Universidad Internacional de La Rioja

Facultad de Derecho

Máster Universitario en Derecho Digital

Retos de la ciberseguridad en el sector empresarial de España y Colombia, un análisis comparado.

Trabajo fin de estudio presentado por:	Yudy Enerieth Garay Bernal
Tipo de trabajo:	Trabajo Fin de Master
Utilizar si se necesita alguna tipología más:	TFM
Director/a:	Enrique Ortega Burgos
Fecha:	05-01-2024

Resumen

Aunque la ciberseguridad tiene sus raíces en los años 50, cuando surgieron las primeras redes informáticas y se expandieron las tecnologías de la información, sus desafíos son constantes y cambiantes, en este momento, controlar la ciberdelincuencia es un reto incesante debido a la rápida adopción de internet y la transformación digital casi obligatoria, por lo que tener claramente reglado como usar y explotar el mundo digital es inminentemente necesario, esto con mayor relevancia en el sector empresarial en donde los activos son el núcleo esencial de la producción, por lo que su protección merece total atención.

Palabras clave:

- Ciberdelincuencia
- Ciberseguridad
- Información
- Cumplimiento
- Empresa

Abstract

Although cybersecurity has its roots in the 50s, when the first computer networks emerged and information technologies expanded, its challenges are incessant and evolving. At this time, controlling cybercrime is a relentless challenge due to the rapid adoption of the internet, and the almost mandatory digital transformation, so having clearly regulated how to use and exploit the digital world is imminently necessary. This necessity is particularly noteworthy in the business sector, where assets serve as the linchpin of production, warranting dedicated attention to their protection.

Keywords:

- Cybercrime
- Cybersecurity
- Information
- Compliance
- Enterprise

Índice de contenidos

Índice de figuras

Índice de tablas

1. Introducción

El aumento del uso de tecnologías de la información ha dado lugar a un aumento significativo de actividades maliciosas cibernéticas en diversos contextos. En la actualidad, la adopción masiva de la tecnología está transformando todos los sectores económicos; impulsando la evolución de productos, acelerando la prestación de servicios, resolviendo necesidades previamente inimaginables, reduciendo tamaños y tiempos de desarrollo, así como abriendo nuevos mercados. Estos avances también presentan objetivos claros para amenazas cibernéticas, con la posibilidad de ser materializados por diferentes actores malintencionados.

A pesar del progreso global, los incidentes cibernéticos han surgido de manera única y especial en cada país, reflejando el nivel de avance tecnológico de cada población. El análisis realizado en este documento busca identificar algunas habilidades y debilidades de los países estudiados, así como las contiendas que enfrenta el sector empresarial en materia de ciberseguridad.

Se examinarán las medidas implementadas a nivel nacional (Colombia-España) para mitigar la delincuencia cibernética. Este análisis proporcionará una comprensión de los compromisos de ambos países en ciberseguridad, identificará lagunas normativas y ofrecerá información valiosa para que el sector empresarial fortalezca sus estructuras de ciberseguridad.

Aunque existen diferencias significativas en las regulaciones y medidas preventivas entre Colombia y España, su proximidad como Estados Miembros de las Naciones Unidas ha acortado esa brecha. La necesidad global de utilizar tecnologías digitales para alcanzar los Objetivos de Desarrollo Sostenible (ODS) ha unido a estos países en un llamado universal para suprimir la pobreza, proteger el mundo y mejorar las condiciones de vida a nivel universal (MINISTERIO DE RELACIONES EXTERIORES 2016).

En 2020, España ocupó el cuarto lugar a nivel mundial en el Global Cybersecurity Index, una medida confiable del compromiso de los países con la ciberseguridad. Este índice, que otorgó a España una puntuación de 98.52 sobre 100, tiene como propósito fundar conciencia sobre la trascendencia y las múltiples dimensiones de este problema (SAN JOSE 2021).

En contraste, en ese mismo periodo, Colombia no recibió reconocimientos y por el contrario experimentó un aumento del 84% en la ciberdelincuencia, según el Ministerio de Justicia. Sin embargo, la intensificación del uso de tecnologías de la información, impulsado, por ejemplo, por los “Días sin IVA” establecidos por el Gobierno Nacional durante la emergencia sanitaria

de la COVID-19, llevó a la administración a reconocer la necesidad de regular de manera preventiva y correctiva la ciberdelincuencia en el ámbito empresarial.

1.1 justificación del tema elegido

¿Por qué abordar la regulación de la ciberseguridad y sus desafíos en las empresas de España y Colombia? Para comenzar, nos permite identificar los riesgos clave y las necesidades de controles o recomendaciones para reducir la exposición de las empresas a las tácticas cambiantes de la ciberdelincuencia. El término "tácticas cambiantes" se refiere a las formas de llevar a cabo dichos ciberataques, y aunque estas no sean completamente novedosas, observamos una evolución en los métodos de operación, lo cual dificulta hacerles frente a estos hechos. Por otra parte, explorar este tema tiene el propósito de destacar las diferencias en los desafíos normativos del sector empresarial en cada una de las naciones estudiadas.

1.2 problema y finalidad del trabajo

El problema plateado abarca la necesidad de identificar las debilidades y/o vacíos normativos de la ciberseguridad en Colombia y España, para lograr establecer propuestas de futuras leyes, políticas y procedimientos que contribuyan al fortalecimiento de la ciberseguridad en el sector empresarial de los países ya mencionados.

1.3 objetivos

Objetivo General:

Avistar gran parte de los retos normativos en materia de ciberseguridad particulares para España y Colombia.

Objetivos Específicos:

- Realizar un análisis comparativo que refleje claramente mínimo tres diferencias existentes en materia de ciberseguridad en el sector empresarial de cada país (España y Colombia) en procedimientos y en normatividad.
- Identificar dos (02) propuestas para futuras leyes, políticas o lineamientos que contribuyan al fortalecimiento de la ciberseguridad en el sector empresarial de España**.**
- Identificar dos (02) propuestas para futuras leyes, políticas o lineamientos que contribuyan al fortalecimiento de la ciberseguridad en el sector empresarial de Colombia.

2. Ciberseguridad: concepto y aspectos relevantes actuales.

Los activos de una empresa, que incluyen bienes, recursos y derechos, representan beneficios valiosos para cada organización y aunque no todos tengan la misma importancia en términos de funcionamiento, liquidez y rendimiento, todos contribuyen en materia de indicadores. Entendiendo este contexto es importante tener claro cómo se puede lograr la protección de dichos activos, por lo que resulta esencial diferenciar la seguridad de la información del concepto de ciberseguridad: La seguridad de la información actúa como una capa de protección para diversos tipos de datos frente a posibles incidentes, mientras que la ciberseguridad se centra en la defensa de computadoras, software, hardware, sistemas electrónicos, redes y datos mediante tecnologías o prácticas ofensivas contra los delitos cibernéticos.

Para el entendimiento de este texto, consideraremos como base de este escrito el concepto de ciberseguridad, entendido como el área de las ciencias de la computación administradora del desarrollo y ejecución de las herramientas o artilugios capaces de proteger la información y la infraestructura tecnológica.

Ahora, el concepto de "delito cibernético" es un término amplio, que comprende escenarios en los que, el componente informático, se halla en el objeto de la actuación penal y también en aquellas en que tal mecanismo es el recurso para ejecutar un objetivo ilícito. De esta manera, el anterior concepto abarca delitos habituales que se perpetran mediante el uso de herramientas informáticas, así como nuevos delitos, que se logran consumar gracias a la existencia de tales recursos (CAVADA HERRERA 2020).

El 2 de noviembre de 1988, se produjo el primer incidente significativo de malware con el ataque del Gusano de Morris, creado por el programador Robert Tappan Morris. Este ataque afectó 6000 servidores, lo que representó el 10% de las máquinas conectadas a la red en ese momento. El Gusano de Morris se propagaba y rebotaba entre equipos, ralentizando e incluso dañando los ordenadores afectados. La magnitud del impacto fue tan notable que incluso afectó al centro de investigación de la NASA.

Tras el correr de los años, y en aras de realizar un análisis más actual, encontramos que, para el 2018 varios autores establecieron el reto y la necesidad de contar con la capacitación y experticia absoluta de la fuerza armada y de los entes judiciales, para que se pudiera disponer de apoyo técnico, mecanismos de investigación y de mejores instrumentos legislativos que

logren ponerle el pecho a la delincuencia informática (ANGUITA OSUNA 2018), pues si bien, la ciberdelincuencia es una problemática que afecta a todos los usuarios de internet, es precisamente el sector corporativo el más perjudicado a nivel económico. Tenemos, por ejemplo, el ciberataque de malware "NotPetya" de 2017, calificado como uno de los más dañinos pues conllevó a un detrimento de más de 10.000 millones de dólares para la multinacional de mensajería FedEx Corp. (BOLLERO 2022).

Dos años más tarde, el 12 de noviembre de 2019, se estrenó el servicio de streaming de propiedad de The Walt Disney Company, DISNEY+, y con ello llegó un robo de credenciales de cuentas masivo, pues apenas unas horas después del lanzamiento del servicio, los piratas informáticos vendían cuentas de Disney+ por tan solo 3 dólares (£ 2,30), cuando una suscripción al servicio costaba 7 dólares (£ 5,40) al mes (EL ECONOMISTA 2019).

Para el 2020, la actividad online se aceleró de manera exponencial derivado del confinamiento y aislamiento por la pandemia Covid-19, lo que originó una importante reflexión respecto de los usos de las tecnologías de la información y sus consecuencias. Los afectados por los distintos ciberataques fueron muchos, llegando la afectación a los más impensables sectores y entidades, casos como el de Joseph James O'Connor conocido como "Plugwalk Joe" condenado en febrero de 2023 por estafa con criptomonedas y SIM swapping quién manipulo las cuentas de Twitter de Elon Musk, Bill Gates y Barack Obama, mediante las cuales, prometía duplicar el monto de los bitcoins recibidos, fueron realmente relevantes (LA NACION 2023).

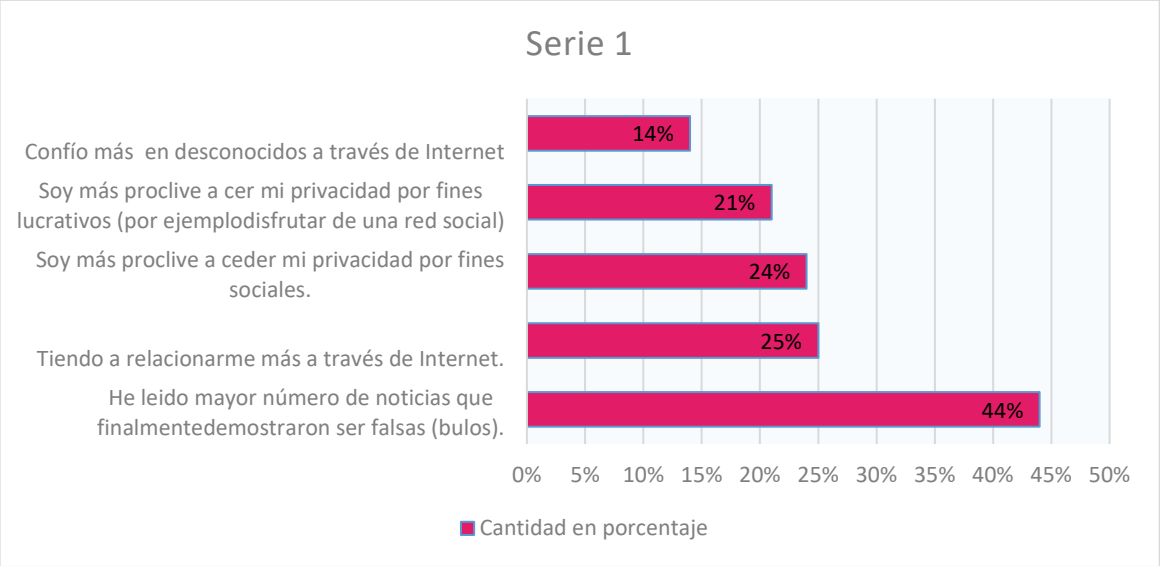

Figura 1."Percepción sobre los hábitos adquiridos tras el confinamiento o motivado por la pandemia" (OBSERVACIBER)

En el segundo semestre 2023, nos enfrentamos a un concepto mucho más amplio, temeroso y exigente: el llamado Metaverso, que nos obliga a exponernos a un universo digital expandido. El Metaverso no es otra cosa que un mundo paralelo que tendrá sus propias cláusulas y disposiciones, ofreciendo un sin número de actividades a través de la inteligencia artificial (IA), la realidad virtual (RV) y la realidad aumentada (RA).

Pero para llegar al tan anhelado Metaverso, el mundo ha transitado por una cadena de etapas interesantes, fructíferas y retadoras. Autores como García Linares nos recuerda que vivimos en una tercera generación del internet, pasando, por 1991 con la publicación del primer sitio web alojado en http://info.cern.ch/hypertext/WWW/TheProject.htm que tenia por fin la recuperación de información de área amplia y el brindar acceso universal a un gran universo de documentos. La segunda generación está ubicada en el periodo comprendido entre 2004 y 2005, vigencias para las cuales se crearon las redes sociales Facebook y YouTube, pues si bien para 1997 se conoció la primera red social denominada “SixDegrees” esta cerró en 2001 por su baja rentabilidad. Como ya se dijo, en la actualidad nos encontramos ubicados en la tercera generación que traza experiencias más profundas, donde los dispositivos de conexión ya no serán solo ordenadores o celulares, sino que se usarán prácticamente como indumentaria, allí están los gadgets, lentes, audífonos, cascos, que nos van a permitir vivir digitalmente. (GARCÍA LINARES 2022)

2.1 Contexto español, desde lo normativo a lo real empresarial

El marco regulatorio de ciberseguridad en España es amplio y robusto, dividido en ocho grandes capítulos que abarcan desde aspectos ontológicos hasta prácticas sociales. Estos capítulos incluyen: **i)** la Constitución, **ii)** la normativa de seguridad nacional, **iii)** infraestructuras críticas, **iv)** seguridad en general, **v)** unidad de atención a incidentes de seguridad, **vi)** telecomunicaciones y usuarios, **vii)** ciberdelincuencia, **viii)** protección de datos y proximidades con la administración.

Desde 1978, la Constitución Española ha garantizado derechos fundamentales que sirven de base para la protección del ámbito digital y la ciberseguridad. Actualmente, estos derechos abarcan el acceso universal a Internet, la libertad de expresión, comunicación e información, la privacidad y protección de datos, el derecho al olvido y otros derechos conexos.

España hace parte del Convenio de Budapest, alianza que se constituye como el primer tratado internacional que aborda los ciberdelitos, ratificado en octubre de 2010. La firma de

esta ratificación en 2010 condujo a la reforma del Código Penal apenas en 2015, que tipificó diversos cibercrímenes, como el acceso no autorizado a sistemas informáticos. En 2015, debido a desafíos identificados para la Seguridad Nacional, se abordó la necesidad de hablar sobre el Sistema de Seguridad Nacional y la gestión de crisis, ambos constituyen conjuntos de acciones destinadas a detectar y evaluar riesgos y amenazas, asegurando una solución favorable y sistematizada de los recursos del Estado.

Dicho lo anterior, desde 2015, se empieza a realizar un análisis en la Unión Europea sobre datos personales, ámbito especialmente sensible, pues es que incluso desde antes de nacer ya muchos están poniendo en exposición su información, a través de la publicación de estudios prenatales o ecografías, se debe resaltar, por ejemplo, que el 81% de los niños con menos de dos años tienen presencia en Internet y el 5% tiene su propio perfil en una red social (GARRIGA DOMÍNGUEZ 2016).

El manejo de información personal en el mundo es una situación imposible de evitar, ya que está inmersa en todo tipo de actividades del diario vivir y a otras de entretenimiento que se han vuelto parte de miles de estilos de vida. Las principales compañías que operan en Internet procesan miles de petabytes de datos al año, por ejemplo, Google procesa más de 24 petabytes de datos al día, mientras que en Facebook se suben fotos nuevas cada segundo para casi un total de 10 millones cada hora y ni hablar de los videos. YouTube por su lado cuenta con alrededor de 1.000 millones de consumidores mensuales y WhatsApp ha derrotado la barrera de los 800 millones de consumidores activos mensuales. Obviamente todos esos millones de usuarios generan enormes cantidades de datos (GARRIGA DOMÍNGUEZ 2016).

