



# Riesgo cibernético y ciberseguros

*En la actualidad, las empresas en Colombia y en el mundo acogen la transformación digital como elemento crítico de supervivencia la inteligencia artificial se presenta como una de las invenciones más revolucionarias en la historia de la humanidad. Bajo este contexto, y en un mundo cada vez más conectado, las ciberamenazas emergen con el potencial de afectar economías enteras; desafortunadamente, los estudios indican que aún estamos lejos de gestionarlas de manera adecuada.*

**Carlos Varela**

Vicepresidente Técnico de Fasecolda de Fasecolda

## Baja resiliencia frente al riesgo cibernético

De acuerdo con el Foro Económico Mundial (FEM), la cuarta revolución industrial está impulsando rápidamente la transformación de todos los sectores de la economía; según sus estudios, en el 2022 se digitalizó cerca del 60% del PIB mundial, y el 70% del nuevo valor creado en la economía durante la próxima década se basará en plataformas habilitadas digitalmente. La transformación es inmensa y se está dando de manera vertiginosa. (DNP, 2019).

Esta transformación también es evidente en el ámbito local. La encuesta de *E-commerce* aplicada a 161 empresas afiliadas a la Asociación Nacional de Empresarios de Colombia (ANDI) revela que los empresarios colombianos reconocen la necesidad de adoptar una estrategia de transformación digital utilizando nuevas tecnologías e integrando herramientas digitales dentro de sus procesos. También reconocen que esta transformación llegó más rápido de lo esperado y sin previo aviso.

Esto representa un importante desafío. En una época en donde muchos empresarios locales enfrentan problemas de liquidez, también deben luchar por permanecer e identificar las oportunidades que les brinda la transformación digital para satisfacer las nuevas exigencias de sus clientes. (ANDI, 2020).

Tanto en Colombia como en el resto del mundo se identifican oportunidades, pero también los riesgos asociados. La encuesta global de ciberriesgo y seguros, realizada el año pasado por Munich Re, reporta que el 83% de los directivos encuestados estiman que sus compañías no están suficientemente protegidas contra las ciberamenazas (Munich Re, 2022).

En el ámbito local, la encuesta de la ANDI muestra que el 61,8% de las empresas contaría con alguna estrategia o acción de seguridad digital, sin embargo, llama la atención que solo el 6,3% cuenta con un área de seguridad de información dentro de la empresa.

➔ Cualquier empresa puede sufrir un evento cibernético incapacitante con el potencial de afectar a toda la cadena de suministro

