber elephant in the boardroom. Cyber-accountability with the five pillars of security framework. Charleston, South Carolina, USA.: ForbesBooks.

Lazarus, R. & Folkman, S. (1986). Estrés y procesos cognitivos. España: Martínez Roca.

Martin, E. (2019). Las 5 fases (o etapas) del duelo: la teoría de Kübler-Ross. https://centrodepsicologiaintegral.com/las-5-fases-o-etapas-del-duelo-la-teoria-de-kubler-ross/

Myles, D. (2023). Waking up to cyber risks. FDI Intelligence. https://www.fdiintelligence.com/content/feature/waking-up-to-cyber-risks-83005

Oktem, C., Pederson, K. & Sallet, J. (2023). How boards can support resiliency in the face of constant crisis. EY Board Matters. https://shorturl.at/uHMO2

Sardar, Z. (2010). Welcome to postnormal times. Futures. 42(5). 435–444. doi:10.1016/j.futures.2009.11.028

Toscano, J. (2023). Final Decision On SEC's Cybersecurity Disclosure Rules Pushed To October. Forbes. https://www.forbes.com/sites/joetoscano1/2023/07/02/final-decision-on-secs-cybersecurity-disclosure-rules-pushed-to-october-2023/

Woerner, S., Weill, P. & Sebastian, I. (2022). Future ready. The four pathways to capturing digital value. Boston, MA. USA: Harvard Business Review Press

Wucker, M. (2021). *You are what you risk. The new art and science of navegating an uncertain world*. New York, USA: Pegasus Book

***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–.*

Madurez Digital

El rumbo estratégico de las empresas en la era tecnológica.

DOI: 10.29236/sistemas.n169a7

Resumen

La medición de la madurez digital es un mecanismo de diagnóstico organizacional moderno que le permite a las organizaciones definir estrategias de transformación digital orientadas a mejorar la competitividad y a desarrollar capacidades de adaptación y anticipación a los cambios del mercado y del entorno tecnológico. La madurez digital se puede definir como la manera "cómo las organizaciones se preparan sistemáticamente para adaptarse de manera consistente al cambio digital en curso" (Kane, 2017). Así mismo, se puede entender como la Integración de operaciones organizacionales y capital humano en procesos digitales y viceversa: procesos digitales en operaciones organizacionales y capital humano (Westerman et al., 2014). En este contexto, el concepto de madurez se refiere al grado en que la empresa ha integrado las nuevas tecnologías digitales en sus procesos y operaciones, siguiendo un enfoque sistemático y estructurado de monitoreo y transformación digital. El nivel de madurez digital influye directamente en la agilidad operativa de la organización, en la capacidad de adaptación al cambio digital del entorno, en su capacidad de innovación continúa basada en el uso de tecnologías digitales tanto emergentes como disruptivas, en la capacidad de respuesta a las demandas del mercado, y en la sostenibilidad.

Palabras Clave

Madurez digital, Transformación digital, Modelos de medición, Dimensiones de la madurez digital, Agilidad en la transformación digital.

Modelos de madurez digital y sus dimensiones

La medición de la madurez digital abarca diversos alcances, enfoques y modelos, motivados por la amplitud y diversidad de sectores que requieren atención desde lo digital. Por un lado, se encuentran los modelos propuestos por firmas consultoras reconocidas como KPMG, McKinsey, Boston Consulting Group, Accenture, Deloitte, PWC, entre otras. Por otro lado, surgen planteamientos fundamentados en la perspectiva de la OCDE y desarrollados a través de un enfoque de capacidades y funciones de las TIC (OECD, 2021). Desde la academia, también se plantean diversos modelos de madurez digital, por ejemplo, basados en capacidades digitales (el qué) y capacidades de liderazgo (el cómo), destinadas a evaluar la organización desde factores estratégicos, tácticos y operativo que entrelazan aspectos sociotécnicos en el contexto de la transformación digital (Bonnet & Westerman, 2020).