Por ello, es que muchos autores hablan de esta era como la de los grandes datos y de lo increíble que los mismos se han convertido en un insumo valioso con valoración tanto económica como social, produciéndose en la minería y análisis de datos un acrecentamiento intensivo de la capacidad informática de almacenamiento y procesamiento de estos, con una tendencia además de compartir y no proteger, pues la afición de los usuarios por el empleo de las redes sociales, cada día es más exponencial desde el contexto de la intimidad (ARROYO GUARDEÑO, MARTINEZ, GAYOSO y HERNÁNDEZ ENCINAS 2020).

Ahora, para mitigar cualquier tipo de vulneración a dichos datos, y a los derechos de su protección, en vigencia 2018 se expidió la Ley Orgánica 3, que tiene por finalidad adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo, relativo a la protección del derecho fundamental de las personas naturales, a la protección de datos

personales, y a brindar garantías referentes al uso de herramientas digitales para la población acorde al precepto establecido en el artículo 18.4 de la Constitución.

En dicha línea, en el 20 de febrero del 2019 se expidió la ley 01, mediante la cual, se dan criterios y estructuras para lograr una seguridad jurídica que contribuya a eliminar los manejos desleales que se enfocan en el apoderamiento indebido de secretos empresariales y que por el contrario se aumente el valor de las innovaciones que las empresas tratan de resguardar como secretos empresariales.

En la misma vigencia (2019) el Gobierno Español expidió su Estrategia Nacional de Bioseguridad, época en la cual no se tenía concebido el resultado que generaría la pandemia COVID 19. En dicho documento está establecido de manera clara que el ciberespacio se ordena como un campo de batalla donde la información y la privacidad de los datos son activos de importante coste y que la progresiva conectividad para este país y la sumisión de redes y sistemas generan importantes vulnerabilidades, dificultando la apropiada protección de la información.

Para el 2020, mediante el Real Decreto 734 de 4 de agosto de 2020, que despliega la ordenación armónica principal del Ministerio del Interior, se entrega como facultad a la Dirección General de Coordinación y Estudios, el desplegar mediante la Oficina de Coordinación de Ciberseguridad[1], las tareas de acercamiento nacional de coordinación operante para el canje de información con la Comisión Europea y los Estados partes, en el cerco de lo determinado por la Directiva 2013/40/UE, dicho cuerpo colegiado se hace reconocido en el sector empresarial pues elabora habitualmente estadísticas de criminalidad, coordina y evalúa operaciones y sistemas frecuentes encauzados a la protección de grupos en estado de vulnerabilidad, y de las infraestructuras críticas y fomenta la participación y colaboración entre instituciones públicas y privadas para generar estudios y análisis sobre temáticas relacionadas con la política de seguridad y la seguridad ciudadana.

En 2021 el Consejo de Ministros aprobó la nueva Estrategia de Seguridad Nacional (ESN) en la cual se reconoce la importancia de fortalecer el multilateralismo para hacer frente a las problemáticas de la ciberseguridad a nivel mundial que incluye además la necesidad de la

[1] La Oficina de Coordinación de Ciberseguridad (OCC) es el organanismo técnico que tiene facultades de coordinación en materia de ciberseguridad que realiza funciones de intercomunicación entre los Centros de Respuesta a Incidentes de Seguridad Informáticas (CSIRT) nacionales de referencia y la Secretaría de Estado de Seguridad.

participación de más actores emergentes y no estatales. En dicho documento se identificaron cuatro (04) dinámicas de transformación global: i) una mayor competición geopolítica; ii) un entorno socioeconómico marcado por las consecuencias de la COVID-19; iii) la aceleración del ritmo de transformación provocada por la tecnología y; iv) el proceso de transición ecológica. Si bien, hasta aquí es evidente la amplia normatividad que España ha desarrollado en pro de la ciberseguridad y su constante y ardua generación de políticas y reglamentaciones a vanguardia, en la actualidad el sector empresarial en diversos sectores en España, afronta una serie de riesgos y amenazas cibernéticos habituales como el malware, el phishing y el *ransomware*, y otras de nueva tendencia como *cryptojacking*, que son generadoras de incidentes ya consumados que han comprometido la integridad y confidencialidad de los datos de las organizaciones viéndose mayormente afectados los sectores de la administración, la salud y los seguros al ser atractivos a los ciberdelincuentes por su gran cantidad de datos sensibles y críticos (LINARES, BLANCO y HERRERA RUBIO 2023).

El aumento de tales amenazas cibernéticas es lo que ha generado que las empresas incrementen el número de personas responsables de ciberseguridad, ya sea desde equipos o unidades internas o externas, por lo que la inversión en ciberseguridad es uno de sus principales indicadores en aumento de las organizaciones, por ejemplo, para 2022, las empresas españolas incrementaron en un 62% su presupuesto (DELOITTE 2022).

Tipo de incidente	INCIDENTES GESTIONADOS						
	2016	2017	2018	2019	2020	2021	2022
Intrusión	14.373	19.275	8.541	6.479	9.557	7.039	7.649
Fraude	11.843	11.959	55.932	31.938	42.641	31.213	33.576
Malware	76.811	81.090	27.016	27.358	46.893	32.605	14.855
SPAM	10.279	7.957	0	0	0	0	0
Disponibilidad	495	514	100	58	1.971	7.177	1.768
Intento de intrusión	381	1.435	396	1.518	1.289	1.753	1.839
Robos de información	37	47	63	77	161	920	823
Contenido Abusivo			9.353	4.064	2.986	5.253	5.110
Recolección de información			5.605	84	87	106	73
Sistema Vulnerable			3.731	31.414	23.161	20.609	51.711
Otros	1.038	787	782	4.407	4.409	2.451	1.416

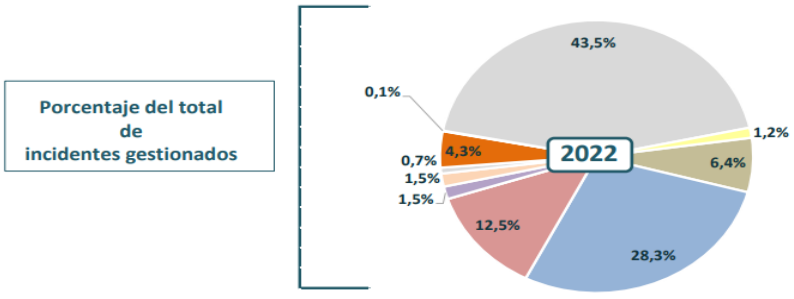

Figura 2. "Incidentes gestionados por el INCIBE-CERT 2022" (Gobierno de España Secretaría De Estado de Seguridad)

Los ciberdelincuentes han hallado en el *ransomware* un negocio bastante lucrativo pues tienen claro que los empresarios pagarían importantes sumas por rescatar su información, es así como durante la primera mitad de 2023 han ido surgiendo nuevas variedades de *ransomware* fundadas en códigos filtrados de variantes preliminares como *Babyk, LockBit* y *Conti*. Sin embargo, los equipos de seguridad informática en empresas responsables por su información han adoptado herramientas en pro de su mitigación, entre las más utilizadas se encuentra el software de detección *endpoint* con capacidades anti *ransomware* con un 87,8%, en segundo lugar, se ubica con un 84,4% la filtración de correo electrónico y análisis de amenazas y con un 22,4% algunas nuevas soluciones basadas en inteligencia artificial (IT RESELLER 2023).

Como ya se dijo, España cuenta con un sólido marco normativo en ciberseguridad, no obstante, la expansión de Internet y la introducción de nuevos servicios, dispositivos móviles, Internet de las cosas, computación en la nube, Big Data y la inminente llegada del metaverso, se plantean dudas sobre la eficacia de la normativa española.

Lo anterior, dado que, no resulta solo importante enfocarse en generar y generar disposiciones sino realizar actualización que además contengan la obligatoriedad de formar mecanismos para determinar la manera más óptima para ser verdaderamente preventivos y así comprobar si los recursos, las instalaciones o los procedimientos de respuesta de una organización están preparados para sufrir una situación de crisis. Esto por ejemplo se podría realizar a través de simulaciones de seguridad que determinen situaciones críticas, acercando a la organización a un escenario de actuación real (DELOITTE 2022).

Por otro lado, cabe destacar que hoy en día la realización de simulaciones de ciber crisis no se limita a ser únicamente una buena práctica de seguridad para las compañías, sino que también se trata en algunos casos de un proceso obligado, dependiendo de la regulación del sector de la industria analizada.

Es crucial tener en cuenta que las formas de vulnerar o poner en peligro los derechos fundamentales mediante innovaciones tecnológicas no siempre están reflejadas en los códigos penales, lo que incluso ha llevado a cambios legislativos recientes para abordar nuevas formas de lesividad no contempladas debido a la taxatividad del principio de legalidad penal (LLEDO YAGUE, BENITEZ ORTÚZAR y MONJE BALMASEDA 2021).

2.2 Contexto colombiano, desde lo normativo a lo real empresarial

El marco normativo colombiano al igual que el español está compuesto de varios y grandes capítulos o cuerpos regulatorios, en esta oportunidad los agruparemos así: **i)** Constitución, **ii)** Comercio electrónico y normatividad anti-trámite, **iii)** Control de legalidad de software y delitos informáticos, **iv)** Habeas Data y protección de datos personales, y **v)** Sociedad de la Información y las TIC. Los artículos 15, 20, 75 y 78 de la Constitución Política Colombiana, componen la base jurídica de la protección al derecho digital. El artículo 15 por su lado refiere el derecho a la intimidad personal y familiar, al buen nombre, y a la garantía que todo el pueblo colombiano tiene de reconocer, reestablecer y remediar o modificar la información que se tenga de una persona en bases de datos y en registros de cualquier tipo de entidad. El artículo 20 de dicha carta magna vigoriza la antes referida protección mediante la garantía de la libertad de manifestar y propagar la ideología, opinión y la salvaguardia de recibir y dar información cierta y ecuánime.

En Colombia, el gobierno ha generado algunas disposiciones que considera necesarias para poner frente a los ciberataques y resguardar la información de su población desde hace más de 10 años, por ejemplo, La Ley 1273 de 2009 es una de las herramientas más transcendentales en este sentido, esta instaura una serie de disposiciones que propenden por la prevención y eliminación de los delitos informáticos, creando además sanciones para aquellos que los cometan.

Derivado de ello encontramos la adición del Código Penal a través de la Ley 1273 de 2009, con un título VII BIS denominado “De la Protección de la Información y de los Datos”, que contempla una serie de delitos derivados de las violaciones al resguardo, la integridad y la asequibilidad de los datos y de los sistemas informáticos, esta normativa además, elimina el anterior artículo 195 que a la letra establecía: “El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa”.

Posterior a la expedición de la ley 1266 de 2008, que tenía por objeto dictar los lineamientos generales del hábeas data y instituir la administración de la información incluida en fichero o herramientas de custodia de datos personales, en particular la financiera, bancaria, comercial, de asistencia y la derivada de otros países, se promulgo, la ley 1581 de 2012, esta, desarrolla el derecho del artículo 15 de la carta magna así como el derecho a la información establecido

en el artículo 20 de la misma, estableciendo además el régimen propio para el tratamiento de datos personales en el territorio colombiano o en aquellos casos en los cuales el responsable del tratamiento o encargado del tratamiento que si bien no este instituido en territorio nacional le sea ajustable la legislación colombiana por aplicación de las normas y tratados internacionales.

Hasta aquí, Colombia demuestra una preocupación tanto por el patrimonio del Estado como de las empresas y la población en general que, podría verse vulnerado a raíz del mal uso de las tecnologías de la información o la debilidad de sus controles, pero existe una muestra más contundente de ello y es que el liderazgo de Colombia, según la categorización mundial de la UIT en materia de ciberseguridad, en el año 2014 consiguió ubicarse en el quinto lugar en el ámbito de las Américas y en el noveno lugar a nivel global, cerca de países como Francia, Egipto, España, y Dinamarca (CORTES BORRERO 2015).

En el contexto reciente, encontramos que el Gobierno Nacional expidió en marzo de 2020 como documento técnico la Política de Operación y Proceso de Tecnologías de la Información, este documento además de contener roles y responsabilidades en materia de seguridad de la información, también relaciona 12 lineamientos en pro de la mitigación. En abril de 2021 se emite la versión No. 08 de dicha política, donde se empieza a crear un límite entre los derechos personales y el ejercicio de estos cuando se está operando para un tercero que presta un bien o servicio a través de una empresa. Este límite está dado para el sector público, no obstante, es más que sano su traslado a la relación entre privados (Política de Operación, Proceso de Tecnologías de la Información. V. 8 2021), tal barrera por ejemplo, se da cuando un empleado tiene por obligación velar por la salvaguarda de las contraseñas asignadas para el ingreso a las distintas aplicaciones y/o servicios de TI, haciéndose responsable por todas y cada una de las acciones que se hagan con su usuario y al límite existente entre el derecho del manejo de su información, pues en todo caso, prima el ser precavido, evitando aquellas situaciones en que se revelen actos que pongan en peligro la seguridad institucional.

Varios estudios indican que, durante el 2022, las delaciones en Colombia por ciberdelitos aumentaron en un 26%, incluso se ha registrado que cada 8 minutos se recibe una nueva denuncia, siendo el hurto por medios informáticos el delito con mayor número de registros. Sin embargo, culminando el primer semestre de 2022, el Tanque de Análisis y Creatividad de las TIC (TicTac) mediante el programa de Seguridad Aplicada al fortalecimiento Empresarial (SAFE) mediante el escrito titulado, “ciberseguridad en la era de la movilidad digital”, indicó

algunas tipologías de cibercrimen que han disminuido, allí encontramos la Violación de Datos Personales en **-11%**, la Suplantación de Sitios Web para apropiarse de Datos Personales en **-13%** y el Uso de Software Malicioso en **-27%** . El mismo estudio el Tanque de Análisis y Creatividad de las TIC (TicTac) y su programa de Seguridad Aplicada al Fortalecimiento Empresarial (SAFE) referenció que continua en aumento la intromisión ilegal a sistema informático que para 2022 enseño 6.407 casos, es decir 46% más que el 2021.

En Colombia recientemente se han dado ataques cibernéticos preocupantes que han desestabilizado las entidades públicas, encontramos, por ejemplo, un ataque al proveedor IFX[2], que afectó a 20 entidades públicas de manera directa y a otras 78 de forma indirecta. Este tipo de ciberataques nos dejan la lección de lo importante y urgente de contar con una estrategia nacional de ciberseguridad integral y suficientemente coordinada entre las entidades del Estado, por lo que es clara la necesidad que desde el legislativo se entienda lo transcendental que es manejar este tipo de emergencias cibernéticas, para lo que se hace necesario tener propuestas sólidas en el congreso que logren su aprobación y una asignación presupuestal que permita la ejecución de tales políticas.

Esto, no solo tendría por objeto generar salvaguarda para las entidades públicas y afirmar el amparo de la información de todos quienes lo conformamos, sino que además genera oportunidades para el sector económico para custodiar las actividades comerciales y obligar a las empresas a alinearse con el derecho digital. El Consejo Privado de Competitividad (CPC) entidad ESAL cuya misión es amparar y asistir el desarrollo de la agenda pública, nacional y regional, en su informe de 2022, indicó que, Colombia ocupó el puesto 87 de 141 naciones en el acogimiento de tecnologías, no obstante, esta evolución no ha sido desde todos los frentes que deberían crecer de manera articulada, pues el marco regulatorio colombiano sigue siendo débil en contextos como claridad, políticas de prevención, políticas de respuesta y

[2] El Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia - MinTIC dio a conocer que, el 12 de septiembre de 2023, IFX Networks fue víctima de un asalto de ciberseguridad de tipo ransomware afectando a más de 762 empresas establecidas en Sur América. En Colombia el ciberataque afectó los canales de información y herramientas de trabajo de varias entidades del sector público como el Ministerio de Salud, la Superintendencia de Salud y el Consejo Superior de la Judicatura, la afectación resulto ser tal que, la Rama Judicial colombiana tuvo que tomar medidas como la suspensión de los términos judiciales en todo el territorio nacional durante el periodo del catorce al veinte de septiembre de 2023, con excepciones muy puntuales. https://www.portafolio.co/tecnologia/ciberataque-en-colombia-acciones-que-se-estan-realizando-para-mitigar-danos-ifx-network-589102

responsabilidades, por lo que la normatividad nacional de ciberseguridad a la fecha requiere ser reforzada en hitos de trascendencia, presupuesto, intervención y estimación para conseguir una conciencia de ciberseguridad sustentable y fortalecida.