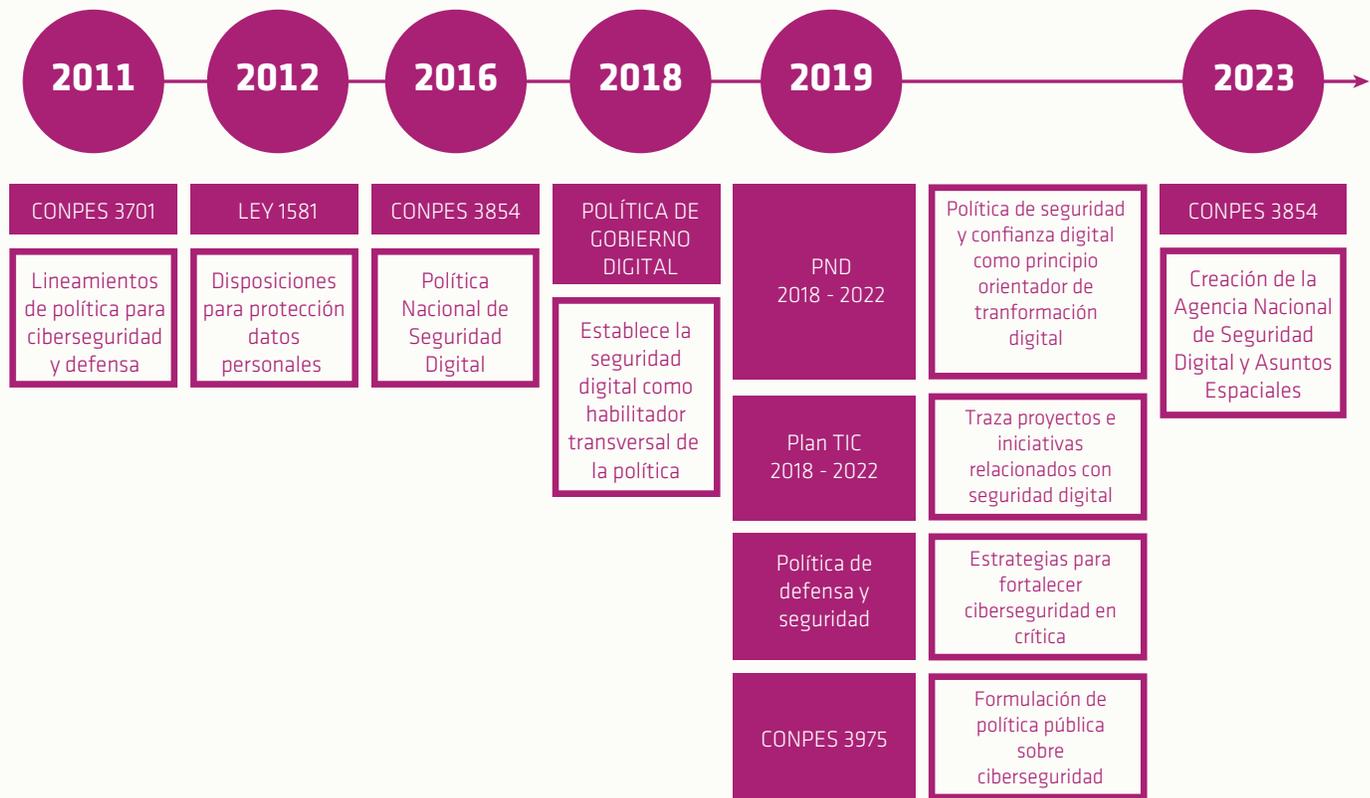
Estos datos permiten inferir un serio problema con la adecuada gestión del ciberriesgo. Cualquier empresa puede sufrir un evento cibernético incapacitante con el potencial de afectar a toda la cadena de suministro y la globalización complejiza aún más el problema. Generalmente, las empresas medianas y pequeñas son las más expuestas a los riesgos cibernéticos, porque pocas cuentan con la capacidad económica y el conocimiento para mitigarlos. Trabajar en aumentar la resiliencia cibernética es un deber de las economías para poder aprovechar la creación de valor que la transformación digital trae consigo.

## La política pública y la ciberseguridad

Las naciones deben estar preparadas para la transformación digital. No se trata solo de la adaptación de las diferentes entidades del Estado, que no son ajenas a los avances de la tecnología, sino de la responsabilidad que enfrentan los gobiernos de crear marcos normativos necesarios para que los actores económicos puedan interactuar y desarrollarse en esta nueva revolución tecnológica.

Colombia ha venido dando pasos importantes en la conformación de dicho marco normativo. Los primeros indicios de políticas para la ciberseguridad y defensa fueron establecidos en el año 2011, en el CONPES 3701. En el año 2012 se sancionó la Ley 1581, con disposiciones para la protección de datos personales, y en 2016 el CONPES 3854 estableció la Política Nacional de Seguridad Digital.

**Figura 1. Marco normativo para la seguridad digital en Colombia**



Desde entonces, los avances en materia de seguridad cibernética se han venido reforzando, muestra de ello es lo dispuesto en el Plan Nacional de Desarrollo 2018-2022 y en el CONPES 3975, este último centrado en la formulación de política pública sobre ciberseguridad (ver figura 1).

El desarrollo normativo más reciente está plasmado en el Plan Nacional de Desarrollo del Gobierno del presidente Gustavo Petro. En las bases de dicho plan se establece que el país debe contar con las suficientes capacidades para garantizar una adecuada y oportuna gestión de las amenazas cibernéticas, y crea la Agencia Nacional de Seguridad Digital y Asuntos Espaciales.

Dentro de esta agencia operará la Dirección Nacional de Seguridad Digital, que tendrá como objeto crear un

ecosistema digital confiable y seguro e implementar acciones para la protección del Estado en general. Esta dirección será la encargada de planificar, coordinar y articular las actividades que fomenten la preparación y la resiliencia del país, y de la generación de hábitos de uso seguro; además, establecerá las propuestas de elementos vinculantes que aseguren el actuar de las entidades del Estado ante posibles amenazas y riesgos de índole digital.

