SEGURIDAD INFORMÁTICA: RELACIÓN E IMPACTO FRENTE A LA LEY DE PROTECCIÓN DE DATOS PERSONALES (LEY 1581 DE 2012)

MARCELA PATRICIA RUIZ GARZÓN
DIANA PAOLA AGUIRRE OLMOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2020

SEGURIDAD INFORMÁTICA: RELACIÓN E IMPACTO FRENTE A LA LEY DE PROTECCIÓN DE DATOS PERSONALES (LEY 1581 DE 2012)

MARCELA PATRICIA RUIZ GARZÓN
DIANA PAOLA AGUIRRE OLMOS

Monografía presentada como requisito para optar al título de:
Especialista en Seguridad Informática

Yina Alexandra González Sanabria
Director de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2020

Nota de Aceptación

_____

_____

Firma del presidente del jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C, 26 de Abril de 2020

DEDICATORIA

A mis padres quienes desde mi infancia forjaron mi personalidad y futuro con gran amor; por ser ellos mi apoyo constante en el logro de mis metas y proyectos. A mi hijo quien a su corta edad representa mi motor, fortaleza y motivación para nunca rendirme y culminar con éxito la meta propuesta.

Diana Paola Aguirre Olmos

DEDICATORIA

A mi hijas y esposo, por la comprensión y el tiempo que me permitieron dedicar a este proyecto. A mis hermanos y sobrino que me apoyaron y me animaron a llegar a la meta de lograrlo. A los profesores, tutor y director que con cada enseñanza nos aportan de manera directa o indirecta a materializar el objetivo.

Marcela Patricia Ruiz

AGRADECIMIENTOS

Queremos agradecer siempre y ante todo a DIOS dueño y señor de nuestras vidas y quien nos bendice en todo y tiene el control de todas las cosas, sobre todo en la actualidad.

A nuestros hijos por su paciencia y espera, en todo momento.

A nuestras familias en general por su apoyo, impulso y empuje a continuar hasta lograrlo.

A nuestro Director de proyecto quien puntualmente nos hizo las observaciones necesarias y nos colaboró de manera especial con el proyecto. Ingeniero Esp. Freddy Enrique Acosta.

A la Universidad Nacional Abierta y a Distancia UNAD, a los profesores y tutores por la orientación, enseñanza y conocimiento impartido de manera profesional y ética.

CONTENIDO

Pág.

LISTA DE TABLAS

pág.

LISTA DE IMÁGENES

pág.

GLOSARIO

AMENAZA: En temas de seguridad una amenaza es la posibilidad de ocurrencia de algún evento o acción que pueda generar algún tipo de daño físico o lógico a un sistema de información o información física, en caso de ser sobre un sistema de información.

ATAQUE CIBERNÉTICO: Son actividades malintencionadas en la red de internet con motivaciones económicas, financieras o sociales que se direccionan a cualquier tipo de organización privada o pública.

BASE DE DATOS: Conjunto de datos personales, organizados de manera tal que se les da un tratamiento a los mismos.

CARDING: Delito a través del cual se realiza uso ilegítimo de una tarjeta de crédito de otra persona con el propósito de realizar fraude.

CONTROL: Acciones, dispositivos, procedimientos, técnicas u otras medidas que ayudan a reducir la vulnerabilidad presente en un sistema de información.

DATO PERSONAL: Es toda aquella información inherente a la persona identificada o identificable y que le da identidad, la describe y precisa. Por ejemplo, número de identificación, edad, estado civil, lugar de residencia, experiencia laboral o académica, entre otros.

DATO PERSONAL PRIVADO: Aquel dato personal que dada su naturaleza intima o reservada únicamente es relevante para el titular.

DATO PERSONAL PÚBLICO: Es aquel dato que no es ni semiprivado, privada o sensible. Dada su naturaleza pueden estar contenidos en registros públicos, por ejemplo, estado civil, profesión u oficio.

DATO PERSONAL SEMIPRIVADO: Es aquella información o dato personal que no tiene naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar a cierto sector o grupo de personas además del propio titular.

DATO SENSIBLE: Es aquella información o dato personal que afecta la intimidad de la persona o cuyo uso inadecuado puede generar discriminación.

ENCARGADO DEL TRATAMIENTO: Persona natural o jurídica, privada o pública, quien a monto propio o en asocio con otros, realiza el tratamiento de datos personales por cuenta del responsable del tratamiento.

FARMING: Es una estafa de larga duración, en la cual los cibercriminales buscan establecer una relación con el objetivo. Normalmente, observan los perfiles de redes sociales del objetivo e intentan construir una relación con él basada en la información que recopilan durante la investigación. Este tipo de ataque también depende del pretexto, ya que el atacante intenta engañar a la víctima por tanto tiempo como puede para obtener todos los datos que sean posibles[1].

HÁBEAS DATA: Es el recurso legal que tiene toda persona de acceder, modificar o rectificar su información personal y de protegerse contra el uso indebido de su propia información por organismos privados y públicos.

INCIDENTE DE SEGURIDAD: Se refiere a la violación de las políticas definidas en una organización y que afecta la operación normal de los recursos informáticos, sistemas operativos o bases de datos.

MALWARE: Programa o código informático malicioso que se produce con el propósito de ingresar a un sistema informático de forma no autorizada para realizar actividades maliciosas como robo de información sensible, control del sistema, entre otras.

PHISHING: Éste es comúnmente un delito de robo de información mediante correo electrónico suplantado, aparentemente un correo de la entidad financiera. Aquí se solicitan datos personales como claves, usuarios, datos puntuales de la cuenta o número de la tarjeta y productos del usuario.

PRETEXTO: Técnica de ingeniería social a través de la cual el ciberdelincuente crea una historia para atrapar a la víctima[2].

PRINCIPIO DE CONFIDENCIALIDAD: Obliga al responsable del tratamiento a guardar secreto profesional sobre los datos recolectados y preservar su confidencialidad.

PRINCIPIO DE SEGURIDAD: Hace referencia al manejo de la información o los datos personales sujetos al tratamiento, adoptando mecanismos técnicos, organizativos o humanos para proteger los registros contra su adulteración, pérdida, consulta o uso no autorizado.

PROFILING: Es un concepto utilizado por las empresas de comercio electrónico y marketing, el cual consiste en elaborar un perfil de la persona, es decir caracterizar la persona en función de sus característica y gustos, de manera que les permita analizar sus preferencias e intereses basados en la información recolectada y el tratamiento automatizado de sus datos personales. Como lo afirma Rocío de

---

[1] Norton. "¿Qué es la ingeniería social?" (En línea) (15 de diciembre 2018) disponible en: https://mx.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html.

[2] Ibid., p. 12.

Rossello en un blog de Abogacía Española,[3] nuestros datos personales actualmente son una "fuente de negocio" especialmente para los gigantes de Internet como Google, Facebook, Amazon para quienes nuestros datos son una fuente de ingreso a través del mercadeo que realizan con esta información.

QUID PRO QUO: Técnica de ingeniería social a través de la cual se pretenden engañar al usuario con ganar algún premio o descuento una vez diligencia un formulario que solicita una gran cantidad de información personal y cuyos datos son utilizados posteriormente para realizar fraude[4].