De acuerdo con la OCDE, los ejercicios de diagnóstico de madurez digital se basan en modelos generalmente de naturaleza descriptiva, sustentada en mediciones cuantitativas del nivel que perciben. Estos modelos no se prescriben de manera genérica ya que se enfocan en los procesos específicos de una organización y en los resultados generales de esos procesos, en tanto que no existe una talla única para todos ni un método detallado que deba ser preferido a otro en todas las circunstancias. Tampoco hay un juicio dentro de los modelos mismos sobre cuál es el nivel óptimo de madurez, esto dependerá de las propias circunstancias, objetivos y prioridades de la organización (OECD, 2021). En ese sentido, una organización que desee medir su nivel de madurez digital se enfrenta a tres escenarios posibles para consolidar su modelo de medición: (1) adoptar un modelo existente (por ejemplo, alguno de los mencionados de las empresas consultoras), (2) diseñar un modelo propio en donde la concepción, diseño, y despliegue del proceso es ad hoc, es decir, a la medida de las características de la organización, y (3) una mezcla de los dos escenarios anteriores.

En cualquiera de los escenarios, uno de los elementos fundamentales del proceso de medición es la identificación de las dimensiones y factores que permiten operativizar la medición. Los modelos de madurez digital consisten en dimensiones y criterios que describen áreas de acción y medidas en varios niveles, los cuales indican el camino de evolución hacia la madurez. Una dimensión es un componente específico, medible e independiente que refleja un aspecto importante, fundamental y distinto de la madurez digital y describe un

área de acción (Teichert, 2019). Existen múltiples dimensiones que se pueden integrar en un modelo de medición. La siguiente no es una lista exhaustiva, pero deja entrever la complejidad involucrada en el proceso de medición: cultura digital, tecnología, procesos y operaciones, estrategia digital, organización, habilidades digitales, innovación, información y experiencia del cliente, gobernanza, visión, ecosistemas, liderazgo, regulación y seguridad, productos y servicios, y modelo de negocio.

Cada dimensión puede desagregarse en una serie de factores que permiten abordar diferentes aspectos que conforman un área de acción particular. Por ejemplo, medir la dimensión de innovación puede requerir medir y analizar aspectos como las capacidades que permiten una forma de trabajo más flexible/ágil, el desarrollo de modelos comerciales disruptivos, el uso de métodos ágiles, el involucramiento del cliente en el proceso de innovación, la financiación de la innovación, la continuidad en la innovación, entre otros.

Tanto las dimensiones como sus respectivos factores convergen en un instrumento de evaluación que extrapola el modelo en un medio operativo de medición. Dicho instrumento contiene una escala de medición de madurez para cada componente, la cual permite cuantificar el resultado y luego clasificarlo, en una categoría de medición específica. Teniendo en cuenta los tres escenarios planteados anteriormente, la organización adoptará un instrumento de medición de referencia, diseñará uno propio (implica definir alcance, diseño, contenido, pruebas, despliegue, mantenimiento), o ajustará uno existente según sus necesidades.

Etapas de la madurez digital

Usualmente, los ejercicios de diagnóstico de madurez digital convergen en un sistema de clasificación que permite asociar un resultado articular con una categoría conceptual definida según el contexto, contenido y escenario de medición. Por ejemplo, desde la academia, Westerman et al. (2014) clasifica los resultados en cuatro categorías como son: principiante (Capacidades digitales y de liderazgo bajas.), conservador (Capacidades digitales bajas y capacidades de liderazgo altas.), fashionista (Capacidades digitales altas y capacidades de liderazgo bajas) y maestro (Capacidades digitales y de liderazgo bajas). Desde el escenario empresarial, Deloitte propone una clasificación en seis categorías, como son: rezagados (ausencia de habilidades digitales estratégicas y operativas), seguidores (con propósito de avanzar), operadores (enfocados en digitalizar los procesos centrales de la cadena de valor), innovadores (demuestra avances en negocios digitales), potenciales (enfocado en desarrollar una estrategia digital alienada a la operativa) y campeones (combinan es-

trategia y operaciones digitales de manera flexible y consistente)[1].