Adicionalmente, se definirá una estrategia para impulsar el concepto de «seguridad digital por defecto», para garantizar la continua prestación de los servicios ofrecidos por las entidades públicas y se establecerán los lineamientos técnicos para adoptar los estándares y buenas prácticas en el tema. (PND, 2023).

Contribuimos a la transformación de la industria con **programas a la medida** de las necesidades y desafíos del sector.

**AUTOESTUDIO**



**EXPERTO EN ANALÍTICA EN SEGUROS**

🕒 52 HORAS    🛒 \$885.500 SIN IVA  
USD \$263

**AUTOESTUDIO**



**EXPERTO EN MARKETING Y VENTAS EN SEGUROS**

🕒 147 HORAS    🛒 \$2.815.200 SIN IVA  
USD \$838

**AUTOESTUDIO**



**EXPERTO EN REASEGURO**

🕒 40 HORAS    🛒 \$931.500 SIN IVA  
USD \$277

**AUTOESTUDIO**



**EXPERTO EN RIESGOS, SUSCRIPCIÓN Y LIQUIDACIÓN DE SEGUROS**

🕒 106 HORAS    🛒 \$1.028.600 SIN IVA  
USD \$306

**AUTOESTUDIO**



**CONTABILIDAD DE SEGUROS Y ANÁLISIS FINANCIERO BAJO NIIF 4 Y NIIF 17**

🕒 70 HORAS    🛒 \$655.500 SIN IVA  
USD \$195

**AUTOESTUDIO**



**DIPLOMADO EN SEGUROS INTEGRAL - CIRCULAR 050**

🕒 180 HORAS    🛒 \$2.670.530 SIN IVA  
USD \$794

## AGENDA ACADÉMICA 2023

### SEPTIEMBRE

- ONLINE**
- DIPLOMADO NUEVAS TENDENCIAS DIGITALES Y HERRAMIENTAS ANALÍTICAS PARA EL SECTOR
- PRESENCIAL**
- CURSO PRÁCTICO EN SEGUROS GENERALES: MANEJO DEL RIESGO, SUSCRIPCIÓN Y RECLAMOS
- ONLINE**
- PROGRAMA PRÁCTICO EN HERRAMIENTAS DE DEGING THINKING EN EL SECTOR

### OCTUBRE

- ONLINE**
- SEMINARIO BÁSICO EN DATA ANALYTICS
- ONLINE**
- TENDENCIAS TECNOLÓGICAS Y SU IMPLICACIÓN EN LOS MODELOS DE NEGOCIO
- ONLINE**
- CURSO DE APLICACIÓN DE METODOLOGÍAS ÁGILES EN LAS ORGANIZACIONES

### NOVIEMBRE

- ONLINE**
- GESTIÓN DEL CAMBIO PARA LA ECONOMÍA DIGITAL
- ONLINE**
- ACTUARIA PARA NO ACTUARIOS
- ONLINE**
- ACTUALIZACIÓN EN SEGUROS DECENAL: UNA VISIÓN TÉCNICO JURÍDICA

### DICIEMBRE

- ONLINE**
- COMPORTAMIENTO DEL CONSUMIDOR Y SEGMENTACIÓN DE CLIENTES
- PRESENCIAL**
- CURSO ESPECIALIZADO DE SUSCRIPCIÓN DE PÓLIZAS DE SEGURO DE CUMPLIMIENTO

Con el respaldo de **fasecolda**  
Federación de Aseguradores Colombianos

### Más Información e Inscripciones

📞 (57-1) 318 5175671 - 317 367 5060  
✉ mercadeoins4@fasecolda.com  
✉ mercadeoins3@fasecolda.com



[www.ins.edu.co](http://www.ins.edu.co)

 INSFasecolda     InsOficial     Instituto Nacional de Seguros - Fasecolda



## El rol de los seguros

En los últimos años, las empresas han venido incrementado su demanda de seguridad cibernética y de protección a través del seguro. Munich Re estima que las primas globales de esta cobertura en 2022 fueron del orden de USD 9 billones y se espera que alcance los USD 25 billones en 2025. Un incremento esperado del 178% en tan solo tres años.