El Consejo Nacional de Política Económica y Social (CONPES) instituido mediante la Ley 19 de 1958 es la más grande potestad territorial de planificación siendo un ente que brinda asesoría al Gobierno en temáticas que impactan de manera importante en la economía y en la sociedad del país. El COMPES 3995 estableció a través de una política nacional de confianza y seguridad digital un análisis de la adopción de modelos y estándares a gestionar que reflejan los desafíos de la cuarta Revolución Industrial (4RI) para el país. En concordancia con lo anterior, el 2022 se estableció como vigencia meta para digitalizar más del 60 % del PIB mundial teniendo claro que la economía durante la próxima década utilizará herramientas habilitadas digitalmente.

Si bien, el COMPES 3995 tenia como propósito generar lineamientos que permitieran fundar acciones que estimularan el desarrollo de la confianza digital y que, por tanto, Colombia le apuntara a ser una nación progresista y competidora en el mundo digital, entendiendo la necesidad de fortalecer habilidades y forjar un cerco normativo solido que propenda por la ciberseguridad, siendo el 2023 el cambio no ha sido para nada visible. Tal situación, es preocupante, pues para el desarrollo de esta política se tuvo proyectado un financiamiento cuantioso desde entidades de distinto orden del sector central como se puede ver a continuación:

Tabla 1. Financiamiento estimado indicativo de la política

Entidad	**2020**	**2021**	**2022**	**Total**
Departamento Administrativo de la Presidencia de la República	-	-	-	-
Departamento Nacional de Planeación	-	1.990	1.010	3.000
Dirección de Nacional de Inteligencia	-	600	-	600
Ministerio de Defensa Nacional	-	-	-	-
Ministerio de Educación Nacional	-	-	-	-
Ministerio de Justicia y del Derecho	24	68	72	164

Ministerio de Tecnologías de la Información y las Comunicaciones	450	2.250	1.850	4.550
SENA	-	14	14	28
Total	**474**	**4.922**	**2946**	**8.342**

DNP, 2020

El 1 de mayo de 2023 el abogado Mauricio Lizcano tomó posesión en Colombia como nuevo ministro TIC y en plena posesión manifestó que trabajaría en equipo con la Administración, sectores económicos como la industria, las colectividades y distintos actores para llevar conectividad a los lugares más apartados del país y hacerle frente a la desigualdad y la pobreza, reconociendo además que Colombia solo logrará un avance real en la economía en la medida en que la tecnología sea la piedra angular.

El ministro actual entiende la necesidad de impulsar en el gobierno políticas garantes en materia de ciberseguridad, posesionando a Colombia como un 'HUB de ciberseguridad, trabajando en el desarrollo de un gran centro de operaciones que articule empresas, talentos, competencias y servicios. Este “HUB” permitirá fortalecer las capacidades del país en materia de seguridad digital, pero, para ello, es indudable que se necesita inversión y confianza en el segmento de las telecomunicaciones.

Y es que no podemos esperar menos: existen estudios serios como el “Securing the Digital Economy”, que determinó que el reporte del 68% de los CEOs de las organizaciones que formaron parte del análisis, indicaron que el porcentaje de dependencia a Internet por ejemplo se ha aumentado del 23% en el que se encontraba para vigencia 2008 a un 100 % a 2018. En todo caso, la evolución reglamentaria de la política de ciberseguridad y ciberdefensa, establecida en los CONPES 3701 y 3854, indica el avance de lo relacionado con soportes documentales en el país, además, demuestra la seriedad con la que se ha embarcado el propósito de complementariedad para lograr el robustecer y mejorar las capacidades de respuesta. No obstante, se necesita que los propósitos del actual gobierno en realidad se consoliden pues si bien es cierto que, la administración del riesgo de la ciberseguridad no debe ser del gobierno nacional ni de forma única, ni de manera excluyente, pues, se debe completar con los proyectos de diversos actores para mitigar las ciber amenazas existentes, la gestión del sector público es fundamental (CUJABANTE VILLAMIL et al 2020).

No podemos decir que el atraso de Colombia en materia de ciberseguridad es absoluto, pero, así como en el contexto normativo, en materia privada algunos datos son realmente preocupantes, pues las sociedades colombianas solo presupuestan el 12% de sus recursos en técnicas y tácticas de seguridad, sin embargo, Colombia en tal sentido realiza inversiones que la ubica en un nivel alto en comparación con el promedio de Latinoamérica en áreas como seguridad móvil, seguridad de acceso a la nube y gestión de vulnerabilidades (SEGURIDAD 360 2022).

Según el análisis del - Digital Trust Insights 2023 Colombia, de PWC, los directivos de las empresas colombianas están más informados respecto de la ciberseguridad, pues el 54% de las empresas son conscientes que a medida en la que han asumido proyectos con mayor digitalización aumentan los riesgos de ciberseguridad, no obstante, esta conciencia se queda corta y solo queda en un mero entendimiento pues solo el 5% de los altos ejecutivos dicen implementar las 10 prácticas estándar para salvaguardar los datos de los clientes (PwC, 2023). Dicho informe, además, muestra datos interesantes que informan respecto de las medidas que las sociedades han ejecutado para mitigar los 10 incidentes más peligrosos relacionados con ciberseguridad.

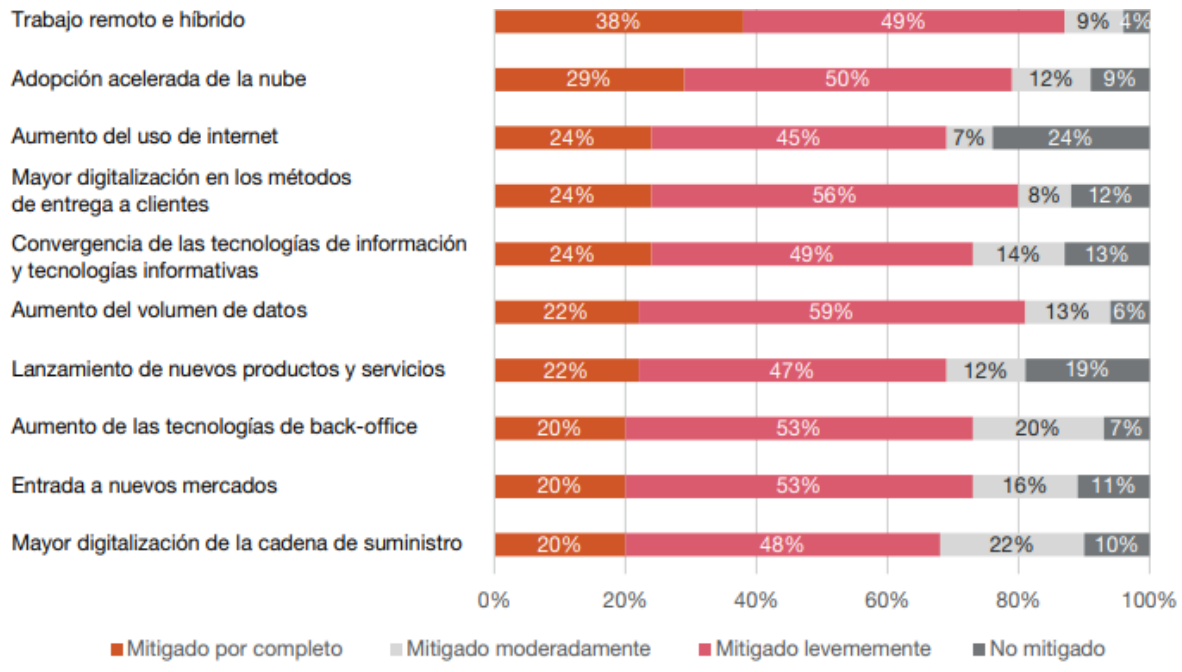

Figura 3 ¿En qué medida las empresas han mitigado los 10 riesgos más importantes relacionados con ciberseguridad? (PwC)

Los riesgos antes identificados se desprenden de los delitos más usuales en Colombia encontrando en el primer lugar, los relacionados con operaciones de hackeo y escape de la información (55%), luego se ubica el *Ransomware* (49%) seguido de la explotación de servicios relacionados con la nube (44%). En el sector empresarial se ha detentado que la comisión de estas conductas punibles usualmente esta relacionada con el manejo del e-mail y la suplantación de cuentas corporativas (PwC 2023).

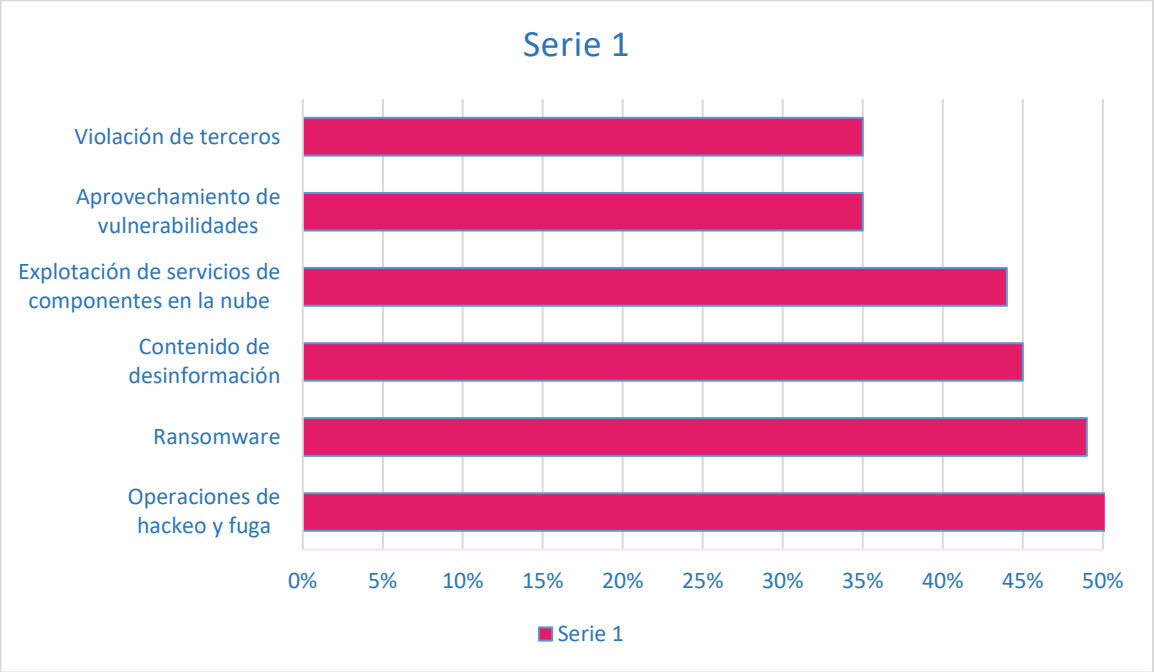

Figura 4 Tipos de ataques cibernéticos que aumentan de forma significativa en las organizaciones colombianas y a nivel mundial, durante el 2023 (PwC)

3. Organismos y programas actuales en materia de ciberseguridad

3.1 Contexto Español

Los programas actuales son coordinados por el Departamento de Seguridad Nacional - DSN adscrito a la máxima autoridad en España desde lo ejecutivo, es decir la Presidencia del Gobierno y por el Consejo Nacional de Ciberseguridad – CNC adscrito al Ministerio de Asuntos Económicos y Transformación Digital que tiene por competencia el progreso de la economía digital, la transformación digital y la ciberseguridad. La CNC, fue creada de manera formal en vigencia 2014 como un órgano colegiado de apoyo bajo la intención de reforzar las relaciones entre la administración pública con competencias en materia de ciberseguridad. (DEL REAL 2022)

Lo anterior, se da en razón a la necesidad de articular los distintos organismos que tiene funciones en materia de ciberseguridad. Esta organización ha sido especialmente pensada por lo que tal planteamiento, por ejemplo, se refleja en el hecho de que el DSN que es un órgano consultivo y de asesoría de la máxima autoridad en lo ejecutivo, ocupa tanto la vicepresidencia como la secretaría del CNC.

Pero el CNC no es el único organismo relevante en materia de ciberseguridad adscrito al Ministerio de Asuntos Económicos y Transformación Digital, pues también encontramos a el Instituto Nacional de Ciberseguridad de España (INCIBE), que actualizó su denominación el 28 de octubre de 2014 pues antes de tal vigencia y desde 2006 era conocido como el Instituto Nacional de Tecnologías de la Comunicación, con esta modificación y actualización, ahora ejercer como aparato nacional que busca que la ciberseguridad se incorpore como una batería en la metamorfosis social, generando posibilidades de innovación y confianza digital para los ciudadanos.

El INCIBE, funciona como una empresa pública con una gran red escolástica y de investigación, entre académicos y empresarios estratégicos, que trabajan en pro de la cultura de ciberseguridad. Debido a esta gran responsabilidad, el INCIBE trabaja a través de la creación

de nuevos organismo y subcentros, en los que encontramos por ejemplo el ObservaCIBER[3] y el INCIBE-CERT.

El INCIBE-CERT es uno de los más importantes proyectos del INCIBE pues es un ente creado para ponerle frente a los riesgos que pongan en peligro la ciberseguridad tanto en le contexto particular como general del sector privado en España pues facilita una respuesta coordinada y eficiente a los ciberataques (CANDAU 2021). El CERT en España (Centro Criptológico Nacional - *Computer Emergency Response Team*) forma parte del Centro Nacional de Inteligencia (CNI) y se encarga de gestionar incidentes de ciberseguridad en sistemas clasificados y en infraestructuras críticas.

Estos CERT de referencia según el artículo 11 del Real Decreto-ley 12/2018, del 7 de septiembre, que versa sobre seguridad de las redes y sistemas de información son:

- El CCN-CERT, del Centro Criptológico Nacional, al que incumbe la seguridad de las entidades del sector público.
- El INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, es aquel organismo dedicado a atender la seguridad del sector privado que además trabaja de manera articulada con el INCIBE y el CNPIC en aquellas situaciones relacionadas con incidentes que afecten a los operadores críticos.
- El ESPDEF-CERT, enfocado en la seguridad del Ministerio de Defensa, es decir en el ámbito propio de las fuerzas armadas, protegiendo entonces los sistemas de información, telecomunicaciones y redes.

Los tres CERT mencionados son organismos útiles para la coordinación nacional e internacional y fungen como un último recurso ante emergencias, por lo que no tienen alcance para resolver la gestión diaria de la ciberseguridad en las organizaciones.

En España, con el ánimo de desarrollar economía y empleo digital, se encontró perentorio impulsar el sector de las telecomunicaciones y el desarrollo de nuevas herramientas digitales, esto, para lograr una adaptación social y territorial, basada en el progreso y amplificación de

[3] Espacio común, para crear estudios de cultura de ciberseguridad desarrollados por distintos actores involucrados que permiten fortalecer y aumentar el conocimiento en transformación digital haciendo de ello un proceso más seguro.

las redes. Por ello, se expidió la Ley 11 del 28 de junio de 2022, la cual indica en su artículo 37 que se propende por un servicio universal y neutral garantizando a todos los consumidores la prestación del servicio sin importar el territorio en el cual se esté ubicado, proporcionado en condiciones de calidad y a costes posibles de cubrir. Este desarrollo supone la generación de más riesgos en materia de ciberseguridad por el uso que la población le dé, por lo que se requiere una adecuada higiene cibernética y un fortalecimiento en capacitación a todo el que opere las TICs.