RESPONSABLE DEL TRATAMIENTO: Persona natural o jurídica, privada o pública, quien a monto propio o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

SEGURIDAD INFORMÁTICA: Cuando hablamos de este concepto, se hace referencia a los procesos, metodologías y soluciones tecnológicas de hardware y software diseñadas y que se espera sean implementadas para proteger la confidencialidad, integridad y/o disponibilidad de la información y en especial de los datos personales que tiene el sector financiero. Es aquí donde se implementan las diferentes medidas de seguridad contra las múltiples amenazas, lo que conlleva a minimizar los riesgos asociados al uso indebido, a una errada divulgación o destrucción de la información, modificación o acceso no permitido.

SKIMMING: Este es un tipo de robo de información para posteriormente realizar fraude, se copian y roban datos de la banda magnética de la tarjeta débito o crédito mediante un dispositivo y micro cámaras que captan la clave de usuario. Estos dispositivos comúnmente son colocados en bares, cajeros automáticos, restaurantes etc.

SMISHING: Este es otro tipo de delito informático que a través de mensajes de texto invita a los usuarios de cuentas bancarias y tarjetas de crédito a ingresar a una página web fraudulenta.

SPEAR PHISHING: Técnica de ingeniería social que consiste en la elaboración de una campaña dirigida a los colaboradores de una compañía en particular. El ciberdelincuente recopila información de su objetivo a través de consultas en internet, redes sociales y posteriormente enviar un correo electrónico con un enlace malicioso[5].

---

[3] ENATIC. "Nuestros datos personales, fuente de negocio y actividades de profiling" (En línea) (17 de octubre de 2019) disponible en: https://www.abogacia.es/2016/09/21/nuestros-datos-personales-fuente-de-negocio-y-actividades-de-profiling/.

[4] ENATIC. "Nuestros datos personales, fuente de negocio y actividades de profiling" (En línea) (17 de octubre de 2019) disponible en: https://www.abogacia.es/2016/09/21/nuestros-datos-personales-fuente-de-negocio-y-actividades-de-profiling/.

[5] Ibid., p. 11.

TITULAR: Es la persona física cuyos datos son objeto de tratamiento.

TRATAMIENTO DE DATOS PERSONALES: Corresponde a toda aquella operación o procedimiento técnico automatizado o no, que permita la recolección, almacenamiento, elaboración, modificación, uso de datos, así como la cesión de datos producto de comunicaciones, consultas, interconexiones y transferencias.

VISHING: Este es un término en inglés que significa voice y phishing, lo cual significa robo de información a través de una llamada telefónica a la que llevan al usuario, de manera engañosa, el usuario se comunica a un centro de atención telefónica similar al de la entidad financiera y termina suministrando datos de sus productos; como número de la tarjeta de crédito, fecha de expiración y nombre de usuario y/o claves, lo cual es suficiente para realizar fraudes.

VULNERABILIDAD: Aquí se entiende como la debilidad que puede presentar la información y la condición o característica que presenta un sistema o entidad y que puede estar susceptible a sufrir un daño (ataque), por causa de una amenaza.

.

RESUMEN

Esta monografía presenta la normatividad vigente frente a la Protección de Datos Personales.[6] Adicionalmente pretende demostrar la relación, el impacto y la contribución desde el ámbito de la seguridad de la información y seguridad informática para la protección de los datos personales en cualquier de los estados de la información, es decir, en reposo, en tránsito y en uso/procesamiento; para el caso y de acuerdo a lo establecido en la legislación hace referencia a la protección de los datos personales durante su recolección, almacenamiento y procesamiento. Se tiene la intención de demostrar dicha relación e impacto específicamente en las Compañías colombianas del sector financiero; lo anterior evidenciado a través de las múltiples vulnerabilidades, amenazas, medidas organizativas, operativas y técnicas.

Para tal efecto, se revisará la normatividad vigente a nivel local e internacional, así como los casos o incidentes de seguridad asociados o que involucran datos personales reportados por entes de control o autoridades en materia de seguridad de la información, así como informes o reportes emitidos por Compañías reconocidas a nivel local y mundial, foros especializados y relacionadas con seguridad de la información y/o seguridad informática.

[6] CONGRESO DE LA REPÚBLICA. Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá D.C., 2012. No 48587. 197 p.

SUMMARY

This monograph presents the current regulations regarding the Protection of Personal Data. Additionally, it aims to demonstrate the relationship, impact and contribution from the field of information security and computer security for the protection of personal data in any of the information states, that is, at rest, in transit and in use / processing; For that matter, and in accordance with the provisions of the legislation, it refers to the protection of personal data during its collection, storage and processing. It is intended to demonstrate this relationship and impact specifically in Colombian companies in the financial sector; the foregoing evidenced through the multiple vulnerabilities, threats, organizational, operational and technical measures.

For this purpose, the regulations in force at the local and international levels will be reviewed, as well as the security cases or incidents associated with or involving personal data reported by control entities or authorities in the area of information security, as well as reports or reports issued by Locally and globally recognized companies, specialized forums related to information security and / or computer security.

INTRODUCCIÓN

Las tecnologías de la información y las comunicaciones inducen cambios que inciden en la sociedad, particularmente con la globalización en relación con la información, generando un exponencial avance en todos los aspectos de la ciencia. Ejemplo de ello es la aparición del Internet y su uso globalizado a nivel personal y en el entorno empresarial el cual nos permite “estar conectados”, sin embargo, al mismo tiempo estos avances tecnológicos también se transforman en una amenaza toda vez que trae consigo la aparición de nuevas vulnerabilidades y riesgos de seguridad dado la fácil accesibilidad y exposición de información vital o sensible para la Compañías (por ejemplo, los datos personales) gracias a esa conectividad. Es aquí, donde cobra importancia la protección de los datos, especialmente los datos personales, para atender esta problemática.

En Colombia lo relacionado con los datos personales es un tema que, aunque se encuentra reglamentado y legislado a través de la Ley 1581 de 2012[7] y sus decretos reglamentarios, está aún no se aplica de la manera más eficiente y estricta. A diario nos encontramos en situaciones en las que nuestros propios datos personales están en manos de personas que no sabemos quiénes son y de dónde sacaron el detalle de nuestros datos personales.

Bajo este precedente, con la elaboración de esta monografía, se pretende explicar la interrelación y el impacto de la seguridad informática en la protección de datos personales, evidenciar las múltiples amenazas y vulnerabilidades presentes en los entornos informáticos que podrían llegar a violar el derecho a la intimidad personal y familiar así como el buen nombre de la persona; finalmente demostrar el aporte o contribución desde la perspectiva de seguridad de la información y seguridad informática en la protección de estos datos a través de un conjunto de medidas organizativas y técnicas para controlar todos los datos que se manejan dentro de una Compañía aprovechando el uso de las nuevas tecnologías desarrolladas en la actualidad.

[7] CONGRESO DE LA REPÚBLICA. Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá D.C., 2012. No 48587. 197 p.

1. DEFINICIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

Cualquier avance o mejora en la tecnología que implique el uso de está por la sociedad desencadena en la necesidad de una actuación o participación desde el ámbito jurídico para evitar y controlar la vulneración de los derechos de las personas. Las leyes y su jurisprudencia se originan como resultado de una exigencia social permitiendo la remediación de conflictos en el dominio individual o colectivo. Una de estas intervenciones jurídicas corresponde a la firma y entrada en vigor de la Ley 1581 de 2012 a través de la cual se pretende el uso y tratamiento correcto de los datos personales, obligando a las compañías colombianas que manejan datos personales a establecer e implementar políticas, procedimientos y controles con este propósito.

La Superintendencia de Industria y Comercio (En adelante SIC) fue delegada como ente de control y vigilancia de la Ley de Protección de Datos Personales, a través de la misma Ley en su artículo 19. La SIC en años recientes ha tenido conocimiento de incidentes de seguridad, ejemplo de ello fueron los ataques sucedidos entre el 2018 y 2019 en países latinoamericanos como Ecuador, México y Chile. Durante el 2018 México fue víctima de ataques de tipo Ransomware en un 3.5%, Chile obtuvo un porcentaje de 1.8%, mientras que en el 2019 Ecuador sufrió una filtración masiva de datos de ciudadanos ecuatorianos (18GB de datos) de acuerdo al reporte dado por la Compañía VPNMentor y cuya filtración involucro datos sensibles tales como: nombres, teléfonos, registro familiares, entre otros[8]; para el caso chileno la Comisión para el Mercado Financiero de Chile informó sobre un incidente relacionado con la fuga de datos de algo más de 41.000 tarjetas de crédito y débito[9]. Los casos de México y Chile "que fueron destacados en las noticias, dejaron en claro que los servicios financieros de América Latina son un blanco de los delincuentes cibernéticos extranjeros y respaldados por estados"[10].

De acuerdo con el estudio realizado por la Organización de Estados Americanos y presentado en el Simposio de Ciberseguridad realizado en el año 2018, se encuentra que:

"El 92% de las entidades bancarias manifiestan que identificaron algún tipo de evento (ataques exitosos y ataques no exitosos) de seguridad digital en contra de la entidad financiera.

[8] BBC News. Londres. Septiembre, 2019.
[9] LA FM. Bogotá D.C. Junio, 2019.
[10] CONTRERAS, Belisario, *et al*. Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe. En: Simposio de Ciberseguridad de la OEA (18: 24-28, Septiembre: Washington DC). Reporte. Washington D.C.: Gobierno de Canadá, 2018. p. 7-8.

Los riesgos de seguridad digital que merecen la mayor atención por parte de las entidades bancarias son: i) el robo de base de datos crítica, ii) el compromiso de credenciales de usuarios privilegiados, y, iii) la pérdida de datos"[11].

La sociedad y la tecnología han evolucionado a un ritmo vertiginoso en los últimos años. Nos encontramos en la era de las telecomunicaciones, en la que el manejo y el intercambio de datos personales se han tornado en una práctica cotidiana en la que interviene el estado, como sector público, y el sector privado, representado por las empresas. En ambos casos, los datos personales son utilizados para actividades relacionadas, sobre todo con la venta de bienes y servicios.

Este tipo de prácticas comporta nuevos riesgos para los ciudadanos, por cuanto las leyes nacionales han establecido normas y procedimientos con la finalidad de buscar un debido tratamiento de la información que se encuentra en las bases de datos. Existe la necesidad de perfeccionar dichas disposiciones y de que las mismas respondan a las necesidades particulares que surgen en una sociedad cada vez más globalizada.

El uso a nivel mundial de las tecnologías de información y comunicaciones ha permitido que en muchas ocasiones los datos personales y sensibles sean utilizados de forma irresponsable para fines distintos para los que fueron recolectados, además que estos datos a veces son intercambiados con otras entidades diferentes a las que el titular de los datos entregó; por tanto, esto va en contra de la privacidad de la persona y puede atentar contra otros derechos y libertades. Todo este uso indiscriminado de los datos personales va en detrimento de nuestra privacidad e intimidad personal y familiar.

Lo anterior arroja como resultado la falta de regulación y control en el uso de los datos personales; por consiguiente, la única manera de evitar que la información y los datos de los usuarios no circule libremente y sin ningún control, surge el concepto de "protección de datos personales"[12].

Debido al poco desarrollo y avance en la aplicabilidad de la Ley 1581 de Habeas Data y Protección de Datos personales, es importante encontrar una practicidad y aplicabilidad de la norma al interior del sector financiero en Colombia. Por lo anterior se espera realizar un análisis de la manera como se aplica actualmente la ley, las normas y decretos al respecto y darle un enfoque primordial a la seguridad Informática.

Adicional y debido a las sanciones vigentes relacionadas con violaciones del

[11] OERTING, Troesls y DOYLE, Sean. Foro Económico Mundial: El panorama de la amenazas a la ciberseguridad en los Bancos de América Latina y el Caribe. Citado por CONTRERAS, Belisario, *et al*. Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe. En: Simposio de Ciberseguridad de la OEA (18: 24-28, Septiembre: Washington DC). Reporte. Washington D.C.: Gobierno de Canadá, 2018. p. 7-8.

[12] COLOMBIA. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. "Protección de Datos Personales" {En línea}. {diciembre 2016} Disponible en: https://www.sic.gov.co/proteccion-de-datos-personales.

habeas data y protección de datos personales, es importante identificar de qué manera la seguridad informática, puede mejorar la aplicabilidad de la norma en cualquier organización, reportes a centrales de riesgo que no corresponden con la realidad, no actualización oportuna de información o por no avisar al deudor antes de hacer el reporte a las centrales de riesgo; esto se acerca al 80% del total de sanciones impuestas.

Como indica la Ley Federal de Protección de Datos Personales..."Es pertinente tener en cuenta las recomendaciones internacionales de derechos humanos con respecto a privacidad, protección de datos personales, vida privada, esto tomando como base casos de éxito como España y México"[13].

1.2. FORMULACIÓN DEL PROBLEMA

Colombia hasta el momento no tiene un nivel de calificación adecuada para la protección de Datos Personales, por eso es importante tener referentes adecuados de otros países como España y México que han tenido avances más significativos y ya cuentan con un nivel garante de confidencialidad, integridad y disponibilidad en la protección y seguridad de Datos personales, este referente lo define la Comisión Europea.

Por lo anterior podemos decir que se tienen muchos interrogantes por aclarar y discutir, tales como: ¿Cuál es el nivel apropiado de Protección de Datos Personales?, ¿Cómo contribuye seguridad informática a la protección de datos personales?

Estos interrogantes y vacíos que surgen serán el punto de partida para realizar el análisis y al determinar el resultado, nos permitirán interpretar de mejor manera, la metodología a aplicar, para dar cumplimiento a la ley desde la perspectiva de seguridad de la información y seguridad informática. [14]

[13] MEXICO. CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN. "Ley Federal de Protección de Datos Personales en Posesión de los Particulares" (En línea). (5, julio, 2010) disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

[14] COLOMBIA. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. "Por violaciones de datos personales, Superindustria ha impuesto sanciones por más de $21 mil millones de pesos" (En línea) (8, junio, 2017) Colombia. Disponible en: https://www.sic.gov.co/noticias/por-violaciones-de-datos-personales-superindustria-ha-impuesto-sanciones-por-mas-de-21-mil-millones-de-pesos

2. JUSTIFICACIÓN

Los expertos, académicos y estudiosos ya hablan de la cuarta revolución industrial, y de la transformación digital o también conocida como la "era digital"; tal como lo afirma Klaus Schwab en su libro La Cuarta Revolución Industrial: "Estamos al borde de una revolución tecnológica que modificará fundamentalmente la forma en que vivimos, trabajamos y nos relacionamos. En su escala, alcance y complejidad, la transformación será distinta a cualquier cosa que el género humano haya experimentado antes"[15] estas tecnologías se soportan primordialmente en dos ejes: la conectividad e interoperabilidad de dispositivos, contenidos y redes y la digitalización del conocimiento o la información.