Estas cifras señalan una gran oportunidad para el sector asegurador, sin embargo, también representan un enorme reto. Por un lado, está la baja resiliencia de las empresas y, por el otro, la falta de comunicación al interior y entre diferentes cadenas de suministro, que complejizan la medición del riesgo.

El documento Global Cybersecurity Outlook 2023, del Foro Económico Mundial, advierte que las organizaciones pequeñas tienen más probabilidades de no contar con una cobertura de este tipo (48%), en comparación con empresas grandes (16%). Hay varias razones que explican este comportamiento: muchos empresarios desconocen la forma en que opera la cobertura, se ha identificado que no hay suficientes profesionales capacitados en el campo del ciberriesgo y su gestión, algunos directivos aún no logran comprender el riesgo al que pueden estar sometidos y, por supuesto, la ciberseguridad implica costos que no todas las empresas pueden enfrentar. (World Economic Forum, 2023)

En consecuencia, el asesoramiento y acompañamiento de las aseguradoras a sus clientes adquiere una dimensión relevante para este riesgo, ya sea a través de acciones individuales o mediante proyectos colectivos, como los que pueden brindar las asociaciones o el trabajo articulado con los gobiernos. Se convierte en tarea obligada coadyuvar a las organizaciones a mejorar la resiliencia cibernética de sus operaciones y, así, aumentar el nivel de protección en las cadenas de suministro.

## La tarea en el ámbito local

Colombia se encuentra en la dirección correcta para la creación de una resiliencia cibernética en los niveles macro-, meso- y micro-, y el trabajo del sector privado se suma a la creación de los marcos normativos. Gremios como la ANDI han venido trabajando de manera intensa con sus afiliados para conocer el estado en que están en el proceso de transformación digital. Por esta razón, Fasecolda ha iniciado un acercamiento a esta entidad, con el propósito de dar a conocer los conceptos de ciberseguridad, gestión del riesgo y seguros cibernéticos. Se ha planteado a las áreas técnicas de la agremiación la necesidad de crear una sinergia que tenga como propósito ayudar a los empresarios, grandes y pequeños, del país a gestionar de manera adecuada el riesgo cibernético y a conocer las opciones de transferencia que les ofrece el mercado asegurador.

Una idea que ha propuesto Fasecolda, y que se está trabajando con las vicepresidencias de Transformación Digital y de Desarrollo Económico y Competitividad de la ANDI, es replicar la encuesta de Munich Re para el país; esto permitiría establecer una línea base que ayudaría a ambos gremios a identificar, con mayor claridad, las acciones que sus afiliados deben adelantar para mejorar la gestión del riesgo cibernético. La sugerencia facilitaría, a su vez, el diseño de soluciones de transferencia de mayor profundidad, a través del seguro.

La realización de la citada encuesta es una de varias opciones que estudian estos gremios, sin embargo, los

→ Colombia se encuentra en la dirección correcta para la creación de una resiliencia cibernética en todos los niveles

acercamientos han dejado claro a ambos sectores la conveniencia de trabajar de manera conjunta para facilitar la transformación digital a la que se requiere migrar.

Otra tarea de importancia mayor para el sector asegurador será la activa participación en las instancias que ha creado el Gobierno nacional, para la implementación de los marcos normativos que permitan aumentar la resiliencia del país ante las ciberamenazas. En este sentido, es prioritario el acercamiento a la Agencia Nacional de Seguridad Digital y Asuntos Espaciales, tan pronto como se establezca, al Ministerio de las TIC y al área de ciberseguridad de la Policía Nacional, entre otros.

Debemos ser conscientes de que la transformación digital que requiere nuestra economía no podría ser completa sin una adecuada transferencia de los riesgos a través de los seguros, y que debemos ser protagonistas activos en este cambio. 

## Referencias

ANDI. (2020). *Según encuesta de la ANDI, comercio electrónico ha tomado fuerza significativa en la actual coyuntura.*

<https://www.andi.com.co/Home/Noticia/15757-segun-encuesta-de-la-andi-comercio-elec>

DNP. (2019). CONPES 3975.

Munich Re. (2022). *Global Cyber Risk and Insurance Survey.*

PND. (2023). *Bases Plan Nacional de Desarrollo 2022-2026.*

World Economic Forum. (2023). *Global Cybersecurity Outlook.*