Encontrando esta necesidad, el INCIBE creó el Programa de Ciber cooperantes en el marco de la Ley 45 de 2015 que versa sobre actividades de voluntariado, con el objetivo de promover la colaboración entre particulares interesados en la divulgación de la ciberseguridad desarrollando charlas de concienciación y formación, con centros y sociedades. Esta actividad además es compensada y el ciber cooperante tiene la oportunidad de recibir una serie de incentivos por su ejercicio, tales como el reconocimiento de la actividad realizada, capacitaciones y talleres de formación en doble vía, escenarios para publicación de artículos y clasificación tipo TOP.

En la actualidad el INCIBE está llevando a cabo varios programas dentro de su proyecto España Digital 2026 encaminados a vigorizar las dimensiones y la esperanza digital de la ciudadanía y las empresas, y a crear cultura de ciberseguridad permitiendo entender los riesgos y perjuicios asociados a la digitalización. La inversión realizada por España para propulsar tales esquemas es importante y el gran reto es lograr su máximo aprovechamiento pues las pymes se verán expuestas ante distintos cambios en su estructura operativa y administrativa. Dichos programas son:

- **Programa (Confía)**: Dirigido principalmente a pymes y profesionales para animar los ambientes y conductos apropiados para la contribución y salvaguardia conjunta ante inminencias comunes.
- **Puesta en marcha del Centro Nacional de Competencias en Ciberseguridad (NCC-ES)**, el cual toma como ejemplo el Centro Europeo de Competencias (ECCC).
- **Programa IncibeEmprende bajo el Programa de Impulso a la Industria de la Ciberseguridad Nacional**: Mediante el cual se propende por el desenvolvimiento y celeridad para la creación de nuevas *start-ups* y crecimiento de *start-ups* ya existentes.

- **Programa Talento Hacker:** Se busca atraer, educar y emplear a trabajadores en el sector de la ciberseguridad.
- **Programa Ciberinnova:** Promueve las habilidades de la industria nacional bajo el Programa Global de Innovación en Seguridad.

Pero no solo el Ministerio de Asuntos Económicos y Transformación Digital y la Presidencia contribuyen con importantes proyectos y organismo a la ciberseguridad nacional que impactan el sector empresarial, por su parte el Ministerio de Defensa tiene a su cargo el Centro Criptológico Nacional - CCN, organismo adscrito al Centro Nacional de Inteligencia – CNI[4], creado a través del Real Decreto 421/2004 con la misión de dar seguridad de las tecnologías de la información y proteger la información clasificada. Para cumplir con los objetivos propuestos el CNN cuenta con diversas soluciones, con denominaciones muy especiales y enfoques fascinantemente innovadores. Para esta época en la página web oficial del CCN encontramos 24 soluciones de las cuales se destacan ocho con gran influencia para el sector empresarial y que se describirán de manera breve a continuación:

- **ADA**, una plataforma de análisis avanzado de malware, pues cuenta con una estructura afable con la que se puede interactuar de forma amigable.
- **AMPARO**, solución exclusiva para las Entidades de Certificación (EC) y Órganos de Auditoría Técnica (OAT) para facilitar los procesos de auditoría.
- **CARLA**, solución de protección centrada en los datos, que permite que la información corporativa viaje segura, pues permite saber quién ha accedido y con qué permisos.
- **EMMA**, solución con la que es posible obtener visibilidad y control de todos activos conectados a la red corporativa.
- **ELENA**, un simulador que permite la capacitación de profesionales gracias a su sistema desarrollados 100% en España basado en soluciones reales, testado por experto y

[4] EL Centro Nacional de Inteligencia CNI tiene a su cargo el programa, sobre formación presencial y online **Ángeles** en temáticas como familiarización en ciberseguridad, capacitación en esquema nacional de seguridad, Cursos específicos desarrollados por el CCN a petición de una organización (Ad Hoc), Curso Gestión de Incidentes de Ciberseguridad, entre otros.

netamente intuitivo. Esta herramienta, posibilita desarrollar y poner en práctica las técnicas para realizar labores de ciber-investigación.

- **GLORIA**, una plataforma que permite la gestión de alertas e incidentes y genera alertas automáticas generadas por el sistema de correlación.
- **INES**, solución que proporciona una herramienta de evaluación constante de la seguridad de los sistemas TIC de las organizaciones.
- **OLVIDO**, solución que realiza borrado de forma segura de ficheros y carpeta.

3.2 Contexto Colombiano

Desde el 2001 a través del COMPES 3701 han existido cuerpos encargados de la ciberseguridad y ciberdefensa en Colombia. El Comando Conjunto Cibernético de las Fuerzas Militares creado en 2011 se encargó de regularizar la contestación a incidentes de seguridad que afectaban la seguridad nacional y surgió como una delegación agregada al Comando de las Fuerzas Militares que tenía por objeto el análisis forense básico, realizar operaciones de ciberdefensa, auditorías y evaluaciones de seguridad, así como brindar capacitación especializada.

Mas adelante se creó el Centro Cibernético Policial como una dependencia de la Dirección de Investigación Criminal - INTERPOL que surge para trabajar de manera paralela y articulada con el grupo investigativo de delitos informáticos fortalecido con la expedición de la Resolución Número 05839 de 2015. Este organismo tiene importantes logros como la Implementación del equipo de respuesta a incidentes informáticos de la Policía Nacional - CSIRT PONAL y la atención judicial de incidentes cibernéticos en distintos ámbitos y esferas.

Desde la rama ejecutiva y con el ánimo de fortalecer los cuerpos ya mencionados, el Ministerio de las TIC, mediante la Resolución 473 del 2022, adicionó el artículo primero de la Resolución 002108 del 2020, para crear el Grupo Interno de Trabajo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT, adscrito al Viceministerio de Transformación Digital; esta entidad surge con el objetivo de poder ejecutar una adecuada diligencia y rastreo de los incidentes cibernéticos de manera concentrada.

En marzo de 2022 y de conformidad con el Plan Nacional de Desarrollo (“PND”), el Gobierno Nacional de Colombia promulgó el Decreto 338 de 2022, normatividad que tiene por objeto puntualizar parámetros macro para robustecer la gobernanza de la seguridad digital, y permitir la creación de un importante modelo de seguridad. De este modelo, se derivan dos

iniciativas dinamizadoras con varios elementos que sirven de base para las líneas de acción orientadas en desarrollar oportunidades y métodos inteligentes que resulten en herramientas de consolidación de información que aporte en la toma de decisiones fiables. La primera iniciativa incluye la implementación de mecanismos de transformación digital y la segunda está encaminada en desarrollar destrezas de ciudades y territorios inteligentes, a través del uso de TIC como artilugios de evolución social, económica y ambiental.

Figura 5. "Política de Gobierno Digital" (Ministerio de Educación)

Ahora, a pesar que existen propuestas consolidadas en normatividades y lineamientos estatales, (elemento importante que refleja el interés del gobierno en desarrollar políticas y estrategias para proteger la infraestructura cibernética y la información en el país) las personas jurídicas dedicadas al comercio no están penetrando la esfera de la prevención, especialmente desde lo que corresponde con el nivel preventivo de ataques cibernéticos, que es inminente a la hora de proteger la información personal de sus clientes y usuarios (BRIGARD URRUTIA 2023).

En el contexto empresarial debemos traer a colación la Superintendencia de Industria y Comercio -SIC, como autoridad nacional que tiene por objeto la salvaguarda de la competencia leal entre comerciantes, de los datos personales y los derechos de los consumidores, pues esta autoridad mediante la expedición de distintas Circulares y Guías, obliga a todas las entidades que están bajo su inspección y vigilancia a informar a la autoridad

de protección de datos cuando se presenten situaciones que se puedan considerar como incidentes de seguridad y exista riesgo en la gestión de la información de los titulares. En concordancia con lo anterior, la SIC ha dispuesto a través de diversas decisiones,[5] como la determinada por la Resolución Número 6369/2019425 al no reportar brechas de seguridad, así como también por la falta de medidas preventivas, la cesión no autorizada de datos, y la falta de manuales para regular el ciclo de vida de los datos, altas sanciones pecuniarias (TEJERINA y BELTRÁN 2020).

El Tanque de Análisis y Creatividad de las TIC (TicTac)[6] mediante el programa de Seguridad Aplicada al fortalecimiento Empresarial (SAFE) indicó que el hurto de información a través de herramientas informáticas en 2022 arrojó un incremento del 15% con 11.078 incidentes puestos en conocimiento de las autoridades judiciales. Las ciudades que presentaron un mayor número de casos fueron las capitales de los Departamentos de Cundinamarca, Antioquia, Cauca, Atlántico y Santander, concentrándose allí más del 70% de las denuncias instauradas durante el primer semestre del 2022, en actividades económicas generadas a través de las plataformas de *e-commerce* y la banca virtual. Tales datos siguen creciendo y no han sido del todo mitigados pese al apalancamiento internacional a través del traslado de buenas prácticas y modelos de otros países parcialmente consolidados.

Desde el contexto internacional, uno de los programas identificados aplicables al pueblo colombiano, es el Programa de Ciberseguridad del CICTE que ayuda a los Estados miembros de la Organización de los Estados Americanos (OEA) en el impulso de generación de estrategias enfocadas a la salvaguarda de la información a nivel técnico y la estructuración de

[5] A pesar de no ser uno de los antecedentes más nuevos, el caso Colmédica del 2016, resuelto en la Resolución N.º 39298/2016427, constituye un hito en la práctica de la SIC por tratarse de una de las sanciones más altas que ha impuesto debido a la publicación de información médica de forma irrestricta, prescindiendo totalmente de las medidas de seguridad que la información sensible demanda, en particular por encontrarse firme y ejecutable. (TEJERINA y BELTRÁN 2020)

[6] El **Tanque de Análisis y Creatividad de las TIC – TicTac** – es el primer tanque de razonamiento e innovación del sector TIC en Colombia, creado en el año 2016 por la Cámara Colombiana de Informática y Telecomunicaciones CCIT, con el propósito de plantear iniciativas de política pública que propendan a la evolución digital, y que se basen en sostenibilidad, competencia económica, inserción social, y poder gubernamental .https://www.ccit.org.co/tictac/

políticas públicas. Sus objetivos están enfocados en dar apoyo para: i) generar mayores facultades técnicas y políticas para advertir, señalar, y atender incidentes cibernéticos, ii) progresar el cambio de información y iii) acrecentar la posibilidad de entendimiento e información sobre incidentes y peligros cibernéticos. Dicho programa ayuda a los Estados miembros de la OEA a desplegar maniobras nacionales de ciberseguridad y que se acomoden al contexto legislativo, cultural, financiero y organizacional de cada Estado Miembro.

Por ejemplo, mediante la publicación del paper "retos y estrategias, las consideraciones de los ataque de *ransomware* de las Américas" la OEA referenció la importancia que en cada una de las organizaciones públicas y privadas se establezca la llamada "ciberhigiene"[7], que en su generalidad se ve afligida por la confianza ingenua de las personas en los mecanismos y herramientas disponibles, así como el acrecentamiento de productos y servicios digitales que se extienden con restringidas medidas de prevención y control. Bajo este escenario de ciberhigiene, los delincuentes no tendrán el espacio ideal para movilizarse con el fin de lograr sus propósitos criminales.

Es en este contexto en donde encaja perfectamente la necesidad del reconocimiento de la existencia de la responsabilidad penal de las personas jurídicas, enfocada en ese permisivismo y falta de rigurosidad de las empresas a través de la cual sus trabajadores o representantes utilizan incluso herramientas digitales puestas a su disposición para desarrollar actividades laborales para realizar actos criminales en materia de ciberdelincuencia (inclusive atentando contra la misma entidad para la que laboran) impone a los administradores el actuar con diligencia y probidad a la sociedad; con el dinamismo que debe aplicar un "ordenado empresario", cumpliendo con la normatividad que le sea exigible, con un nivel de atención y ejercicio fiel del cargo, con deberes de supervisión y control de la empresa y una obligatoria debida y adecuada información (GÓMEZ HERVÁS 2021).

Pero ¿por qué resulta tan importante reforzar este contexto de responsabilidad? A pesar de que en Colombia en el año 2022 se generaron una serie de políticas y normativas que tienen

7 Kaspersky.es: Conceptúa el ciberhigiene como aquella que tiene como propósito el mantener el vigor y salvaguarda necesaria del hardware y el software, a fin de asegurar que estén resguardados contra ataques como el malware. Así pues, si se vuelve una práctica reiterativa y bien ejecutada será más que seguro que nuestros datos estén bien cuidados.

por finalidad mitigar la ciberdelincuencia del sector empresarial, se dieron varios incidentes de seguridad notables, algunos de ellos son:

- En el mes de noviembre, El Diario LA REPUBLICA (2022) público el post en X de EMP en el que le ponían de presente a la ciudadanía que se encontraban atendiendo un incidente de ciberseguridad, por lo que se había solicitado a todo el personal, laborar desde sus casas. Informando además que la situación no tenía afectación en la prestación de los servicios que suministran y que además tienen incidencia en las necesidades básicas de la población pues son energía, agua y gas.
- Un mes después, el periódico PORTAFOLIO (2022) compartió la situación por la que había pasado el Grupo Keralty, que reúne a las empresas de salud Sanitas y Colsanitas debido al ataque de los piratas informáticos RansomHouse, quienes se apoderaron de 0,7 terabytes de información de dichas entidades, que contenía información y balances de tipo presupuestal y financiero, así como información personal.
- El domingo 22 de enero de 2023 Giovanny Mesa, gerente general de Audifarma, cadena de droguerías que le presta sus servicios a distintas EPS, comunicó que fueron víctimas de un asalto informático en su infraestructura tecnológica, por lo que se tuvo que suspender el uso de los servidores físicos y virtuales como medida de protección de la información tanto de la entidad como de los usuarios.

Este tipo de incidentes no solo afectan la estabilidad de las empresas o sus finanzas al tener que invertir en recursos para reforzar la protección de los sistemas de información, sino que además perturban los servicios que prestan a la comunidad que en algunos casos hacen parte de las necesidades básicas de la población. Además, el riesgo en el que se ve envuelta cualquier organización frente a un ataque de ciberdelincuentes afecta su reputación corporativa, al generarse inseguridad y desconfianza en sus procesos internos y servicios, sin mencionar otras afectaciones a su patrimonio al verse en la obligación de pagar cuantiosas multas en el respectivo contexto legal.

Los informes del CCIT[8] en Colombia han incluido que los gremios con mayor riesgo en ciberdelincuencia son: la educación, la industria y la salud; siendo el sector PYME (pequeñas y medianas empresas) las más afectadas por lo ciberataques en Colombia.

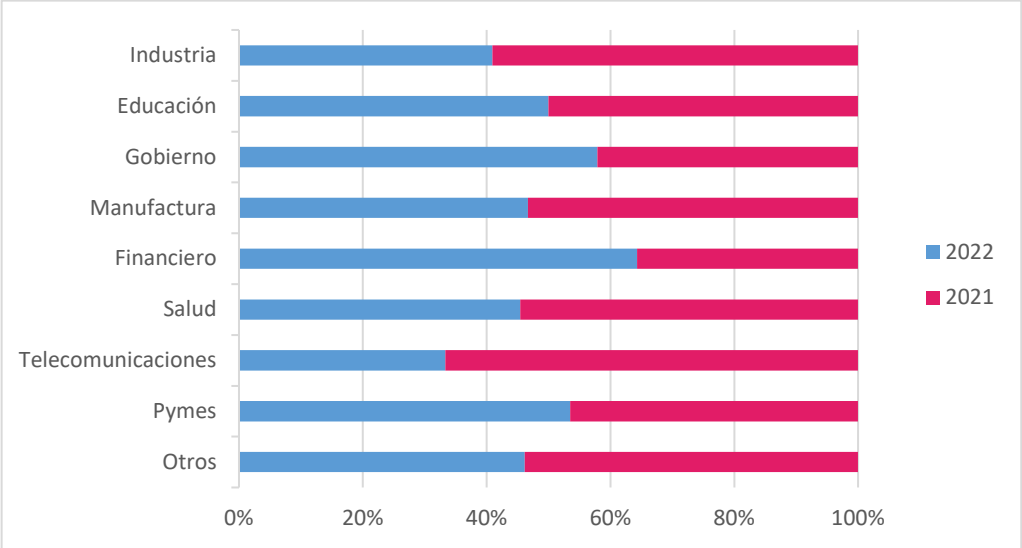

Figura 6. "Sectores más afectados 2021-2021" (BAUTISTA GARCIA, F., GUZMÁN MESA, L. y BLANCO, L.)