Enfoque de agilidad en la madurez digital

La agilidad significa ser capaz de adaptarse y/o anticiparse rápida y fácilmente a los cambios. Lo opuesto a ser ágil es ser rígido o inflexible (Leonard-Barton, 1992). Ignorar el cambio cuando ocurre es como enterrar la cabeza en la arena. Las características nucleares (categorizadas como conocimientos y habilidades, sistemas técnicos, sistemas de gestión, y valores y normas asociados a la creación de conocimiento), se solidifican en el tiempo y son distintivas, es decir, no pueden imitarse con facilidad y generan ventaja. Las rigideces, por su parte, dificultan el desarrollo de las acciones de transformación y de la evolución del ecosistema (Ortiz Pabón, 2023).

El enfoque de agilidad es una parte integral de la madurez digital. Existen tres atributos principales que caracterizan la agilidad: Velocidad, Enfoque y Flexibilidad (Perkin & Abraham, 2021). Cada atributo se correlaciona con los contextos claves del negocio: competitividad, clientes y organización. La velocidad indica el ritmo y progresión de la organización a través de la adopción, aplicación y/o adaptación de sus procesos desde el contexto digital. El enfoque busca generar el impulso organizacional necesario para que la transformación digital despegue, acelere y adquiera la cadencia suficiente para el cumplimiento de los objetivos y metas propuestos. Por su parte, la flexibilidad implica crear la cultura, el entorno y las estructuras para moverse rápidamente y con agilidad a través de la coordinación multidisciplinar, toma de decisiones, gobierno, análisis y entendimiento de los entornos productivos y colaborativos y una cultura digital caracterizada por el empoderamiento, la autonomía, el dominio y el propósito.

Cada elemento es esencial para la madurez digital. Sin velocidad se pierde el momento, sin enfoque se vuelve difuso el gobierno y la dirección, y sin flexibilidad se pierde el poder de adaptación. Dado que estos elementos fundamentales no se excluyen mutuamente, sino que son combinatorios al exponer los componentes esenciales del cambio, y de acuerdo con (Perkin & Abraham, 2021) se puede representar una fórmula de agilidad para la madurez digital de la universidad:

$$\text{Agilidad} = (\text{Velocidad} \times \text{Enfoque} \times \text{Flexibilidad})$$

Por supuesto, se pueden tener varias combinaciones de estos atributos, como se observa en la figura 1.

[1] https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Deloitte%20Digital%20Maturity%20Index-Survey%202022.pdf

	Enfoque	Flexibilidad	= Lento
Velocidad		Flexibilidad	= Despreocupado
Velocidad	Enfoque		= Sofocado
Velocidad	Enfoque	Flexibilidad	= Éxitoso

Figura 1
Fuente: (Perkin & Abraham, 2021)

Impulsores de la madurez digital

El propósito de transformar digitalmente una organización requiere el desarrollo de un conjunto amplio y diverso de activos y capacidades denominados impulsores digitales (Gurumurthy, R & Schatsky, D, 2019). Dichos impulsores tienen un mayor impacto cuando se ejecutan de manera conjunta, en lugar de desarrollarlos de manera selectiva. Por ejemplo, las fábricas de software desde comienzos de este milenio comenzaron a certificar sus procesos de desarrollo de software, lo que las llevó a generar una capacidad distintiva respecto a otros fabricantes y adoptaron el marco de referencia CMMI, un diferenciador que se comporta como un impulsor frente al mercado.

El mayor beneficio se puede obtener cuando las organizaciones aplican los impulsores ampliamente, en múltiples componentes del modelo de negocio, y con un alcance medido por la relevancia de la función de negocio impactada y el resultado esperado en términos de la generación de valor para el cliente. Los impulsores de la madurez digital incluyen: una Infraestructura flexible y segura, acciones estandarizadas de gestión y gobierno de datos, una mentalidad digital que permea toda la organización, el pensamiento ecosistémico digital, una manera inteligente de operación, la visión holística del cliente, y un modelo de negocio adaptable al mundo digital. Los impulsores digitales son necesarios, pero no suficientes, dado que existen otras condiciones intangibles de la madurez digital, como son la educación e innovación digital, el liderazgo, la cultura digital y la confianza, los cuales con factores contingentes a los impulsores mencionados.