Todo este desarrollo tecnológico es parte de nuestro diario vivir y ha modificado nuestra manera de vivir, de trabajar y de interactuar o relacionarse con los demás. Por eso se considera que actualmente somos la Sociedad de la Información, gracias a la "era digital". La promesa de la era digital es la capacidad espontánea y sin fronteras para compartir información.

Esta vertiginosa evolución que transforman y facilitan nuestra cotidianidad, también trae consigo desafíos y amenazas potenciales para nuestra seguridad y privacidad. Por lo tanto, a medida que la información del mundo migra hacia el ciberespacio, las capacidades de regulación y vigilancia deben establecerse proporcionalmente y a la misma velocidad.

Todo lo anteriormente mencionado permite resaltar que proteger los datos de las personas es primordial, toda vez que el riesgo es alto ante las constantes amenazas aunadas a la ausencia de conciencia en seguridad de la información por parte de las personas tanto en su ámbito laboral como personal. Por esto, es de resaltar, la relevancia que tiene para la Compañías contar con herramientas adecuadas para la protección de los datos personales de sus clientes, proveedores, empleados o terceros, durante todo su ciclo de vida (creación o recepción, procesamiento, almacenamiento y eliminación).

La nueva legislación europea deja de manifiesto el derecho que tiene toda persona por su privacidad e intimidad, especialmente en la era digital. El nuevo reglamento europeo, aplicable desde el 25 de mayo del 2018, incluye los nuevos derechos de los ciudadanos europeos acordes con la problemática actual, por ejemplo, el derecho al olvido, el derecho a oponerse a la elaboración de perfiles, el derecho a la portabilidad de datos, entre otros. Además de nuevos derechos el GRPD trae cambios significativos como mayor transparencia informativa, exigen nuevas

[15] ESPAÑA. WORLD ECONOMIC FORUM. "La cuarta revolución industrial-Klaus Schwab" (En línea)(diciembre 2016) Disponible en: http://40.70.207.114/documentosV2/La%20cuarta%20revolucion%20industrial-Klaus%20Schwab%20(1).pdf

garantías, evaluación de riesgos para determinar las medidas de seguridad necesarias en la protección de los datos.

En Colombia se han dado avances con respecto a la definición de la norma o Ley Estatutaria 1266 del 2008 y es importante resaltar que al referimos a ella se debe tener en cuenta la Protección de Datos sensibles y la Protección de Datos personales de niños, jóvenes y adolescentes; principios básicos de la norma y objeto principal de la misma, esto como consecuencia que en la Ley 1266 solo se protegen los datos personales del sector financiero y de las personas involucradas con el sector financiero; aquí no se tuvo todo el grupo objetivo a ser protegido dentro del marco legal"[16].

Como lo menciona Lucero Galvis en el artículo de la Revista LEBRET, en nuestro país "Un avance importante a nivel jurídico se observa con la Ley Estatutaria 1266 de 2008, la cual regula en forma más detallada el derecho fundamental de habeas data que se aplica, en su orden, a bases de datos de carácter financiero, comercial y proveniente de terceros países. Posteriormente, la Ley Estatutaria 1581 de 2012 ha significado un adelanto importante en torno a la protección de cualquier dato personal que sea administrado por entidades públicas y privadas, de acuerdo con los principios generales establecidos en la Constitución. Esta última ley establece dos categorías de datos que requieren de protección especial y cuyo tratamiento está, en términos generales, prohibido: los llamados datos sensibles que son los que afectan la intimidad de las personas o cuyo uso indebido puede generar discriminación (etnicidad, ideología, orientación política, datos de salud y/o orientación sexual, entre otros) y los datos personales de los niños, niñas y adolescentes. La norma designó la autoridad competente en términos de protección de datos y prohibió la transferencia de datos a países que no tengan un nivel adecuado de protección de estos"[17].

[16] Cano, Lucero Galvis. "Protección de datos en Colombia, avances y retos". Revista Lebret 4, n.º 4 (1 de enero de 2012): 195-214. (En línea). (13 marzo de 2008) disponible en: https://doi.org/10.15332/rl.v4i4.336 p.199.
[17] Ibid., p. 19.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Establecer la relación, impacto y contribución de la seguridad informática frente al cumplimiento de la Ley de Protección de Datos Personales, en las Compañías del sector financiero en Colombia.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar la normatividad relacionada con Protección de Datos Personales a nivel nacional e internacional.

- Recolectar información sobre ataques informáticos que involucren datos personales, basado en informes o reportes generados por Compañías reconocidas a nivel local, regional y/o mundial; de manera que permita determinar la tipología de amenazas que afectan la seguridad de los datos personales.

- Definir mejoras e identificar la pertinencia de la seguridad informática en las compañías colombianas del sector financiero para la protección de datos personales, como resultado del análisis a partir de la información recopilada respecto a la normatividad vigente y los ataques informáticos.

4. MARCO DE REFERENCIA

4.1 ANTECEDENTES

En el desarrollo del presente documento se toman como referencias los siguientes proyectos o trabajos de grado:

- Trabajo de grado “Big data: la puesta en crisis de la protección de datos personales” realizado por Juan Fernando Bernal Jiménez y Felipe Valencia Serrano mediante el cual pretende demostrar la oposición que existe entre el principio y las herramientas jurídicas para la protección de los datos personales y los mecanismos implementados por las Compañías que soportan sus estrategias de negocio en el Big Data que les permiten esquivar la legislación en esta materia

- Trabajo de grado “Protección de datos personales en los servicios de internet” de Carmen Carolina Soto y Camilo Andrés Ducuara (2018) a través del cual analizan las brechas y la robustez de la legislación colombiana en materia de protección de datos personales frente a la web.

- Trabajo de grado “herramientas jurídicas para la protección de los datos personales en Colombia: análisis del grado de protección jurídica del habeas data” Realizado por Camilo José Puello Rincón (2016) cuyo objetivo principal es realizar un análisis del nivel de protección del Habeas Data a través de los mecanismos jurídicos existentes en Colombia y tomando como marcos de referencia los estándares en la materia definidos por la Unión Europea y Estados Unidos.

- Tesis “Protección de datos personales en las redes sociales digitales” de Edgar Guijosa Delgado (2013) a través del cual genera una reflexión sobre la protección de los datos y la privacidad especialmente en las redes sociales tales como Facebook, Twitter, LinkedIn y otras.

Así como otros trabajos de grado y artículos relacionados con la materia referenciados a lo largo del documento.