8 La Cámara Colombiana de Informática y Telecomunicaciones CCIT, fue creada en 1993 como una entidad gremial dedicada ha realizar asesoramiento a las empresas asociadas, con el finde promover el bienestar y mejoramiento de sus actividades.

4. Análisis comparativo de algunos contextos normativos (España-Colombia) de interés para el sector empresarial.

El mundo experimenta cambios rápidos en todos los aspectos, pero la velocidad es aún mayor en el ámbito digital pues la investigación, el consumismo, el desarrollo y la innovación son algunos de los factores que, conllevan su aceleración. Si bien, la tecnología sirve como respaldo para tareas diarias, solución de problemas y es fundamental en la esfera del entretenimiento, las comparaciones internacionales son esenciales para el diagnóstico, la evaluación y la evolución positiva, ya que ser competente no basta en un entorno de cambio acelerado y algunos países deben mirar hacia afuera para mantener su capacidad.

Es fundamental destacar que la ciberseguridad es un reto en constante evolución, y ningún país está plenamente inmune a los ciberataques; sin embargo, del análisis realizado en los capítulos anteriores resulta evidente concluir que los controles de seguridad desde roles y responsabilidades y la conciencia de la ciberseguridad son elementos cruciales. Se debe tener en cuenta que, la ciberseguridad es un esfuerzo continuo y multidimensional que requiere la participación de actores competentes, actualización de conocimientos y estrategias de seguridad.

Dicho lo anterior, se han seleccionado tres grandes panoramas a comparar que son fundamentales para una adecuada protección de los activos digitales y la información sensible de una empresa y en tal sentido mitigar los riesgos de la ciberdelincuencia:

i) Brechas de seguridad de datos personales,

ii) Responsabilidad penal de la persona jurídica,

iii) El experto a cargo de la seguridad informática.

Comparar el nivel de desarrollo en ciberseguridad entre países es complejo y aún más enfocado a las prácticas empresariales en donde la libertad de empresa y la autonomía no permiten en el contexto privado coaccionar la implementación de controles específicos, por tanto, tal comparación debe realizarse desde factores o contextos definidos, por lo que no es suficiente hablar en general de un marco legal y normativo.

4.1 Análisis comparativo entre España y Colombia - brechas de seguridad de datos personales

En España, el Reglamento General de Protección de Datos - RGPD define las infracciones de seguridad de los datos, como aquellas vulneraciones a los sistemas corporativos o a los equipos personales ocasionados por la pérdida, el detrimento o transformación accidental o ilícita de datos personales compartidos, almacenados o asistidos de otra forma, o el uso no permitido a dichos datos. Lo anterior, se da con base en lo dispuesto por el artículo 33 del (RGPD) que preceptúa el compromiso de notificar los incidentes en los que se vean afectados los datos personales que puedan conjeturar un peligro para los derechos y libertades de las personas naturales a las cuales les pertenecen los datos, notificación que, por regla general se hace ante la Agencia Española de Protección de Datos (AEPD) como jurisdicción de vigilancia competente.

En Colombia las disposiciones generales para la protección de datos personales, se encuentran desarrolladas a través de la Ley Estatutaria 1581 de 2012, sin embargo, esta norma no establece de manera particular el procedimiento para manejo y notificación de una brecha de seguridad. Por su parte la circular 003 de 01 de agosto de 2018 de la Superintendencia de Industria y Comercio - SIC, en el literal f del numeral 2.1 establece la obligación de realizar reportes de novedades entre ellas de incidentes de seguridad, no obstante, solo establece el termino para hacerlo sin ninguna especificidad, dicho esto, el único documento que da algún bosquejo de como los responsables y encargados del tratamiento de datos personales deben operar los incidentes de seguridad es la Guía para la Gestión de Incidentes de Seguridad en el Tratamiento de Datos Personales, de la SIC que, además referencia y toma como base las Guías de la Agencia Española de Protección de Datos - AEPD. Así pues, entendiendo el desequilibrio regulatorio en cada uno de los países analizados en el presente texto, se hace necesario realizar un poco más a fondo el análisis de esta temática para lograr detectar elementos que pueden tomarse como buenas prácticas regulatorias para la ciberseguridad en las empresas colombianas, por lo que a través de las siguientes tablas se realizará una comparación normativa referente a: **i)** Requisitos para notificación de Brecha de Seguridad, **ii)** Excepciones a la notificación, **iii)** Herramientas para la notificación de Brechas de Seguridad, **iv)** Contenido de la notificación de brecha de seguridad y **v)** Roles y responsabilidades en la notificación y manejo de Brechas de Seguridad

Tabla 2. Análisis comparativo entre España y Colombia - Brechas de Seguridad de Datos Personales

BRECHAS DE SEGURIDAD DE DATOS PERSONALES

	ESPAÑA	***COLOMBIA***
Requisitos para notificación de Brecha de Seguridad	Según artículo 33 del RGPD la notificación está proyectada en dos fases, que en lo posible deben hacerse de forma simultánea, la primera a la autoridad competente que debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes al conocimiento del responsable y la segunda a los interesados dentro de los 30 días siguientes. Ahora bien, El artículo 34 del RGPD expone una serie de lineamientos para realizar una debida comunicación al interesado cuando existe violación de la seguridad de los datos personales, así pues, se debe tener en cuenta que: **SE DEBE NOTIFICAR:** Se notifica si vulnera los derechos e intereses de las personas físicas **NO RESULTA SER:** La mera sospecha de que ha existido una brecha sin que se conozcan mínimamente sus circunstancias no resulta ser soporte suficiente para notificación.	El Capítulo II, Título V de la Circular Única de la SIC establece que las organizaciones que están obligadas a inscribir las Bases de Datos Personales ante el Registro Nacional de Bases de Datos – RNBD, deben reportar los incidentes de seguridad dentro los 15 días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o el área encargada de atenderlos a través del enlace previsto en la página web de la SIC. Ahora, quienes no se encuentren obligados a registrar sus Bases de Datos en el RNBD de igual manera deberán hacer el reporte en los términos ya mencionados. Dentro de la Guía para la gestión de incidentes de seguridad en el tratamiento de datos personales de la SIC se recomienda a las organizaciones resolver los siguientes cuatro interrogantes para estructurar su propio procedimiento de atención a incidentes de seguridad: ¿Cuándo?, ¿Cómo?, ¿Quién? ¿Qué debe incluirse en la comunicación?

BRECHAS DE SEGURIDAD DE DATOS PERSONALES

	ESPAÑA	COLOMBIA
Excepciones a la notificación	Según el numeral 3 del artículo 34 del Reglamento General de Protección de Datos – RGPD no será necesaria la notificación cuando el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas que hagan ininteligibles los datos personales, como el cifrado; o cuando el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado. Ahora, si bien el literal c del numeral 3 del artículo 34 establece como excepción a la notificación personal cuando esta sea considerada como desproporcionada por el esfuerzo de su particularización, no comparto la inclusión en el apartado pues esta no se deja de realizar, sino que cambia el mecanismo de envío haciéndose mediante vías públicas que en mi juicio resultan aún mucho más contundentes y efectivas para el interesado.	Dado que la ley 1581 de 2012 no hace ninguna distinción entre que incidente de seguridad se debe reportar y cual no se considera que debe ser reportado, todos independientemente de su impacto y manejo deben ser reportados. La implementación de medidas de protección técnicas y organizativas apropiadas y su impacto positivo en la mitigación de riesgos no son tenidas en cuenta como excepciones a la notificación. Frente a ello, el Decreto 1377 de 2013, establece en sus artículo 26 y 27 que el responsable del tratamiento de datos personales debe ser capaz de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012, tal verificación, podrá ser tenida en cuenta por la SIC al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley.

BRECHAS DE SEGURIDAD DE DATOS PERSONALES

	ESPAÑA	COLOMBIA
Herramientas para la notificación de Brechas de Seguridad	A la fecha, las responsables del tratamiento de datos y los roles de delegado y encargado cuentan con una serie de herramientas gratuitas dispuestas por la Agencia Española de Protección de Datos (AEPD), de estas, se deben destacar las que a continuación se enuncian: - Un recurso útil que ayuda a la toma de decisiones, evaluando la obligación de notificar a las personas físicas afectadas. Esta se denomina "**Comunica-Brecha RGPD**". - Un recurso útil que ayuda a la toma de decisiones, evaluando el compromiso de comunicar a la Agencia Española de Protección de Datos. Esta se denomina "**Asesora Brecha**" - Una herramienta denominada "**Facilita Emprende**" que permite caracterizar los tipos de tratamiento realizados por empresas, emprendedores y startups que además se identifican por un fuerte elemento innovador por lo que el uso de las tecnologías se hace inminente.	La Superintendencia de Industria y Comercio – SIC en su calidad de autoridad nacional de protección de datos, no tiene implementada ninguna herramienta o recurso que sirva al sector empresarial en la autogestión de incidentes, ni como instrumento de soporte a manera consultiva. Dentro de su sitio web por ahora solo se encuentra material de consulta de preguntas frecuentes y un Manual de Usuario del Registro Nacional de Bases de Datos – RNBD.

BRECHAS DE SEGURIDAD DE DATOS PERSONALES

	ESPAÑA	COLOMBIA
Contenido de la notificación de brecha de seguridad	El numeral 2 del artículo 34 del Reglamento General de Protección de Datos – RGPDN establece que, la notificación de una brecha de seguridad a los interesados se debe hacer a través de una comunicación que utilice un lenguaje claro y sencillo, en ella se deberá indicar: **i)** el nombre y los datos de contacto del delegado de protección de datos y demás datos de contacto para información; **ii)** la descripción de posibles efectos y **iii)** la descripción de las medidas adoptadas, incluidas aquellas de mitigación propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales. En cuanto a la notificación a la autoridad competente, según el artículo 33 del RGPDN, esta debe contener la misma información que la emitida a los interesados más la descripción de la naturaleza de la violación de la seguridad de los datos personales, y en posible, las categorías y el número aproximado de interesados afectados	la Guía para la gestión de incidentes de seguridad en el tratamiento de datos personales de la SIC indica que las comunicaciones deben ser suficientemente claras y precisas para que los titulares de la información entiendan lo delicado del incidente y así, tomen las medidas que consideren apropiadas en pro de la protección de sus datos, no obstante, no precisa de manera clara su contenido. Ninguna norma lo hace. Ahora, en lo que respecta a la notificación a la autoridad competente para conocer el asunto, es decir la SIC, no encontramos con el mismo vacío normativo aclarando que, se pude solventar de manera parcial con lo establecido en la Guía para implementación del Principio de la responsabilidad Demostrada (*Accountability*), pues referencia que como mínimo debe informarse el tipo de incidente, la fecha de la que ocurrió, la fecha en la que se tuvo conocimiento, la causal, el tipo de dato personal comprometido y la cantidad de titulares afectados.

Roles y Responsabilidades en la notificación y manejo de Brechas de Seguridad

BRECHAS DE SEGURIDAD DE DATOS PERSONALES

ESPAÑA	**COLOMBIA**
Los artículos 24 y 28 del Reglamento (UE) 2016/679 determina de manera general varias de las obligaciones de los responsables y de los encargados de los datos personales, pero son los artículos 33 y 34 de dicho Reglamento los que particularizan las responsabilidades de tales roles frente a la existencia de una brecha de seguridad. Ahora frente a lo que corresponde al delegado de protección de datos se tiene por base lo referido en el artículo 39 del Reglamento (UE) 2016/679. Dicho lo anterior, tenemos por responsabilidades para cada rol las siguientes: **DELEGADO DE PROTECCIÓN DE DATOS:** - Comunicar y advertir al responsable/encargado del tratamiento sobre sus deberes y compromisos relacionados con las brechas de datos personales. - Cooperar con la entidad de inspección en lo referente a gestión de brechas de datos personales. - Ser el canal de comunicación con la entidad de inspección competente.	Según Los artículos 17 y 18 de la Ley 1581 de 2012 dentro de los roles y responsabilidades frente al manejo de brechas de seguridad encontramos: **ENCARGADO:** - Tramitar las consultas y reclamos. - Informar a la SIC cuando se generen situaciones que vayan en contravía de los parámetros de seguridad establecidos y que además impliquen peligros que afecten los datos de los titulares. - Cumplir las instrucciones y requerimientos que imparta la SIC. **RESPONSABLE:** - Requerir al encargado, la obediencia de los contextos de seguridad y privacidad de la información de los titulares. - Gestionar las peticiones y reclamos. - Anunciar a la autoridad cuando se conozca alguna violación a los códigos de seguridad y se den dificultades en la gestión de la información de los titulares. - Obedecer las indicaciones y lineamientos de la SIC

ENCARGADO: - Informar al responsable de las brechas de datos personales. - Ayudar al responsable en la gestión de la brecha de datos personales. **RESPONSABLE:** - Implantación del proceso de gestión de brechas. - Evaluación de las consecuencias para los derechos y libertades de las personas. - Notificar la brecha de datos personales a la Autoridad de Control.	Si bien la Ley 1581 de 2012 no relaciona ningún otro rol en materia de protección de datos personales, la Delegatura para la Protección de Datos Personales de la SIC hace algunas recomendaciones para el nombramiento y definición de funciones de un **OFICIAL DE PROTECCIÓN DE DATOS PERSONALES - OPD**, lo anterior en concordancia con el numeral 2.2.2.25.4.4. del Decreto Único Reglamentario 1074 de 2015, del Sector Comercio, Industria y Turismo, en el que refiere que todo responsable y encargado del tratamiento está en el deber de elegir a una persona natural o una dependencia que ostente el encargo de proteger los datos personales y gestionar las peticiones elevadas por los titulares, no obstante, en tal documento no se refiere ninguna obligación para el OPD en materia de brechas de seguridad.

(Elaboración propia)

4.2 Análisis comparativo entre España y Colombia- Responsabilidad penal de la persona jurídica

La responsabilidad penal de las personas jurídicas fue incluida en el Código Penal Español con la modificación del año 2010, según el artículo 31 bis de dicha norma las personas jurídicas son penalmente responsables cuando: **a)** los delitos son ejecutados en su favor de manera directa o indirecta por representantes legales o por quienes de forma individual o como miembro de un cuerpo colegiado de la persona jurídica, están acreditados para tomar decisiones u ostentan facultades de organización y control. **b)** los delitos son realizados en el

desarrollo de funciones sociales y por cuenta y en beneficio directo o indirecto de quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, permitieron la ejecución por incumplimiento de sus obligaciones.

Así como en España, en muchos países de Europa y de Suramérica se han realizado reformas de las normatividades penales para incorporar la responsabilidad penal de la persona jurídica, pues esta introducción esta derivada de la necesidad de tener modelos de organización solidos con políticas *compliance* y de gestión de prevención desde el contexto penal.

En Colombia desde el legislativo esta temática fue normada, en su momento, mediante el artículo 26 de la Ley 491 de 1999, que consagró la responsabilidad penal de las personas jurídicas, sin embargo, dicho artículo fue declarado inexequible por la Corte Constitucional con la Sentencia C-843 de 1999, por considerarse que vulneraba el principio de legalidad.

La idea de atribuir responsabilidad penal a las personas jurídicas ha tenido por derroteros el elemento de la acción y el principio de culpabilidad (imputabilidad, capacidad de motivación, el poder de decisión de obrar de otra manera). Se debe reconocer que Colombia de manera alineada con las recomendaciones de la Asociación Internacional de Derecho Penal, ha establecido una serie de consecuencias accesorias para las personas jurídicas, tales como clausura, y disolución de la sociedad aplicables a las sociedades en cuyo seno se han cometido los actos punibles, no obstante, considero que así como se dan una potestades de especial protección a las personas jurídicas de naturaleza privada mediante los articulo 38 y 58 de la Constitución Política a las mismas se les debían imponer obligaciones de cara a no realizar acciones que terminen en hecho delictivos, máxime cuando los daños causados son producto de los defectos de la estructura de la administración (BAZZANI MONTOYA 2001).