Conclusión

La medición de la madurez digital se erige como un imperativo estratégico del proceso de transformación digital. Las empresas que no se adapten o anticipen al cambio del contexto digital, es decir, que no maduren digitalmente, corren el riesgo de quedar rezagadas y perder competitividad. Pensar y actuar sobre el proceso y en el producto de la maduración son aspectos fundamentales para la ruta de transformación digital. Modelos, dimensiones y enfoques de madurez son

insumos para el análisis de la madurez digital de una organización. La madurez digital se vuelve crucial para la competitividad en un entorno de negocios dinámico y complejo tecnológicamente.

Referencias

Bonnet, D., & Westerman, G. (2020). The New Elements of Digital Transformation. MIT Sloan Management Review, 62(2). https://sloanreview.mit.edu/article/the-new-elements-of-digital-transformation/

Gurumurthy, R & Schatsky, D. (2019). Pivoting to digital maturity: Seven capabilities central to digital transformation. Deloitte Insights.

Kane, G. C. (2017). Digital maturity, not digital transformation. MIT Sloan Management Review, 1.

Leonard-Barton, D. (1992). Core capabilities and core rigidities: A paradox in managing new product development. Strategic Management Journal, 13 (S1), 111-125. https://doi.org/10.1002/smj.4250131009

OECD. (2021). Digital Transformation Maturity Model. https://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/digital-transformation-maturity-model.htm

Ortiz Pabón, E. (2023). Ecosistemas de negocios, innovación y emprendimiento. Un marco de referencia y un caso de aplicación. Editorial Pontificia Universidad Javeriana. http://repository.javeriana.edu.co/handle/10554/65287

Perkin, N., & Abraham, P. (2021). Building the agile business through digital transformation. Kogan Page Publishers.

Teichert, R. (2019). Digital transformation maturity: A systematic review of literature. Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis.

Westerman, G., Bonnet, D., & McAfee, A. (2014). Leading Digital: Turning Technology Into Business Transformation. Harvard Business Press.

Néstor Armando Nova Arévalo *es Ingeniero de Control y Magister en Ingeniería Industrial de la Universidad Distrital Francisco José de Caldas y Doctor en Ingeniería de la Pontificia Universidad Javeriana en Colombia. Especializado en el diseño de sistemas de gestión de la información y del conocimiento. Cuenta con una amplia experiencia profesional, destacándose como profesor, investigador y consultor en diversas universidades de prestigio en Colombia además de ser profesor visitante en Purdue University en USA. Cuenta con experiencia como consultor en temas relacionados con la transformación y madurez digital de las organizaciones y el diseño y aceptación de tecnologías. Actualmente dirige programas corporativos de formación en ciencia de datos para empresas del sector salud, petróleo, financiero, entre otros. Su trayectoria académica incluye el liderazgo de cursos en áreas como la gestión y organización del conocimiento, gobierno de datos, e inteligencia de negocios. Además, ha sido autor de publicaciones destacadas en el ámbito de la gestión del conocimiento y ha participado en conferencias internacionales sobre business intelligence, madurez digital de las organizaciones, oportunidades desde la inteligencia artificial (IA) para la gestión del conocimiento.*

Open Source

Apalancador de la Transformación Digital

DOI: 10.29236/sistemas.n169a8

Resumen
El concepto de transformación implica un cambio en la manera de pensar, en la manera de hacer las cosas y por supuesto, en la manera como vivimos. Con la llegada de las tecnologías informáticas en siglo pasado y su adopción vertiginosa en los últimos 30 años, todos los aspectos de la sociedad se han visto afectados. La incorporación de nuevas tecnologías se debe realizar con una perspectiva optimista, donde el concepto de cambiar lleva a nuevas dinámicas que evolucionan las maneras como hacemos las cosas. Muchas de las tecnologías modernas, cuentan con comunidades que investigan, desarrollan y comparten el conocimiento bajo el concepto de código abierto o mejor conocido como "*open source*". Estos modelos de trabajo, casi filantrópicos, aportan a la innovación en general de la sociedad y es por esta razón que se articula muy bien con organizaciones que buscan en la transformación digital un apalancador para lograr el éxito.