4.2 MARCO TEÓRICO

4.2.1 Antecedente legal y normativo de la protección de datos personales. El término “privacidad” usualmente se relaciona con la protección de datos personales; la protección de datos tiene su primer relato en el año en 1890 por cuenta del artículo de dos abogados en la revista *Harvard Law Review* (vol. IV, núm. 5, 15 de diciembre de 1890, págs. 194-220) donde recapitulaban el principio fundamental del individuo sobre la protección de su vida privada: “La prensa está traspasando, en todos los ámbitos, los límites de la propiedad y de la decencia. El

chismorreo ha dejado de ser ocupación de gente ociosa y depravada para convertirse en una mercancía, buscada con ahínco e incluso, con descaro…Con el fin de entretener al indolente, columna tras columna se llenan de chismes insustanciales, obtenidos únicamente, mediante la intromisión en el ámbito privado"[18]. Este escenario propició el surgimiento de la legislación y normatividad asociada a la protección de datos personales.

La normatividad relacionada con la protección de datos personales tiene sus inicios en la Declaración Universal de los Derechos Humanos de 1948 promulgada por la Asamblea General de las Naciones Unidas y en la cual a través del Artículo 12 establece que "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques"[19], posteriormente este mandato fue reafirmado a través del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, en su Resolución 2200 A (XXI) que data del año 1966. Luego en el año 1969 fue incluido en el artículo 11 de la Convención Americana sobre Derechos Humanos.

En Europa surgió el concepto de protección de datos personales, en Estados Unidos un concepto similar denominado *privacidad*, sin embargo, sus alcances son diferentes. En México el debate alrededor de este tema inició en el 2001 y solo hasta el 2010 fue aprobada la "Ley Federal de Protección de Datos Personales en posesión de los particulares"[20].

4.2.2 En Colombia. En el País este mandato se estableció a través de la Constitución Política en su artículo 15 referido a que "toda persona tiene derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas"[21].

Posteriormente este derecho a la *intimidad* es reglamentado a través de la Ley 1266 de 2008 Habeas Data "por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros

[18] Warren, Samuel, Brandeis Louis, *El derecho a la intimidad*, Editorial Civitas S.A., Madrid 1995, p. 25.
[19] PARIS. ASAMBLEA GENERAL DE LAS NACIONES UNIDAS. "Resolución 217 A (III) Declaración Universal de Derechos del Hombre (en línea). (10 de diciembre de 1948)) París, Naciones Unidas. 1948. Disponible en: https://www.un.org/es/universal-declaration-human-rights/index.html
[20] MEXICO. DIARIO OFICIAL DE LA FEDERACIÓN. "Ley Federal de Protección de Datos Personales en Posesión de los Particulares" (En línea). (5 julio de 2010) disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf
[21] CONGRESO DE LA REPÚBLICA. Constitución Política de Colombia. Bogotá. (4, julio, 1991). Gaceta Constitucional número 114. 1991.

países y se dictan otras disposiciones"[22] y la Ley 1581 de 2012 "por la cual se dictan disposiciones generales para la protección de datos personales"[23]**.**

Estas leyes fueron posteriormente reglamentadas a través de los Decretos 1377 de 2013, Decreto 886 de 2014 y Decreto 1759 de 2016.

Sin embargo, la legislación actual existe la necesidad de incorporar nuevos preceptos toda vez que no aborda temas como el derecho al olvido y la designación o nombramiento de un Oficial de protección de datos que hacen parte de los nuevos requisitos del Reglamento General de Protección de Datos (GDPR).

4.2.3 En la Unión Europea. A través del Convenio Europeo de Derechos Humanos de 1950 Europa reconoció el derecho a la *privacidad*; este tratado define que "que todo el mundo tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. Se prohíbe la injerencia de la autoridad en el ejercicio de este derecho salvo cuando dicha injerencia esté prevista por la ley y sea necesaria en una sociedad democrática para la protección de intereses generales importantes y legítimos"[24].

Durante los años 70 en Europa se expidieron las primeras leyes sobre la protección de los datos personales. Dentro estás Alemania adoptó la primera ley del mundo en Ley de Land Hesse en 1970 y solo aplicaba al estado de Hesse. En Suecia se adoptó la Datalagen en 1973; Ley Federal sobre protección de datos (República Federal Alemana, 27 de enero de 1977), Alemania la Bundesdatenschutzgestez que correspondía a la Ley Federal sobre protección de datos que entró en Vigor en el año de 1977; y Francia la Ley "Informática, Ficheros y Libertades del 6 de enero de 1978"[25]. En el Reino Unido, la Data Protection Act se adoptó en 1984. Por último, los Países Bajos adoptaron los Wet Persoonregistraties en 1989. Como se evidencia estas leyes fueron expedidas entre los años de 1970 a 1980 en un contexto tecnológico esencialmente diferente al actual; en efecto, comenta LAZPITA que "*las primeras leyes sobre esta materia, conocidas como primera generación de protección de datos, tenían en común la convicción de que había llegados el momento de reaccionar ante la informatización progresiva de la sociedad y también, la incertidumbre acerca de sus implicaciones inmediatas, así como de las medidas precisas que debían tomarse. Eran rígidos instrumentos de*

[22] CONGRESO DE LA REPÚBLICA. Ley 1266 (31, diciembre, 2008). Por la cual se dictan las disposiciones generales sobre el hábeas data. Diario Oficial. Bogotá D.C., 2008. No 47219. 11 p.
[23] CONGRESO DE LA REPÚBLICA. Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá D.C., 2012. No 48587. 197 p.
[24] Tribunal Europeo de Derechos Humanos. "Convenio Europeo de Derechos Humanos (CEDH)" (En línea) (4, noviembre de 1950) disponible en: https://www.echr.coe.int/Documents/Convention_SPA.pdf
[25] PEREZ-LUÑO. Enrique César. El procedimiento de Habeas Data. El derecho procesal ante las nuevas tecnologías. Madrid: DYKISON, S.L. 336 p. ISBN 978-84-91-48-231-4.

una época caracterizada por una tecnología hoy casi obsoleta: unos bancos de datos muy caros, escasos, voluminosos y, por lo tanto, fácilmente localizables"[26].

En 1981 el Consejo de Europa el Convenio 108, con el fin de proteger a las personas respecto al tratamiento automatizado de sus datos de carácter personal. Sin embargo, esta regulación necesitaba una actualización de manera urgente, que la adaptase a las realidades de la nueva era digital con la aparición de tecnologías como el Big Data y Machine Learning, por tal razón se firmó una nueva versión de este Convenio en octubre de 2018 y el cual fue acogido por los estados miembro del Consejo Europeo e incluyó otro países como Uruguay[27].

Desde 1995 hasta mayo de 2018, el principal instrumento jurídico de la Unión Europea fue la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Directiva sobre protección de datos)[28]. Se adoptó en 1995, en un momento en el que varios Estados miembros habían adoptado ya leyes nacionales de protección de datos y surgió en respuesta a la necesidad de armonizar dichas leyes para garantizar un elevado nivel de protección y la libre circulación de datos personales entre los diferentes Estados miembros. Esta Directiva reflejo los principios en materia de la protección de datos personales que ya contenían las leyes nacionales y el Convenio 108, aunque en muchos casos los ampliaba. Esta Directiva fue derogada posteriormente por el Reglamento 2016/679 o más conocido como el Reglamento General de Protección de Datos (GDPR) y el cual entró en vigencia en mayo de 2018.