En el ámbito de la criminalidad organizacional la necesidad de contar con nuevas herramientas jurídicas enfocadas a la responsabilidad penal constituidas en atención a la realidad nacional y mundial para enfrentar los desafíos económicos de la digitalidad, es inminente, por lo que desarrollar buenas prácticas y estrategias político criminales en ocasión a la comisión de delitos penales y en desarrollo de una actividad empresarial, reclama un abordaje integrador y seguro (RAMÍREZ 2021). Así pues, a continuación, se abordará un análisis comparativo normativo con visiones diferentes desde donde el modelo español brindará importantes elementos que pueden servir de parámetros orientadores y esclarecedores para la regulación colombiana.

Tabla 3. Análisis comparativo entre España y Colombia- Responsabilidad penal de la persona jurídica

RESPONSABILIDAD PENAL DE LA PERSONA JURÍDICA

	ESPAÑA	**COLOMBIA**
Cuando se habla de responsabilidad penal de la persona jurídica	Muchos han sido los cuestionamientos de tener en la legislación la incorporación de tal responsabilidad, entre estos, se encuentra la "dificultad" o la inviabilidad de que se ejerza una debida defensa y por tanto se considere que exista vulneración al debido proceso, en tal sentido en España se realizó la introducción del artículo 786 bis de la LECrim, mediante el cual se establece que se podrá elegir por el colectivo la persona que se considere pueda comparecer ante el juzgado quien además no deberá tener intereses contrapuestos con los intereses de la persona jurídica. Esta norma, además, se hace extensa con el artículo 839 bis de la Ley de Enjuiciamiento Criminal, la cual dispone que, de existir resistencia de comparecer por parte de la persona jurídica, y por tanto no se presenta a la autoridad judicial, la persona jurídica será declarada rebelde y el trámite judicial continuará.	EL ordenamiento jurídico colombiano cuenta con dos normatividades desde la jurisdicción penal que sancionan la comisión de personas jurídicas por conductas punibles, encontramos así, el artículo 91 de la Ley 906 de 2004 que establece que el juez de control de garantías ordenará a la autoridad competente la suspensión de la personería jurídica o al cierre temporal de los locales o establecimientos abiertos al público, de personas jurídicas o naturales, cuando existan motivos fundados que permitan inferir que se han dedicado total o parcialmente al desarrollo de actividades delictivas. A través de la ley 211 de 2021 la norma antes referida fue adicionada en su parágrafo incluyéndose que cuando se hubiese suspendido o cancelado la personería jurídica la persona natural o jurídica estará inhabilitada para constituir nuevas personerías jurídicas y establecimientos de comercio hasta que el Juez de Conocimiento tome una decisión definitiva.

Sanciones en materia de responsabilidad penal para la persona jurídica

RESPONSABILIDAD PENAL DE LA PERSONA JURÍDICA

ESPAÑA	COLOMBIA
De conformidad con los parámetros establecidos por el artículo 31 bis una persona jurídica será responsable de los delitos comprendidos en los artículos 197, 197 bis y 197 ter, y por ello se le podrá imponer la pena de multa de seis meses a dos años. Se debe reconocer que la norma española ha tenido en cuenta varios escenarios que emiten lineamientos específicos cuando la empresa que se considere responsable penalmente sea parte de aquellas que prestan un servicio de interés económico general, precaviendo que las sanciones no repercutan en desfavorecimiento a la colectividad, como el caso de un cierre definitivo. Así pues, para tales casos se contempla de acuerdo con el artículo 31 quinquies que solamente se impondrá las penas previstas en los literales a) y g) del apartado 7 del artículo 33 es decir, multa por cuotas o proporcional e intervención judicial.	Si bien es cierto que en Colombia no existe una norma que de manera específica regule la responsabilidad penal de personas jurídicas, es tan bien cierto que desde el criterio jurisprudencial si se ha tenido análisis de ella, por ejemplo en la sentencia C- 320 de 1998, (daño al ecosistema y por ende afectación medioambiental), la alta corte indicó que, a la ley no se le prohíbe sancionar el abuso de la personalidad jurídica, que puede derivarse de la utilización del esquema societario con móviles penales o de enriquecimiento ilícito, por lo que se consideró legitimo el dar lugar a variadas reacciones del ordenamiento jurídico en relación con los actos societarios, el objeto social, el patrimonio social o la persona jurídica misma.

RESPONSABILIDAD PENAL DE LA PERSONA JURÍDICA

Modelos empresariales creados de manera preventiva a la imputación de responsabilidad penal de la persona jurídica

ESPAÑA	COLOMBIA
Resulta así pues, estar tan articulado el código penal con la necesidad de modelos de empresa para la prevención delitos, el control empresarial de las conductas de los trabajadores y directivos de la empresa, la existencia de un programa estratégico para detectarlos, la existencia de buenas prácticas de actuación, para dar respuesta a una posible infracción en el interior de la organización, es decir la existencia de *compliance* pueden llegar a determinarse como eximentes de responsabilidad según lo recogido en el apartado dos del actual artículo 31 bis del Código Penal. Por tanto, se considerará como eximente que operaria una vez probada que se ha incorporado en la organización de las personas jurídicas los modelos de prevención, y que estos han operado de forma correcta, idónea, dando	En Colombia han cursado en el Congreso de la República, varias discusiones legislativas entorno a la responsabilidad penal de las personas jurídicas, dichos proyectos de ley buscan mediante regímenes de responsabilidad penal y administrativa en las personas jurídicas, el fortalecimiento de la cultura organizacional, la prevención de los delitos empresariales y la salvaguarda del orden económico y social (RAMÍREZ. 2021) En el año 2014 la sala de casación penal de la Corte Suprema de Justicia explico algunos de los argumentos que no han permitido que en Colombia se fije una normativa solida en materia penal para la responsabilidad de las personas jurídicas, quedando únicamente disposiciones para ello en materia civil y administrativa[9]. Tales argumentos están previstos desde dos contextos el primero en el campo estrictamente dogmático, sustentado

9 Artículo 35 Ley 1778 de 2016 "Por la cual se dictan normas sobre la responsabilidad de las personas jurídicas por actos de corrupción transnacional y se dictan otras disposiciones en materia de lucha contra la corrupción" indica que cuando exista sentencia penal condenatoria contra el representante legal o las administradores de una sociedad que tenga su domicilio en Colombia o de una sucursal de sociedad extranjera, y esta ya se encuentre en firme por el delito de cohecho, en algunos casos la Superintendencia de Sociedades SIC podrá aplicar multas de hasta doscientos mil (200.000) salarios mínimos legales mensuales vigentes.

muestras que la persona jurídica ha actuado con respeto al derecho. Vale la pena resaltar del análisis realizado por la circular FGE N.º 1/2016 (sobre la responsabilidad penal de las personas jurídicas tras la reforma del Código Penal) que, si la persona jurídica carece de estructura corporativa como los negocios unipersonales tendría que pensarse en la posibilidad de imputar tan solo a la persona física, esto para evitar la doble incriminación vulnerado el principio non bis in ídem.	en el aforismo *societas delinquere non potest*- basado en la subjetivización del principio de culpabilidad, que advierte la voluntad solo a la persona humana. El segundo derivado de la imposibilidad de una rehabilitación entendida como fin fundamental de la pena. No obstante, tales argumentos no desconocen la importancia de nuevas herramientas jurídicas para enfrentar los desafíos económicos y sociales que se derivan de la globalización, tecnificación y tras nacionalidad en un contexto de delincuencia económica instituida.

(Elaboración propia)

4.3 Análisis comparativo entre España y Colombia el rol del chief information officer o experto a cargo de la seguridad informática

El 28 de enero de 2021 se realizó la publicación en el BOE de la RD 43, conocida como la ley NIS, este real decreto está enfocado en normar a los operadores de servicios esenciales, pero sin aplicación a los operadores de servicios de comunicaciones electrónicas y los prestadores de servicios electrónicos de confianza siempre y cuando no estén catalogado como operadores críticos. Esta norma supone un avance importante en materia de ciberseguridad pues refiere **la obligatoriedad de la creación de la figura del responsable de Seguridad de la Información - RSI**. El perfil del RSI al que también se le denomina CISO (*Chief Information Security Officer*) apunta a *Information Security Officer*) apunta a alguien que esté certificado en los procesos de su propia empresa, para entender que se debe proteger y con quien se debe interactuar.

En Colombia a diferencia no sucede lo mismo pues no existe una norma específica que regule directamente el cargo de Chief Information Security Officer (CISO), no obstante en vigencia

2022 la ley 2195 mediante su artículo 9, dio un salto importante en materia de *compliance*, adicionando el artículo 34-7 a la Ley 1474 de 2011 el cual, constriñe a las personas jurídicas sujetas a su examen, atención o control a adoptar programas de transparencia y ética empresarial que contengan instrumentos y normas internas de auditoría.

Tabla 4. Análisis comparativo entre España y Colombia el rol del *Chief Information Officer* o experto a cargo de la seguridad informática

CHIEF INFORMATION OFFICER

	ESPAÑA	**COLOMBIA**
El CISO en el sector empresarial	En materia empresarial en España el **CISO** tiene un importante rol a desarrollar pues su principal función en desplegar una estrategia de seguridad con medidas de protección adecuadas y en todo caso alinea con los objetivos comerciales. Este profesional debe tener estricta relación comunicación con las áreas de TI, seguridad y negocio (CAMPANA 2023).	Si bien en Colombia no encontramos una norma que desde el contexto nacional imponga a las empresas en general la obligación de incorporar dentro de su estructura organizacional un CISO, el Ministerio de las Tecnologías de la Información y las Comunicaciones - MinTIC ha impulsado un espacio junto a la plataforma de educación en línea Platzi un espacio de capacitación para los directores de Sistemas de Información y de Seguridad de la Información, quienes fungen en la mayoría de los casos como CISO, como estrategia para que aminorar los riesgos relacionados con la información de las empresa y trazar entornos que permitan dar continuidad de negocio (CIBERILATAM 2021)**.**

(Elaboración propia)

Aquí resulta interesante ver como desde el Ministerio de las Tecnologías de la Información y las Comunicaciones - MinTIC se entregan recursos para aportar formación al personal de las empresas interesadas en la protección de la ciberseguridad, pero no se dedican esfuerzos a sacar regulaciones que por lo menos obligue a los sectores más críticos y que impacten en las necesidades básicas de la población al prestar algunos tipos de servicios a tener dentro de su estructura un responsable de Seguridad de la Información – RSI o CISO.

Es España el panorama es muy diferente pues los retos a hoy no radican en tener o no un CISO dentro de la estructura organizacional, sino de los desafíos de las temáticas a empleados sobre los riesgos potenciales del uso de IA generativa pues, por ejemplo**,** si un empleado pide ayuda a ChatGPT para escribir una comunicación a un proveedor, la plataforma necesitará obtener cierta información personal de ese cliente, para poder proyectarla, eso conlleva a que, los datos estarán en los servidores de OpenAI durante el tiempo de elaboración, así pues de manera puntual la apuesta debe estar enfocada en concientizar y trasladar los controles que se necesitan implementar (ASOCIACIÓN ESPAÑOLA DE EMPRESAS DE CONSULTORIA 2023).

5. DE LEGE FERENDA (recomendaciones) para fortalecer el sector empresarial basadas en los dos sistemas jurídicos comparados

Nada más conveniente que soportar las recomendaciones a realizar en los principios promulgados por Paris en el llamado de 2018, que se realizó por el presidente de la República Francesa, Emmanuel Macron, durante el Foro de Gobernanza de Internet celebrado en la UNESCO y el Foro de Paz de París.

Este llamado es a la unidad y la cooperación entre Estados, socios del sector privado, el mundo de la investigación y la sociedad civil a través de nueve principios comunes para proteger el ciberespacio. De los nueve principios establecidos he considerado enfocar las recomendaciones en el panorama previsto por tres de ellos, a saber: **principio No. 7** "Higiene cibernética", enfocado en la necesidad de fortalecer una ciberhigiene avanzada para todos los actores; **principio No. 8** " Sin hackeo privado", el cual tiene por alcance el generar acciones para impedir que los agentes no estatales, que incluye el sector privado, realicen ataques para sus propios propósitos o los de otros agentes no estatales; ; **principio No. 9** "Normas internacionales", cuyo fin es implementar normas internacionales de actuación responsable, así como medidas de fomento de la cordialidad y credibilidad en el ciberespacio.

5.1 Referencia a propuestas para futuras leyes, políticas o lineamientos que contribuyan al fortalecimiento de la ciberseguridad en el sector empresarial de España.

- Dado que España se encuentra en un momento de organización normativa, junto con un análisis dedicado y constante a distintas temáticas en ciberseguridad y con una fase próximas de consumación en la transformación digital de la empresa, del emprendimiento digital y del sector público, la emisión de la Estrategia Nacional de Inteligencia Artificial es totalmente pertinente.

  El uso correcto de este campo científico podrá desembocar en importantes herramientas de seguridad que comprendan el funcionamiento y existencia de amenazas, trabajando de la mano con una responsable gestión de los datos personales y de la ética del individuo humano, pues, **sería de gran utilidad**, reducir al mínimo los falsos positivos, de forma que los avisos generen una preocupación real y provoquen

una inspección manual profunda (MESEGUER GONZÁLEZ, y LÓPEZ DE MÁNTARAS BADIA 2017).

De tal forma la recomendación está orientada a emitir una política mediante la cual se obligue en principio a algunos de los sectores más críticos y por ende más conscientes de la necesidad de seguir caminando en pro de la ciberseguridad a generar inversión en materia de Inteligencia Artificial, no obstante, para ello se debe fijar desde el Gobierno Español una normativa necesaria para permitir sandboxes regulatorios para probar la aplicación de la Inteligencia Artificial a quienes han invertido y son competentes para ello.

- Crear una Política que incite a la **cultura de ciberseguridad en las organizaciones**, especialmente en las pymes, creando incluso sanciones para quienes permitan ciertos incidentes de seguridad que a hoy no deberían ocurrir y que se generan en virtud del uso inadecuado de las tecnologías de la información, ello incluiría el incumplimiento de las rutinas de ciberhigiene mínimas en los sistemas computacionales. En este aspecto es importantísimo **el educar al sector empresarial en riesgos** para lograr trasmitir que el no poner frente a la ciberseguridad implica la perdida de activos como datos y propiedad intelectual, lo que conllevaría a una imposibilidad de operación.
- Se debe fijar una **normatividad de seguimiento y control** para las pymes con el fin de poder identificar el grado de ejecución de las medidas implementadas para la seguridad de la información y corregir las desviaciones significativas.
- Considero que **seguir creciendo en el desarrollo de normatividades de estricto cumplimiento** para el sector empresarial es una necesidad urgente, por cuanto algunos sectores están apartados de la ciberseguridad al no ser un foco de ataque o pensar que los riesgos no son tan impactantes. Las normas técnicas como reglas a ser adoptadas de manera voluntaria por las partes interesadas, no son la solución, por el contrario, reflexiono en que estas pueden llevar solo al nivel de certificación sin tener de fondo una implementación real y productiva.

5.2 Referencia a propuestas para futuras leyes, políticas o lineamientos que contribuyan al fortalecimiento de la ciberseguridad en el sector empresarial de Colombia.

- La expedición de una **Ley de Ciberseguridad Nacional**, como un apropiado marco normativo que provea una importante credibilidad en el uso de las TIC**,** fortalecería la adecuada gestión de los riesgos asociados a ciberseguridad empresarial y permitiría el lograr alcanzar un entendimiento de la necesidad de utilizar herramientas para la protección de su información, sistemas y servicios, pues la estandarización de la ciberseguridad puede considerarse no solo una cuestión estratégica dentro de las organizaciones, sino además una medida de costo beneficio.

  Adoptar el modelo español del código de derecho de la ciberseguridad, conllevará a que la población le dé la importancia que merece al observar un contexto jurídico robusto, claro, completo y apartado de permitir cualquier interpretación alejada de la voluntad del legislador.