Palabras clave
Transformación digital, Open Source, Innovación, Digitalización, Comunidad

Introducción

La Transformación Digital es el resultado de la incorporación de tecnologías informáticas en la sociedad. En el camino de adopción de tecnologías existen diferentes etapas, la conversión analógica-digital donde solo se toma ventaja de las características básicas de la digitalización de la información y las de rediseño de los procesos existentes para adoptar tecnologías informáticas, buscando optimizaciones de manera transversal. Las consecuencias de estos verdaderos procesos de rediseño se enmarcan en lo que hoy se llama Transformación Digital.

La transformación digital en los diferentes sectores

Dado que la transformación digital abarca todos los aspectos de la humanidad, podemos hablar de este fenómeno en diferentes contextos [1], entre los cuales encontramos los corporativos y los gubernamentales.

Sector corporativo

Casos muy conocidos por su trascendencia internacional como el desvanecimiento de “Blockbuster” [2] y “Kodak” son solo ejemplos con mucha resonancia que dan muestra de la evolución de todas las aristas de la economía y de la sociedad en un mundo que evoluciona de la mano de la tecnología. Revoluciones que se dan el sector de transporte con Uber, en hotelería con AirBnB, retail con Amazon, entretenimiento con Netflix, relacionamiento social con Facebook son solo ejemplos primarios de la evolución de la sociedad bajo una base tecnológica que permea todos los componentes de nuestras dinámicas individuales y colectivas.

Para algunas compañías, que hacen parte de negocios de tradición que vienen operando desde hace muchas décadas, la digitalización es solamente el punto de partida para procesos realmente transformadores, donde se catalizan verdaderas revoluciones cuando se incorporan nuevas tecnologías como la inteligencia artificial, realidad virtual, blockchain y el internet de las cosas, entre otras. En otros casos, con compañías que nacieron en un mundo completamente digital donde la dinámica es vertiginosa, la adopción de modelos de innovación puede darse de una manera más natural, sin embargo, estas empresas también están sujetas a estar repensando sus modelos de negocio frecuentemente.

Sectores gobierno

En muchos países existe una estrategia de gobierno electrónico o gobierno digital como se conoce en Colombia [3]. El común denominador de todos ellos es que se busca el aprovechamiento de las tecnologías informáticas para mejorar y

fortalecer la relación entre el ciudadano y el estado. Con esta política se crea un mandato a las entidades del estado, donde los procesos de transformación tienen un fin legítimo que a la postre redunda en beneficio para la sociedad, pues al conseguir eficiencias en el modo de operación del estado, se consigue una optimización en el uso de los recursos públicos, pudiendo aumentar no solamente cobertura, sino también la calidad.

Los gobiernos no deben subestimar nuevas tecnologías que sacuden el status quo de industrias consolidadas. Un ejemplo de ello son las criptomonedas basadas en tecnologías como Blockchain, que buscan la descentralización de la información y que hoy por hoy plantean alternativas muy interesantes de inversión a las ya existentes en el mundo financiero tradicional. Es por esto, que vienen en curso interesantes apuestas desde los gobiernos sobre estos nuevos escenarios financieros, con reglamentaciones que permiten contar con garantías y condiciones para estos nuevos actores. [4][5]

La relevancia de tecnologías como Blockchain en el marco del concepto de transformación digital radica en que con estas innovaciones se puede llegar incluso a cuestionar la existencia de algo que damos por cierto, como lo es, el valor y la generación misma del dinero [6]. Cuando estos conceptos revolucionarios tocan la puerta, vale la pena escucharlos, entenderlos y buscar la mejor manera de aprovecharlos. Esa es la esencia misma de la transformación digital.