4.2.4 En América Latina. Países como México, Colombia, Argentina, Paraguay, Perú y Brasil cuenta con legislación cuentan con legislación para la protección de datos personales y las cuales han tenido como marco la legislación europea.

Argentina fue uno de los primeros países en desarrollar este tipo de legislación y la misma estaba sin actualizar desde el año 2000, sin embargo a partir de la entrada en vigencia de la GDPR de la Unión Europea en el año 2018 se propuso una proyecto de ley que reemplazar su legislación y de manera que ésta fuera alineada con la GDPR y la cual fue enviada al Congreso de ese país para someter a aprobación a través del Mensaje 147/2018.

---

[26] LAZPITA GURTUBAY, María. 1994. Análisis comparado de las legislaciones sobre protección de datos de los Estados miembros de la Comunidad Europea. Informática y Derecho 6-7 (La protección de datos personales en la L.O.R.T.A.D y derecho comparado): Mérida, España. p 403-404

[27] La Vanguardia. Madrid "España y 20 países firman protocolo para el Convenio de Protección de Datos". (en línea)(10 de Octubre 2018). Disponible en: https://www.lavanguardia.com/politica/20181010/452291023498/espana-y-20-paises-firman-protocolo-para-el-convenio-de-proteccion-de-datos.html

[28] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO 1995 L 281.

En México aparece por primera vez a través de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental del año 2002 y la cual concluye con la actual Ley Federal de Protección de Datos Personales en Posesión de los Particulares del año 2010[29].

De acuerdo con lo mencionado por Jacomé Mayorga Tania en su artículo en la revista Dominio de las Ciencias países como Ecuador, Venezuela y Bolivia actualmente se encuentran sin regulación para la protección de los datos personales.

Para el caso de Brasil se carecía de legislación en la materia hasta el año 2018 cuando fue aprobada la Ley General de Protección de Datos (Ley 13709 de 2018) y entró en vigencia a partir de febrero del 2020.

Con la entrada en vigencia del Reglamento General de Protección de Datos (GDPR) de la Unión Europea en mayo de 2018 se han generado reformas a la legislación existente en esta materia en países como Brasil, Chile, Argentina y México.

4.3 MARCO CONCEPTUAL

A continuación, se describen algunos conceptos básicos y que son relevantes en el tema central de esta investigación.

4.3.1 Amenaza. Acción u hecho que pone en riesgo la seguridad de la información. Existen diferentes tipos de amenazas de acuerdo a su naturaleza; por lo tanto existen amenazas generados por las personas, por el medio ambiente o factores naturales.

4.3.2 Ataque informático. Acciones que pretenden dañar o perjudicar un sistema informático a través de la exposición, alteración, destrucción, robo u obtención de acceso no autorizado o uso no autorizado de un activo de información de la organización.

4.3.3 Confidencialidad. Propiedad o atributo de la información a través de la cual se permite el acceso a la información únicamente a las personas autorizadas.

[29] CONGRESO GENERAL DE LOS ESTADOS UNIDOS MEXICANOS. Ley 156 (5, julio, 2010). Por el cual Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Diario Oficial de la Federación. México D.F, 2012. 18 p.

4.3.4 Dato personal. Cuando hablamos de un dato personal, es parte de la identidad de una persona; únicos como nombre, apellido, dirección o más allá puede ser la huella dactilar, documento de identidad entre otros.

4.3.5 Delito informático. Es una actividad realizada por expertos en tecnología en la que hacen mal uso de los sistemas informáticos y pueden realizar diferentes tipos de faltas que son clasificados como delitos, los cuales pueden afectar tanto a personas como a organizaciones.

4.3.6 Disponibilidad. Cuando se habla de disponibilidad se espera que la información o los datos se encuentren a disposición en el momento que se requiera.

4.3.7 Integridad. Aquí se refiere a que el dato o la información se mantenga desde su origen hasta el destino igual, sin alteraciones y que sea igual desde cualquier fuente donde se consulte.

4.3.8 Ransomware. Este es un tipo de malware o software malicioso, que si se ejecuta puede bloquear el computador y prohíbe acceder al mismo hasta que se pague un rescate por la información capturada en el ordenador.

4.3.9 Seguridad de la información. Conjunto de medidas o controles técnicas y organizativas implementadas por una organización para proteger la información, en formato físico y/o digital, contra la pérdida de confidencialidad, integridad y disponibilidad.

4.3.10 Seguridad informática. Conjunto de técnicas y mecanismos implementados por una organización para proteger la información contra la pérdida de confidencialidad, integridad y disponibilidad, enfocado o centrado en los sistemas informáticos.

4.3.11 Ingeniería Social. Acción de manipular a las personas por medio de la manipulación psicológica y/o habilidades sociales para obtener información con el propósito de ejecutar posteriormente algún tipo de ataque.

4.3.12 Incidente de seguridad. Es un evento confirmado que impide la operación normal de la organización y que indica que se ha violado la política de seguridad de la información, adicional indica que ni se han tomado las suficientes medidas preventivas para la protección de los sistemas.

4.3.13 Phishing. Mecanismo o técnico de ingeniería social por medio de la cual se pretende engañar a la víctima a través de la suplantación de un sitio de confianza con el propósito de robar información confidencial de manera fraudulenta, por ejemplo: contraseña, número de tarjeta de crédito.

4.3.14 Riesgo de seguridad. Un riesgo es la probabilidad latente de que ocurra un incidente de seguridad, por lo tanto se deben tomar las respectivas prevenciones para que no se convierta en incidente.

4.3.15 Robo de Identidad. Es el hecho de apropiarse de la identidad de una persona haciéndose pasar por ella, generalmente para obtener un beneficio económico. También, es utilizado con el fin de perjudicar a una persona, por ejemplo, difamando o manchando su nombre creando perfiles falsos en redes sociales.

4.3.16 Malware. Este es un tipo de software que causa daños a la información, son los llamados virus, troyanos, gusanos o spyware, se encuentran ocultos en los correos o en la información que recibimos por diferentes medios informáticos.

4.3.17 Vulnerabilidad. Es normalmente un error que se presenta en nuestros sistemas de información y que se debe identificar y corregir, para que no sea una amenaza o en casos extremos se presente un incidente de seguridad.

4.4 MARCO LEGAL

4.4.1 Constitución política de Colombia. Carta magna o ley suprema donde se definen los derechos y deberes de los colombianos.

4.4.2 Ley Estatutaria 1266 de 2008. "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones"[30].

4.4.3 Decreto reglamentario 1727 de 2009. "Por la cual se determina la forma en la cual lo operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la provenientes de terceros países, deben presentar la información de los titulares de la información"[31]

4.4.4 Decreto Reglamentario 2952 de 2010. "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008"[32]

---

[30] CONGRESO DE LA REPÚBLICA. Ley 1266 (31, diciembre, 2008). Por la cual se dictan las disposiciones generales sobre el hábeas data. Diario Oficial. Bogotá D.C., 2008. No 47219. 11 p.