  Adicional a ello, es recomendable que dicha normativa indique en materia empresarial la autoridad competente a la que se debe compartir las respectivas evidencias de la existencia de las políticas y determinar las sanciones respectivas por incumplimiento.

  Dado que los ciberdelitos son tan cambiantes y todas las esferas de la ciberseguridad también lo son, tener un instrumento único permite que la actualización sea más rápida, coherente y organizada. Además, este documento se podría utilizar como una carta de navegación en el tema para aplicación y análisis de la materia permitiendo a los profesionales del derecho tener un panorama claro sobre el cual trabajar para proponer nuevas normativas a fin de lograr una adecuada protección empresarial en donde se garantiza a través del artículo 58 de la constitución política, la propiedad privada y otras garantias adquiridas a traves de las normas de derecho privado, que no pueden ser desconocidas ni quebrantadas por nuevas disposiciones.
- En lo que corresponde a **datos personales**, actualmente, está siendo revisado el proyecto de ley número 153 del 2023 para actualizar la ley 1581 de 2012, que está basado según su capítulo séptimo, en el Reglamento General de Protección de Datos, reconociendo su estructura de marcos normativos sólidos con elevados estándares de

privacidad y seguridad en el procesamiento de datos personales. Dada esta adopción el nuevo esquema propuesto pasa de 30 artículos a 108 artículos.

La propuesta de actualización de la norma contine algunos temas álgidos y sobre los cuales Colombia no tiene avances sólidos y legalizar sobre ello, podría llegar a ser bastante confuso. Así pues, el proyecto antes referido en su artículo 90, indica que quienes desarrollen o hagan uso de la neurotecnologia deberán garantizar la protección de los derechos fundamentales a la intimidad de las personas, haciendo referencia a los neuroderechos sin ni siquiera abordar su concepto. Vale la pena resaltar que temáticas como esta requiere un amplio análisis ético que a la fecha en Colombia no existe.

- Frente a **seguridad de la información**, se debe decir que Colombia no tiene una normatividad especifica que regule esta temática de manera particular, pues solo encontramos algunos parámetros generales de aplicación un tanto antiguos como: **i)** la Ley 1341 de 2009, mediante la cual se establecieron principios y conceptos sobre la sociedad de la información y las TIC, **ii)** la Ley 1273 de 2009, que crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos", **iii)** la Ley 1712 de 2014, que crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y **iv)** algunos parámetros internacionales como los establecidos a través del Convenio sobre la Ciberdelincuencia de Budapest adherido a partir del 16 de marzo de 2020.

  Con el nuevo gobierno nacional se promulgó el Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad", que incluyó la Transformación Digital Pública para las entidades estatales del orden nacional a través de la obligación de crear planes de acción que incorporen mecanismos coligados a tecnologías emergentes, determinados como aquellos de la Cuarta Revolución Industrial, sin embargo, dentro de los proyectos y principios estratégicos de transformación digital incluidos en dicho plan específicamente en el artículo 147 ninguno hace referencia a la seguridad de la información, situación que se recomienda sea revisada por cuanto nada se hace con tener políticas para priorizar el uso de las tecnologías emergentes de la cuarta revolución para prestar los servicios del estado sin determinar medidas mínimas de seguridad para la información que viajará a través de ellas.

Si bien en 2009 la ley 1341 a través del artículo cuarto indico como una obligación del estado la Intervención en el sector de las Tecnologías de la Información y las Comunicaciones, especialmente, en el desarrollo de los principios de intervención contenidos en la Constitución Política, para proteger los derechos de los usuarios, velar por la calidad, eficiencia y adecuada provisión de los servicios, y la promoción de la digitalización, 13 años después con el Plan Nacional de Desarrollo 2018- 2022. "Pacto por Colombia, Pacto por la Equidad", se incluye nuevamente este compromiso, pero esta vez delegada a cada una de las entidades del sector público para que a través de la creación de planes de acción se lleven los procesos a una Transformación Digital Pública. Trece años en los que se sigue hablando de procesos digitales de uso de las tecnologías de la información y no se indican de manera clara el deber de tener medidas de seguridad.

En conclusión, la recomendación particular en este contexto está determinada en la necesidad de generar una normatividad especifica en la que se indique de forma albúmina cuál es el equipo de respuesta a incidentes de seguridad informática de referencia, las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales y el rol en el que recaerá tal compromiso

- Considerando que para Colombia el punto de quiebre de los ciberataques a empresas, en gran medida está en la **falta de capacitación** y **cultura en ciberseguridad**, se hace necesario estructurar un programa que permita el obtener conocimientos e informar a las organizaciones de todos los sectores (pero realizando un cronograma por sectores atendiendo de manera principal aquellos que tienen estricta relación con los servicios públicos) cuales son las estrategias necesarias para anticipar los ataques, tocando tanto la esfera de la detección como la necesidad de implementar medidas de seguridad.

  El modelo que se recomienda es bajo una estructura semejante a la desarrollada en 2020 por el Centro Criptológico Nacional, bajo un portal de formación y cultura de ciberseguridad denominado ÁNGELES. Dicho portal, ofrece de manera gratuita formación básica y cursos de gestión o de especialización flexible (comenzar y finalizar los cursos de su interés en el momento que decida) en diferentes materias relacionadas con ciberseguridad y tecnologías de la información.

Esta recomendación además de apuntarle a impulsar la cultura en ciberseguridad y obtener resultados de buenas prácticas en el sector corporativo impulsa el perfeccionamiento profesional de perfiles profesional en materia de derecho digital e ingeniería informática fomentando la promoción y conservación de estos escasos talentos.

- Si bien en materia de *complience* Colombia ha avanzado mediante la ley 177 de 2016, entrando un poco más en el mundo de la responsabilidad administrativa de las personas jurídicas, los programas de cumplimiento necesitan ser abordados de manera interdisciplinar por lo que es inminente el abordar el derecho penal desde una concepto más moderno, pues suponer modelos orientados a la prevención en ciberdelincuencia y al fortalecimiento de medidas que cultiven la ética empresarial conllevan la necesidad de generar tanto reglas de cumplimiento obligatorio como sanciones por su no aplicación o por consumación.

Figura 7 "propuestas normativas (leyes, políticas o lineamientos) que contribuyan al fortalecimiento de la ciberseguridad en el sector empresarial de Colombia" (Elaboración propia)

5.3 recomendaciones conjuntas

- Nada más conveniente que la propuesta presentada el 18 de abril de 2023 por la Comisión Europea, referente a la necesidad de aprobar una la Ley de Cibersolidaridad *(Cyber Solidarity Act*), cuyo objeto es el reforzar la solidaridad entre los diferentes Estados Miembros compartiendo información respecto de las buenas prácticas para reaccionar de manera adecuada ante la presentación de incidentes de ciberseguridad, este tipo de ciberescudo tiene proyectado incluso servir con ayuda financiera a fin de dar asistencia mutua entre estados miembros. Si bien, Colombia no hace parte directa de la Unión Europea como si lo es España este primero tiene importantes alianzas que considero conllevan a que como aliado pueda tener una participación importante a través de la nueva ley de Cibersolidaridad por lo que sería ideal que la EU tenga en cuenta la posibilidad de tener esa proyección de elaboración encendida a más Estados preocupados e interesados en la ciberseguridad. Considero que esta extensión es prudente no solo por ir en línea de su objeto "refuerzo de la solidaridad" si no, además, por su necesidad práctica, pues no se puede pasar por alto la importante relación productiva derivada del Acuerdo Comercial entre Colombia y la UE que va más allá del comercio abarcando temáticas como la protección del medio ambiente, los derechos humanos, medidas arancelarias, servicios y propiedad intelectual.
- Promover un pensamiento con enfoque crítico en ciberseguridad ayuda a detectar patrones y comportamientos inusuales que podrían indicar un ataque; el pensamiento crítico permite a los profesionales con roles de responsabilidad o consultoría el adaptarse rápidamente a los cambios, aprendiendo nuevas técnicas y consiguiendo herramientas para gestionar posibles riesgos. Ahora en lo que refiere a los ciudadanos conllevaría a seleccionar de manera adecuada la información, por cuanto esta no resulta ser siempre cierta y por el contrario desinforma. Aquí, es inminente comprometer a los medios de comunicación por su papel relevante en el intercambio de información y la influencia en la sociedad.

6. Conclusiones

Las siguientes conclusiones dan respuesta a los objetivos planteados al inicio del documento, si bien el primero está proyectado para avistar los retos normativos en materia de ciberseguridad particulares para España y Colombia, estos, han sido tocados en el último capítulo del texto de manera especial, por lo que las disoluciones a continuación listadas consuman de manera puntual el estado de la ciberseguridad en el sector empresarial de cada país (España y Colombia) en procedimientos y en normatividad.

Primera. – La ciberseguridad bien desenvuelta acelera la innovación y la creación de valor en todas las empresas, pues no se tendrían obstáculos al momento de desarrollar nuevos proyectos innovadores y de transformación, por tanto, un país con un marco normativo solido en materia de ciberseguridad corresponde a un Estado preparado para abrir nuevos ingresos y oportunidades de mercados con total confianza en quienes además desean invertir.

Segunda. **–** España ha sido país pionero en la estructuración de normatividades de ciberseguridad, si bien ha tomado algunos asuntos de buenas prácticas de otros países de la Unión Europea, su reglamentación esta desarrollada a la par de las necesidades de sus sectores económicos y avance en el uso de las tecnologías de su población, su reglamentación a sido constante y se agrupa en un solo cuerpo normativo llamado código del derecho de la ciberseguridad, lo que permite su congruencia temática en distintas áreas y al momento de generarse una actualización la identificación de apartados para su modificación es más sencilla, lo que replica en tiempos más reducidos para tales ajustes y poder caminar siempre en la actualidad y en la respuesta a las necesidades del mundo digital.

Tercera. **–** Como se pudo referenciar a lo largo del texto Colombia a tenido importantes intensiones en materia de Ciberseguridad, pues siendo un país que pone su atención en la economía y en las alianzas que se necesita para poder impulsarla, le termina siendo obligatorio ir a la marcha de la prevención de la ciberdelincuencia, sin embargo, las políticas fijadas se han quedado en copiar modelos además amputados para mostrarse sencillos al momento de su acogimiento. Tal situación, acaba siendo totalmente perjudicial pues no existe seguridad jurídica al momento de intentar su adopción, pues muchos elementos quedan a la interpretación con posibilidades de que al momento de su ejecución vaya en contravía de la intensión del legislador.

Cuarta. **–** Se encontraron tres grandes cuestiones que tiene importancia en el sector empresarial y que son bastante disimiles en los países analizados, el manejo de las brechas de seguridad de datos personales, la responsabilidad penal de la persona jurídica, y el ejercicio del experto a cargo de la seguridad informática. De tal análisis se pudo ultimar que para Colombia estos son escenarios de importante atención para el legislativo pues el panorama actual normativo no conlleva una adecuada protección de los activos digitales y la información sensible de una empresa.

Referencias bibliográficas

Bibliografía básica

ANGUITA OSUNA, J. <<Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea>>: *Revista de estudios en seguridad internacional*. 2018, Vol. 4, Nº. 1 , pp. 107-126. [consulta: 6 de noviembre de 2023]. ISSN-e 2444-615.Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6526292

ARROYO GUARDEÑO, D., MARTINEZ, GAYOSO, V. y HERNÁNDEZ ENCINAS, L. (2020). Ciberseguridad: (ed.). Editorial CSIC Consejo Superior de Investigaciones Científicas. Disponible en: https://bv.unir.net:2769/es/ereader/unir/172144

BAUTISTA GARCIA, F., GUZMÁN MESA, L. y BLANCO, L. *Informe anual de Ciberseguridad*. Comportamiento de las cifras del ciberdelito 20221-2023. CCTI.2023.

BAZZANI MONTOYA D. <<Análisis constitucional de la responsabilidad penal de las personas jurídicas>> 2001[consulta: 27 de noviembre de 2023]. Disponible en: file:///C:/Users/proyecto.usta/Downloads/Dialnet-AnalisisConstitucionalDeLaResponsabilidadPenalDeLa-5312259%20(1).pdf

BOLLERO, D. <<Los misiles se imponen a la ciberguerra>> 2022. [consulta: 28 de septiembre de 2023]. Disponible en: http://www.insumisos.com/L3CTUR45/2022/LECTURAS-1A-MARZO-2022.pdf

BRIGARD URRUTIA. <<Panorama General de la Ciberseguridad>>.2023[consulta: 25 de septiembre de 2023]. Disponible en: https://bu.com.co/es/insights/noticias/panorama-general-de-la-ciberseguridad

CANDAU, J. <<Ciberseguridad. Evolución y tendencias>>. Instituto Español de Estudios Estratégicos, IEEE.ES. 2021, pp 1-36. [consulta: 25 de septiembre de 2023]. Disponible en:https://www.ieee.es/Galerias/fichero/docs_marco/2021/DIEEEM11_2021_JAVCAND_Ciberseguridad.pdf

CAMPANA, N. << ¿Qué hace un Chief Information Security Officer (CISO)? >> 2023. [consulta: 05 de diciembre de 2023]. Disponible en: https://www.freelancermap.com/blog/es/que-hace-chief-information-security-officer-ciso/

CAVADA HERRERA, J. << Cibercrimen y delito informático: Definiciones en legislación internacional, nacional y extranjera>> *Biblioteca Nacional del Congreso de Chile/BCN.* 2020. [consulta: 25 de septiembre de 2023]. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/29012/2/Definicion_y_regulacion_de_cibercrimen_y_delito_informatico_JPC_edit.pdf

CIBERILATAM <<Colombia refuerza la formación en seguridad digital de los CIO y CISO>>. 2021. [consulta: 06 de diciembre de 2023]. Disponible en: https://www.segurilatam.com/actualidad/ciberseguridad-colombia-refuerza-la-formacion-en-seguridad-digital-de-los-cio-y-ciso_20210504.html

CORTÉS BORRERO, R. <<Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia>>. Revista de derecho, comunicaciones y nuevas tecnologías, Nº. 14, 2015, pp. 1-17[consulta: 06 de noviembre de 2023]. disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7496888

CUJABANTE VILLAMIL, X. *et al* <<Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares>>. Revista Científica General José María Córdova (Revista colombiana de estudios militares y estratégicos) Bogotá D.C., Colombia.2020. Volumen 18, número 30, pp. 357-377 [consulta: 06 de noviembre de 2023]. ISSN 1900-6586 (impreso). Disponible en: https://revistacientificaesmic.com/index.php/esmic/article/view/588/666

DEL REAL, C. <<Panorama institucional de la gobernanza de la ciberseguridad en España>> *Revista de Estudios Jurídicos y Criminológicos*, 2022, No. 6, pp. 15-51 [consulta: 29 de noviembre de 2023]. ISSN-e 2660-7964. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8753130

DELOITTE. << El estado de ciberseguridad en España>>. 2022. [consulta: 04 de diciembre de 2023]. Disponible en: https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html

EL ECONOMISTA << Usuarios denuncian hackeo de sus cuentas de Disney Plus>>. 2019. [consulta: 25 de septiembre de 2023]. Disponible en: https://www.eleconomista.net/economia/Usuarios-denuncian-hackeo-de-sus-cuentas-de-Disney-Plus-20191120-0017.html#google_vignette

GARCÍA LINARES, R. <<Estamos a un paso del metaverso. Cambios en las redes sociales>> Gaceta CCH. UNAM. 2022. [consulta: 3 de noviembre de 2023]. Disponible en: https://gaceta.cch.unam.mx/es/estamos-un-paso-del-metaverso

GARRIGA DOMÍNGUEZ, A. *Nuevos retos para la protección de datos personales: en la era del Big Data y de la computación ubicua* (ed.). Dykinson. (2016). [consulta: 17 de noviembre de 2023]. Disponible en: https://bv.unir.net:2769/es/lc/unir/titulos/58235

GÓMEZ HERVÁS, N. *Normativa de Ciberseguridad* [en línea*]* (1 ed.). RA-MA Editorial. (2021). [consulta: 18 de noviembre de 2023]. Disponible en: https://bv.unir.net:2769/es/lc/unir/titulos/222663

IT RESELLER. <<España es uno de los países que más ciberataques detecta>>. 2023 [consulta: 4 de diciembre de 2023]. Disponible en:
https://www.itreseller.es/seguridad/2023/08/espana-es-uno-de-los-paises-que-mas-ciberataques-detecta

IT RESELLER. << Las empresas españolas han perdido el 8% de sus ingresos debido a ciberataques >>. 2023 [consulta: 4 de diciembre de 2023]. Disponible en:https://www.itreseller.es/seguridad/2023/11/las-empresas-espanolas-han-perdido-el-8-de-sus-ingresos-debido-a-ciberataques

IT RESELLER. <<El 39% de las empresas españolas considera alta su exposición a los ciberataques>>. 2023 [consulta: 4 de diciembre de 2023]. Disponible en: https://www.itreseller.es/seguridad/2023/12/el-39-de-las-empresas-espanolas-considera-alta-su-exposicion-a-los-ciberataques

LA NACIÓN. <<Cinco años de cárcel para el ladrón que se apoderó de las cuentas de Twitter de Bill Gates y Elon Musk para organizar una estafa con bitcoin>>.