El Open-Source como apalancador de la transformación digital

El desarrollo de tecnología se divide en dos. Por un lado, tenemos las tecnologías propietarias, de código cerrado, donde celosamente se cuida el código fuente con el que se genera las aplicaciones y lo que se comercializa es el derecho a su uso. Bajo este modelo, las oportunidades de evolución de la tecnología están limitadas a las personas que tienen acceso a este código fuente.

Por otro lado, tenemos las tecnologías de código abierto, donde todo el mundo tiene acceso al código fuente. Esta colaboración entre individuos anónimos enriquece la innovación y no se limita exclusivamente a que miembros de una misma organización puedan trabajar de forma simultánea en mejorar todos los aspectos de un mismo proyecto. Pensar que miles de individuos están trabajando en un solo proyecto puede sonar caótico, pero lo cierto es que al interior de cada proyecto open-source existe un modelo de cooperación y toda una organización para gestionar la madurez de las contribuciones. Cuando esto se escala, surgen organizaciones sin ánimo de lucro, que apoyan a los proyectos open-source, como por ejemplo el “Cloud Na-

tive Computing Foundation (CNCF)", que cuenta con más de 157 proyectos con más de 178.000 individuos realizando contribuciones a lo largo de 189 países. [7].

Cuando una compañía, en el marco de la transformación digital, decide dar el salto hacia la implementación de nuevas capacidades de negocio, apalancándose en tecnología, puede usar el open-source, pero para ello debe empezar a seleccionar hábilmente en cuáles proyectos debe prestar atención. En el caso del CNCF, se tiene acceso de manera libre, a una clasificación de cada uno de los proyectos por área de interés y también la calificación del nivel de madurez en el que se encuentra cada proyecto. Dentro de las distintas áreas de interés, encontramos categorías para Inteligencia Artificial [8], como "Machine learning", "Deep learning", "Distributed Computing" o para construcción de aplicaciones nativas de nube. [9].

Reflexiones finales

Hoy es obligatorio pensar en transformación digital no solamente como un proyecto que tiene un fin, sino también como un proceso de mejora continua, tal como el propuesto bajo el marco de kaizen [10]. Todos los días, surgen nuevas ideas, nuevos casos de uso sobre tecnologías emergentes, que pueden revitalizar las compañías, generando nuevas líneas de negocio o simplemente optimizando las existentes.

En los últimos años, se ha venido hablando mucho sobre el concepto de transformación digital, sin embargo, su aplicación e implementación en las organizaciones sigue siendo un reto. Su abordaje debe considerar aspectos como:

- Conocer tecnología. Una aproximación es contar con aliados estratégicos que estén monitoreando permanentemente los proyectos innovadores que surgen en las comunidades.
- Contar con la visión para aplicar nuevas tendencias tecnológicas de manera conveniente. La tecnología por sí misma no tiene valor. El valor aparece cuando se utiliza de manera apropiada para resolver una problemática.
- Diseñar una hoja de ruta que proporcione lineamientos claros y precisos. Contar con modelos continuos tipo kaizen son indispensables. Con cada mejora planteada, se pueden usar esquemas tipo lean-startup [11] que se fundamentan en el concepto de producto mínimo viable para realizar pruebas sobre las hipótesis planteadas.
- Gestionar el cambio para disminuir la resistencia al mismo, mediante un acompañamiento para mejorar la cultura de la orga-nización, permitiendo a los equipos involucrados ejecutar transiciones de una manera más sencilla.

El paso del mundo analógico al mundo digital le pasó factura a

todas aquellas empresas que no abrazaron la tecnología y que no tuvieron la visión de su negocio bajo un modelo digital. Conocer estas historias nos enriquece y nos permite ampliar la visión hacia futuras oleadas de nuevas tecnologías.

Referencias

[1] Mirzagayeva, Shamiya; Aslanov, Heydar (2022-12-15). "The digitalization process: what has it led to, and what can we expect in the future?" (PDF). Metafizika. 5 (4): 10–21. eISSN 2617-751X. ISSN 2616-6879. OCLC 1117709579. Archived from the original (PDF) on 2022-11-12. Retrieved 2022-10-14.