[31] CONGRESO DE LA REPÚBLICA. Decreto 1727 (16, agosto, 2012) Por la cual se determina la forma en la cual lo operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la provenientes de terceros países, deben presentar la información de los titulares de la información. Diario Oficial. Bogotá D.C., 2012. No 48524. 1 p.

[32] CONGRESO DE LA REPÚBLICA. Decreto 2952 (6, agosto, 2010) Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008. Diario Oficial. Bogotá D.C., 2010. No 47793. 16 p.

4.4.5 Ley 1273 de Delitos informáticos de 2009. "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"[33].

4.4.6 Ley 1581 de 2012. Tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada"[34].

4.4.6 Decreto 1377 de 2013. "Por el cual se reglamenta parcialmente la Ley 1581 de 2012"[35].

4.4.7 Decreto 886 de 2014. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos"[36].

4.4.8 Decreto 1074 de 2015. "Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo" [37].

4.4.9 Decreto 1081 de 2015. "Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República"[38].

---

[33] CONGRESO DE LA REPÚBLICA. Ley 1273 (5, enero, 2009) Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008. Diario Oficial. Bogotá D.C., 2009. No 47223.

[34] CONGRESO DE LA REPÚBLICA. Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá D.C., 2012. No 48587. 197 p.

[35] CONGRESO DE LA REPÚBLICA. Decreto 1377 (27, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Diario Oficial. Bogotá D.C., 2013. No 48834. 28 p.

[36] CONGRESO DE LA REPÚBLICA. Decreto 886 (13, mayo, 2014). Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos. Diario Oficial. Bogotá D.C., 2013. No 49150. 89 p.

[37] CONGRESO DE LA REPÚBLICA. Decreto 1074 (26, mayo, 2015). Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Diario Oficial. Bogotá D.C., 2015. No 49523. 711 p.

[38] CONGRESO DE LA REPÚBLICA. Decreto 1081 (26, mayo, 2015). Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República. Diario Oficial. Bogotá D.C., 2015. No 49523. 1458 p.

4.4.10 Decreto 1759 de 2016. “Por el cual se modifica el artículo 2.2.2.26.3.1 del Decreto 1074 de 2015 - Decreto Único Reglamentario del Sector Comercio, Industria y Turismo”[39].

4.4.11 Decreto 1115 de 2017. “Por el cual se modifica el artículo 2.2.2.26.3.1 del Decreto número 1074 de 2015 - Decreto Único Reglamentario del Sector Comercio, Industria y Turismo”[40].

4.4.12 Circular Básica Jurídica (C.E. 029/14) Parte I Título II Capítulo I. “Canales, medios, seguridad y calidad en el manejo de información en la prestación de servicios financieros”[41].

4.4.13 Circular Básica Jurídica (C.E. 029/14) Parte I Título I Capítulo VI. “Reglas relativas al uso de servicios de computación en la nube”[42].

[39] CONGRESO DE LA REPÚBLICA. Decreto 1759 (8, noviembre, 2016).Por el cual se modifica el artículo 2.2.2.26.3.1 del Decreto 1074 de 2015- Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Diario Oficial. Bogotá D.C., 2016 No. 5051. 2 p.

[40] CONGRESO DE LA REPÚBLICA. Decreto 1115, (29, junio, 2017). Por el cual se modifica el artículo 2.2.2.26.3.1 del Decreto número 1074 de 2015 - Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Bogotá D.C., 2017. No 50279. 38 p.

[41] SUPERINTENDENCIA FINANCIERA DE COLOMBIA. "Circular Básica Jurídica (C.E. 029/14) Parte I Título II Capítulo I" (En línea). (16 diciembre 2019) disponible en: https://www.superfinanciera.gov.co/publicacion/10102519

[42] SUPERINTENDENCIA FINANCIERA DE COLOMBIA. "Reglas relativas al uso de servicios de computación en la nube" (En línea). (16 diciembre 2019) disponible en: https://www.superfinanciera.gov.co/publicacion/10083444

5. NORMATIVIDAD PROTECCIÓN DE DATOS PERSONALES

A continuación, se recopila la información relacionada con la normatividad y legislación relacionada con el tema materia de esta investigación no experimental. En ese sentido, se aplica una tabla para la recopilación de la información.

5.1 A NIVEL INTERNACIONAL

5.1.1 Unión Europea

Tabla 1. Legislación en la Unión Europea

Organización o entidad emisora	Norma	Descripción	Año de expedición
Organización para la Cooperación y el Desarrollo Económico (OCDE)	Directriz	Protección de la intimidad y de la circulación transfronteriza de datos personales.	1980
Consejo de Europa	Convenio 108	Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal	1981
Organización de la Naciones Unidas	Directrices	Regula los archivos de datos personales informatizados	1990
Parlamento Europeo y del Consejo de la Unión Europea	Directiva 2002/ 58/CE	Regula el tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)	2002
Parlamento Europeo y del Consejo de la Unión Europea	Directiva 2006/24/CE	Reforma la Directiva 2002/58/CE, reglamenta la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones	2006
Parlamento Europeo y del Consejo de la Unión Europea	Directiva 2009/136/CE de 25 de noviembre de 2009	Reforma por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE	2009

Organización o entidad emisora	Norma	Descripción	Año de expedición
		relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) no 2006/2004 sobre la cooperación en materia de protección de los consumidores.	
Parlamento Europeo y del Consejo de la Unión Europea	Reglamento 2016/679	Establece el nuevo marco regulatorio en materia de la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Más conocido como el Reglamento General de Protección de Datos (RGPD) y es la norma marco de referencia para aplicable a los países miembro de la Unión Europea Este reglamento permite mejorar el control que tiene el ciudadano sobre su información privada y el uso de ésta en el mundo digital de hoy (redes sociales, banca electrónica, teléfonos inteligentes, IoT, entre otros).	2016
Parlamento Europeo y del Consejo de la Unión Europea	Directiva 2016/1148	Establece los lineamientos destinados a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.	2016

Fuente: Elaboración propia basada en los datos obtenidos en la página web del Parlamento Europeo.

5.1.2 España

Tabla 2. Legislación en España

Organización o entidad emisora	Norma	Descripción	Año de expedición
Cortes Generales	Constitución Artículo 18.4	La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos	1978
Cortes Generales	Ley Orgánica 5/1992	Conocida como LORTAD, regula el tratamiento automatizado de los datos de carácter personal	1992
Cortes Generales	Ley Orgánica 15/1999	Conocida como LOPD, esta ley se establecer para la protección de datos de carácter personal. Derogó la LORTAD	1999
Cortes Generales	Ley Orgánica 3/ 2018	LOPDGDD: Protección de datos personales y garantía de los derechos digitales	2018

Fuente: Elaboración propia basada en los datos obtenidos en la página web de la Agencia Española de Protección de Datos.