LA REPÚBLICA <<EPM, Sanitas y Afinia continúan en jaque por ataque cibernético contra sus sistemas >>. 2022 [consulta: 26 de septiembre de 2023]. Disponible en: [consulta: 29 de septiembre de 2023]. Disponible en: https://www.lanacion.com.ar/tecnologia/cinco-anos-de-carcel-para-el-ladron-que-se-apodero-de-las-cuentas-de-twitter-de-bill-gates-y-elon-nid26062023/

LA REPUBLICA https://www.larepublica.co/empresas/epm-sanitas-y-afinia-continuan-en-jaque-por-ataque-cibernetico-contra-sus-sistemas-3513721

LINARES, F., BLANCO, A. y HERRERA RUBIO, C. <<La importancia de la ciberseguridad en las empresas de seguros en España >>. 2023 [consulta: 26 de septiembre de 2023].

Disponible en: https://www.linkedin.com/pulse/la-importancia-de-ciberseguridad-en-las-empresas-seguros-espa%c3%b1a-z640f/?originalsubdomain=es

LLEDO YAGUE, F. BENITEZ ORTÚZAR, I. y MONJE BALMASEDA, O. *La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0: los desafíos jurídicos, éticos y tecnológicos de los robots inteligentes* [en línea]. (ed.). Madrid, Dykinson. 2021 [consulta: 25 de septiembre de 2023]. Disponible en: https://bv.unir.net:2769/es/ereader/unir/189569?page=81

Ministerio de Educación Nacional de Colombia. <<Guía de implementación de la política gobierno digital, Ministerio de Educación >> 2023. [consulta: 18 de octubre de 2023]. Disponible en: https://www.mineducacion.gov.co/1780/articles-398739_recurso_22.pdf

Ministerio de Relaciones Exteriores. << Agenda 2030 Lograr el desarrollo sostenible en un mundo diverso>> 2016 [consulta: 18 de octubre de 2023]. Disponible en: https://www.cancilleria.gov.co/sites/default/files/Fotos2017/ods-version_digital-web-2017.pdf

MESEGUER GONZÁLEZ, P. y LÓPEZ DE MÁNTARAS BADIA, R. *Inteligencia artificial*. (ed.). Madrid, Spain: Editorial CSIC Consejo Superior de Investigaciones Científicas. (2017). 2022 [consulta: 17 de noviembre de 2023]. Disponible en: https://bv.unir.net:2769/es/ereader/unir/42319?page=8

Política de Operación, Proceso de Tecnologías de la Información. V. 8 2021. Disponible en: https://www.funcionpublica.gov.co/documents/34645357/34703081/Politica_de_operacion_v8.pdf/51801258-9e11-43b7-85cb-c942e9d669e6?t=1658857188654

PORTAFOLIO <<Ataque informático a Sanitas no comprometió información de usuarios>>. 2022 [consulta: 17 de noviembre de 2023]. Disponible en: https://www.portafolio.co/negocios/empresas/eps-sanitas-detalles-del-ciberataque-que-sufrio-grupo-keralty-575968

Presidencia del Gobierno e España <<Estrategia Nacional de Ciberseguridad, Gobierno de España>>. 2019. [consulta: 5 de octubre de 2023]. NIPO (edición on-line):042-19-0129-4. Disponible en:https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

Presidencia del Gobierno de España <<Estrategia de Seguridad Nacional (ESN), Gobierno de España>> Catálogo de publicaciones de la Administración General del Estado. 2021.

[consulta: 5 de octubre de 2023]. NIPO (edición on-line) 089210375. Disponible en: https://www.dsn.gob.es/sites/dsn/files/ESN2021%20Accesible_1.pdf

PwC << Los líderes corporativos unidos para lograr la ciberseguridad, Global Digital Trust Insights)>>. 2023 [consulta: 06 de diciembre de 2023]. Disponible en: https://www.pwc.com/co/es/publicaciones/digital-trust-insights/2023/dti-2023-version-completa.pdf

RAMÍREZ P. <<La responsabilidad penal de las personas jurídicas y *compliance* en Colombia: realidades y desafíos>>. *UNA Rev. Derecho.* 2021. Vol. 6 (2). pp. 97-124. [consulta: 21 de noviembre de 2023]. ISSN 2539-5343 Disponible en: http://hdl.handle.net/1992/54874

SAN JOSE, J. <<España logra el 4º puesto a nivel mundial en el Índice Global de Ciberseguridad 2020>> 2021. [consulta: 25 de septiembre de 2023]. Disponible en: https://derechodelared.com/espana-indice-global-de-ciberseguridad-2020/

SEGURIDAD 360 <<Top 17 de las mejores empresas de Ciberseguridad en Colombia >>. 2022 [consulta: 06 de diciembre de 2023]. Disponible en: https://revistaseguridad360.com/destacados/empresas-de-ciberseguridad-en-colombia/

TEJERINA, O. y BELTRÁN, M. (2020). Aspectos jurídicos de la ciberseguridad. (1 ed.). Paracuellos de Jarama, Madrid, RA-MA Editorial. [consulta: 5 de octubre de 2023]. Disponible en: https://bv.unir.net:2769/es/ereader/unir/222712?page=427.

<<Cinco años de cárcel para el ladrón que se apoderó de las cuentas de Twitter de Bill Gates y Elon Musk para organizar una estafa con bitcoin: Joseph O'Connor, uno de los responsables de la estafa difundida en Twitter usando cuentas de personas conocidas durante julio de 2020, fue sentenciado a cinco años de cárcel>>. *La Nación* [online]. 2023 ProQuest Central. Disponible en: https://www.proquest.com/docview/2829639011/fulltext/452ACB8B92304765PQ/1?accountid=142712

Bibliografía complementaria

ÁVILA, A. <<Costo de pólizas por ciberseguridad subió hasta 25 por ciento tras pandemia, Milenio, México>> *Milenio*. 03 de agosto de 2022. Disponible en:

https://www.milenio.com/negocios/precio-ciberseguridad-aumento-pandemia-lockton-mexico

BELTRÁN, M. Y SEVILLANO, F. *Ciberseguridad industrial e infraestructuras críticas* [en línea]. (1 ed.). Paracuellos de Jarama, Madrid, RA-MA Editorial. (2021). Disponible en: https://bv.unir.net:2769/es/ereader/unir/222659?page=364

BERROCAL LANZAROT, A. *Derecho de supresión de datos o derecho al olvido* [en línea]. (ed.). Editorial Reus. (2017). [consulta: 20 de noviembre de 2023]. Disponible en: https://bv.unir.net:2769/es/lc/unir/titulos/46691

BOTERO. M. <<El ataque cibernético que sacude a Colombia>> *Revista pesquisa Javeriana* [consulta: 18 de octubre de 2023]. Disponible en: https://www.javeriana.edu.co/pesquisa/ciberataque-ifx-networks-colombia/

BLANCO NAVARRO J. <<Ciberseguridad Post Pandemia>>, pp. 136- 145. En HUESCA GONZÁLEZ, A y GRIMALDO SANTAMARIA O. (coord.) Aspectos Sociales en la Seguridad Ciudadana, ProQuest E-book Central. [en línea] Dykinson, S.L., 2021. [consulta: 27 de septiembre de 2023]. Disponible en: https://bv.unir.net:2056/lib/univunirsp/detail.action?docID=6661374

CIRCIA, <<Cyber Incident Reporting for Critical Infrastructure Act of 2022>>. 2022. [consulta: 06 de noviembre de 2023]. Disponible en: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

DEPARTAMENTO NACIONAL DE PLANEACIÓN Consejo Nacional de Política Económica Y Social República de Colombia <<COMPES 3995, política nacional de confianza y seguridad digital>> 2020[consulta: 06 de noviembre de 2023]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

FERNÁNDEZ GONZÁLEZ, F. y otros. <<Revisión sistemática de la Jurisprudencia española sobre ciberseguridad y privacidad>>*. RDU Revistas especializadas*. 2021, núm. 24, pp 153. [consulta: 25 de septiembre de 2023]. ISSN digital 2444-5762. Disponible en: https://e-archivo.uc3m.es/bitstream/handle/10016/34078/revision_RPDD_2021.pdf?sequence=1

FORBES, <<Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know>>.2022. [consulta: 05 de noviembre de 2023]. Disponible en: https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=1560a1647864

IBERDROLA. <<Metaverso, el lugar donde la realidad física y la virtual se dan la mano>>. 2022 [consulta: 4 de noviembre de 2023]. Disponible en: https://www.iberdrola.com/innovacion/metaverso#:~:text=El%20concepto%20de%20metaverso%20apareci%C3%B3,y%20convergente%20con%20la%20realidad

KOLODNER, J. y MUKHI, R. <<Cybersecurity: Continued Cyberattacks and New Regulations Result in Increased Risk>> 2023. [consulta: 06 de noviembre de 2023]. Disponible en: https://www.clearygottlieb.com/news-and-insights/publication-listing/cybersecurity-continued-cyberattacks-and-new-regulations-result-in-increased-risk#_ftn1

KPMG. <<Una triple amenaza en las américas>>.2022 [consulta: 26 de septiembre de 2023]. Disponible en: https://assets.kpmg.com/content/dam/kpmg/co/pdf/2022/01/Triple%20amenaza%20en%20las%20Am%C3%A9ricas%20-%202022%20KPMG%20Fraud%20Outlook%20-%20ESP.pdf

MARIANO, R. y NÚÑEZ, G. << Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe>>, *Naciones Unidas*, 2023. [consulta: 25 de septiembre de 2023]. Disponible en: https://repositorio.cepal.org/server/api/core/bitstreams/2db8feef-29d6-4981-9741-9ad3154d3789/content

MUÑOZ NIETO, M. <<El inicio del procedimiento de la ejecución hipotecaria: demanda ejecutiva, competencia y despacho de ejecución>>. Revista del Centro de Estudios Jurídicos y de Postgrado, S.L. (CEJUP). N.º 7 de Elche. p.p.215 [consulta: 22 de noviembre de 2023]. Disponible en: https://cejup.es/wp-content/uploads/2022/10/No-3-2022-REVISTA-CEJUP-OCTUBRE-2022.-1.pdf

Organización of American States <<Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas>> 2015, pp 2-55[consulta: 7 de octubre de 2023]. Disponible en:https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Portection%20de%20la%20Inf%20Critica.pdf

ORTIZ.C. <<El rol del CISO y la protección de los activos digitales>>. *El Financiero.* 16 de octubre de 2023. Disponible en: https://www.proquest.com/docview/2878210792?parentSessionId=6lPBzCzNtmiNW%2FmfoD5k26L7gjIDphN96jQyxcayrSI%3D&pq-origsite=summon&accountid=142712

ORZA LINARES, Ramón. <<Derechos fundamentales e internet: nuevos problemas, nuevos retos>>. ReDCE. 2012. núm. 18 pp 275-226. [consulta: 5 de octubre de 2023]. Disponible en: https://www.ugr.es/~redce/REDCE18pdf/10_orza_linares.pdf

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO- SIC << Guía para la implementación del principio de responsabilidad demostrada (*Accountability*)>>. [consulta: 28 de noviembre de 2023]. Disponible en: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

Web

<<Actualización de 2023 de la tabla de contraseñas de Hive Systems>> 18 de abril de 2023.Disponible en: https://www.hivesystems.io/

<<Safe Online Surfing Internet Challenge>> 20 de septiembre de 2023. Disponible en: https://www.fbi.gov/news/espanol

<<20 recomendaciones para proteger su actividad en Internet>> 26 de marzo de 2020. Disponible en: https://www.mintic.gov.co/portal/715/w3-article-126363.html

<<Visualizing The 50 Biggest Data Breaches From 2004–2021 >> 01 de junio de 2022. Disponible en: https://www.visualcapitalist.com/cp/visualizing-the-50-biggest-data-breaches-from-2004-2021/

<<Ángeles Formación, capacitación y talento en ciberseguridad >> Disponible en: https://angeles.ccn-cert.cni.es/es/oferta-formativa#especializacion

https://www.observaciber.es/

Informes

GUTIERREZ J. *et al. Informe sobre la cibercriminalidad en España*. Dirección General de Coordinación y Estudios Secretaría de Estado de Seguridad. 2021

MUNIESA TOMÁS, P. *Informe sobre la cibercriminalidad en España*. Dirección General de Coordinación y Estudios Secretaría de Estado de Seguridad. 2022

Instrumentos citados

Declaración de Fortalecimiento de la Seguridad Cibernética de las Américas. Organización de los Estados Americanos, 9 de marzo de 2015. Disponible en:

https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Declaracion%20del%20Fortalecimiento%20de%20la%20Seguridad%20en%20las%20Americas.pdf

Declaración sobre la Protección de Infraestructura Crítica ante las Amenazas Emergentes. Organización de los Estados Americanos, 23 de marzo de 2015. Disponible en: https://www.oas.org/en/sms/cicte/documents/sessions/2015/CICTE%20DOC%201%20DECLARACION%20CICTE00955S04.pdf

Guía para la notificación de brechas de datos personales. Disponible en: https://www.aepd.es/documento/guia-brechas-seguridad.pdf

Presidencia de Gobierno. Estrategia Nacional de Bioseguridad. 2019. Disponible en: file:///C:/Users/proyecto.usta/Downloads/Estrategia%20Nacional%20de%20Ciberseguridad%202019%20(1).pdf

Legislación citada

Colombia. Decreto 1377 de 2013. *Diario Oficial 48834*, junio 27 de 2013.

Colombia. Ley 1266 de 2008. *Diario Oficial 47.219*, diciembre 31 de 2008.

Colombia. Ley 1581 de 2012. *Diario Oficial 48587*, octubre 18 de 2012.

España. Constitución española, de 29 de diciembre de 1978. *Boletín Oficial del Estado*, núm. 311.

España. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín Oficial del Estado,* 24 de noviembre de 1995. núm. 281.

España. Real Decreto 146/2021, de 9 de marzo, por el que se modifican el Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales, y el Real Decreto 734/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior. *Boletín Oficial del Estado,*12 de marzo de 2021, núm. 61. Disponible en: https://www.hacienda.gob.es/BoletinesHacienda/Boletines/2021/71412.pdf

España. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. *Boletín Oficial del Estado,* 4 de mayo de 2016.

Listado de abreviaturas

AEPD	Agencia Española de Protección de Datos
AV	Antivirus
CERT	Equipo de respuesta a emergencias informáticas
CNI	Centro Nacional de Inteligencia
CNPIC	Centro Nacional de Protección de Infraestructuras Críticas
EC	Entidades de Certificación
EPS	Entidad promotora de salud
ESN	Estrategia de Seguridad Nacional
IA	Inteligencia artificial
INCIBE	Instituto Nacional de Ciberseguridad es ciberseguridad
IPS	Instituto prestador de salud
MinTIC	Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia
MSP	Proveedor de servicios gestionado
OAT	Órganos de Auditoría Técnica
OPD	Oficial de Protección de Datos Personales-
RGPD	Reglamento General de Protección de Datos
SIC	Superintendencia de Industria y Comercio
STIC	Seguridad de las Tecnologías de Información y Comunicaciones
VPN	Red Privada Virtual)
TIC	Tecnologías de la información y la comunicación