[2] MBA Knowledge Base. (2023). "Case Study: How Netflix Took Down Blockbuster". https://www.mbaknol.com/management-case-studies/case-study-how-netflix-took-down-blockbuster/

[3] Gobierno Digital, Ministerio de Tecnologías de la Información y las Comunicaciones, Colombia. (2023). https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/

[4]https://telecomunicaciones.uexternado.edu.co/legalidad-de-las-criptomonedas-avance-significativo-en-la-economia-digital-de-colombia/

[5] Dow Jones (2023). https://www.dowjones.com/professional/risk/glossary/cryptocurrency/us-eu-regulation/

[6] Penagos Bonilla, Daniel Andrés;(2022) "Tecnologías de la cuarta revolución industrial y su aplicación en la Armada Nacional de Colombia, Capitulo 10, Blockchain: conceptos y aplicaciones". ISBN 978-958-784-876-2

[7] Cloud Native Computing Foundation-Annual Report 2022. https://www.cncf.io/reports/cncf-annual-report-2022/

[8] Cloud Native Computing Foundation-LF AI & Data Foundation Interactive Landscape (2023) https://landscapeapp.cncf.io/lfai/

[9] Cloud Native Computing Foundation - Cloud Native Interactive Landscape (2023). https://landscape.cncf.io/

[10] Kaizen Institute. "Harnessing the Power of Digital Transformation". (2023) https://kaizen.com/insights/digital-transformation-failure-strategy-uk/

[11] Alonso, Maria, "Lean Startup: qué es y como implantarlo". (2023) https://asana.com/es/resources/lean-startup

***Daniel Andrés Penagos Bonilla**. Ingeniero de Sistemas de la Universidad Nacional de Colombia, con especialización en Construcción de Software y maestría en Arquitectura de TI de la Universidad de los Andes. Tiene más de 20 años de experiencia relacionada con desarrollo y arquitectura de software. Fue coautor del libro "Tecnologías de la Cuarta Revolución Industrial y su aplicación en la Armada Nacional de Colombia" y actualmente trabaja en Red Hat, donde tiene el rol de Senior Cloud Services Black Belt para Latinoamérica.*

AFILIATE
BENEFICIOS

- Inclusión en el gremio de Ingenieros de Sistemas más importante del país.
- Asesoría en trámite para la tarjeta profesional.
- Certificado de Miembro Profesional de la Asociación.
- Podrá escoger la participación en una de las Jornadas académicas organizada por ACIS sin costo adicional.
- Actualización en formación profesional y académica de manera constante.
- Descuentos especiales en cursos y eventos exclusivos en el área de las TIC.
- Pertenecer a los grupos de interés especializados en el sector (GI).
- Candidato a Director o CoDirector de Grupo de Interés (GI).
- Revista Sistemas (Publicación virtual Trimestral).
- Candidato a Miembro de Consejo Editorial de la Revista Sistemas.
- Asesoría en la edición de hojas de vida.
- Referencia profesional para empleos.
- Candidato a participación Profesional en proyectos de ACIS.
- Candidato a participar en eventos nacionales e internacionales como delegado de ACIS.
- Candidato a participar en Consultorías solicitadas a ACIS por entidades públicas o privadas.
- Referencia Profesional a Cargos Público Ejecutivo.
- Referencia Profesional para Miembro de la Junta Directiva ACIS o Externa.
- Referencia Profesional para Perito de Procesos de Arbitraje.
- Acceso diferido a la base de Webinars de ACIS. Consulte la Programación de Conferencias o YouTube
- Podrá tener su correo con @acis.org.co
- Acceso a Oportunidad laboral en nuestros portales Oferta de Empleo y Perfil de Ingenieros.
- Suscripción Anual.
- Descuento por Antigüedad.
- Descuento en Convenios.

ACIS

Más Información en:
www.acis.org.co
3015530540 - 3043463413

Para solicitar sus beneficios o afiliarse debe enviar un correo electrónico a suscripciones@acis.org.co