5.1.3 Argentina

Tabla 3. Legislación en Argentina

Organización o entidad emisora	Norma	Descripción	Año de expedición
Convención Nacional Constituyente	Constitución Política Art. 43	Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística	1994

Organización o entidad emisora	Norma	Descripción	Año de expedición
Congreso	Ley 25.326	Ley de Protección de los Datos Personales, habeas data, derechos y garantías constitucionales, banco de datos personales, derecho a la intimidad, información sensible, rectificación del error, supresión de datos, obtención de datos, información errónea o desactualizada, Derecho constitucional, Derecho informático, Derecho civil	2000
Poder Ejecutivo Nacional	Decreto 995	Régimen Legal de Habeas Data	2000
Poder Ejecutivo Nacional	Decreto 1558	Reglamentación de la Ley 25.326	2001
Congreso	Ley 26. 343	Ley de Protección de los Datos Personales, banco de datos personales, ley modificatoria, Derecho constitucional, Derecho informático y a través de la cual se incorporó el artículo 47 a la Ley 25.326.	2007
Congreso	Ley 26.951	Registro Nacional “No Llame”, ésta fue reglamentada por el Decreto 2501/14 y cuyo propósito es proteger al titular del abuso de los procesos de contacto, publicidad, oferta, venta y regalo de bienes y servicios no solicitados de telefonía.	2014
Agencia de Acceso a la Información Pública	Resolución 40	Política Modelo de Protección de Datos Personales para Organismos Públicos.	2018
Agencia de Acceso a la Información Pública	Resolución 47	Medidas de seguridad recomendadas para el tratamiento y conservación de los datos personales en medios no informatizado	2018

Fuente: Elaboración propia basada en los datos obtenidos en la página web del Congreso de la Nación Argentina

5.1.4 Estados Unidos

Tabla 4. Legislación en Estados Unidos

Organización o entidad emisora	Norma	Descripción	Año de expedición
Congreso de Estados Unidos	HIPPA	Ley de Transferencia y responsabilidad del Seguro Sanitario - HIPPA, por sus siglas en inglés. Esta Ley fue decretada en el año 1996 y a través de la cual se pretende proteger la información relacionada con la salud de la persona. Específicamente, HIPAA especifica quién puede tener acceso a dicha información	1996
Congreso de Estados Unidos	COPPA	Ley de Protección de la Privacidad de Menores de los Estados Unidos como un mecanismo para la protección de la privacidad de los menores de 13 años y específicamente enfocada a aquellos sitios web dirigidos a niños	1998
Gobernador de California	CCPA Ley de Privacidad del Consumidor	Ley de privacidad en línea de California y través de la cual se exige a las compañías proteger la información personal de los consumidores.	2018

Fuente: Elaboración propia basada en los datos obtenidos en la página web del Congreso de Estados Unidos y la Ofician del Abogado General del Departamento de Justicia del Estado de California.

5.1.5 México

Tabla 5. Legislación en México

Organización o entidad emisora	Norma	Descripción	Año de expedición
Congreso de la Unión	Ley Internacional de Transparencia y Acceso a la Información Pública Gubernamental y Privada	Protección de datos personales para el ámbito público	2002

Organización o entidad emisora	Norma	Descripción	Año de expedición
Congreso de la Unión	Ley Federal de Protección de Datos Personales en Posesión de los Particulares.	Tiene como propósito la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.	2010
Congreso de la Unión	Ley General de protección de Datos Personales en Posesión de Sujetos Obligados	Establece las bases, principios y procedimientos para garantizar el derecho que tiene toda persona al tratamiento lícito de sus datos personales, a la protección de estos, así como al ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición de sus datos personales en posesión de sujetos obligados.	2017

Fuente: Elaboración propia basada en los datos obtenidos en la página web de Diario Oficial de la Federación.

5.2 A NIVEL NACIONAL

5.2.1 Colombia

Para el desarrollo de este análisis de información, es necesario enfatizar en las leyes y decretos que rigen la protección de datos personales, los aspectos para tener en cuenta al momento de hacer uso de la información personal de cualquier cliente, proveedor, empleado u otro en Colombia y sobre todo en materia de protección de datos personales, junto con una breve descripción para cada una:

Tabla 6. Legislación en Colombia

Organización o entidad emisora	Norma	Descripción	Año de expedición
Asamblea Nacional Constituyente	Constitución Política de Colombia Art. 15	Norma reina en cuanto al derecho a la intimidad y la protección de datos. Este artículo señala que: “Todas las personas tienen derecho a la intimidad personal y familiar y a su buen nombre, y el Estado, debe respetarlos y hacerlos respetar. De igual modo, tienen derecho	1991

Organización o entidad emisora	Norma	Descripción	Año de expedición
		a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas"[43].	
Congreso de la Republica	Ley 1266 del 2008	Ley de Habeas Data. Regula el manejo de la información recolectada en bases de datos, especialmente la financiera, crediticia, de servicios y la proveniente de terceros países"[44]. Sin embargo, como se menciona esta ley estaba enfocada exclusivamente a la protección de los datos de carácter financiero y comercial.	2008
Presidencia de la República	Decreto 1727 de 2009	Reglamenta la Ley 1266 de 2008, por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información[45].	2009
Presidencia de la República	Decreto 2952 de 2010	Reglamenta los artículos 12 y 13 de la Ley 1266 de 2008 "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones"[46].	2010
Congreso de la Republica	Ley 1581 de 2012	Esta es una de las principales leyes que debemos tener en cuenta al momento	2012

[43] ASAMBLEA NACIONAL CONSTITUYENTE. Constitución Política de Colombia (20 de julio de 1991). Gaceta Constitucional. Bogotá D.C., 1991. No. 116. 8 p.

[44] CONGRESO DE LA REPÚBLICA. Ley 1266 (31, diciembre, 2008). Por la cual se dictan las disposiciones generales sobre el hábeas data. Diario Oficial. Bogotá D.C., 2008. No 47219. 11 p.

[45] PRESIDENCIA DE LA REPÚBLICA. Decreto 1727 (16, agosto, 2009) Por la cual se determina la forma en la cual lo operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la provenientes de terceros países, deben presentar la información de los titulares de la información. Diario Oficial. Bogotá D.C., 2012. No 47350. 1 p.

[46] PRESIDENCIA DE LA REPÚBLICA. Decreto 2952 (6, Agosto, 2010). Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008. Diario Oficial, Bogotá D.C., 2010. No. 47.793. 3 p.

Organización o entidad emisora	Norma	Descripción	Año de expedición
		de revisar y analizar la protección de datos, pues el objeto de esta ley dice lo siguiente: "La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada"[47] La Ley se establecen ocho (8) principios que rigen la protección de los datos y los cuales deben ser aplicados a las bases de datos personales objeto de tratamiento, esto incluye la colección, uso, almacenamiento, transmisión y eliminación. Dentro de estos principios se pueden relacionar y alinear cinco (5) de ellos con los atributos de la información: confidencialidad, integridad y disponibilidad; estos atributos o propiedades de la información son el eje central dentro de la gestión de seguridad de la información e informática. Estos principios son: ● **Principio de veracidad o calidad:** La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales,	

[47] CONGRESO DE LA REPÚBLICA. Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá D.C., 2012. No 48587. 197 p.

Organización o entidad emisora	Norma	Descripción	Año de expedición
		incompletos, fraccionados o que induzcan a error; ● **Principio de transparencia:** En el Tratamiento debe garantizarse el derecho del Titular a obtener del responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan; ● **Principio de acceso y circulación restringida:** El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley; Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley; ● **Principio de seguridad:** La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; ● **Principio de confidencialidad:** Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la	

Organización o entidad emisora	Norma	Descripción	Año de expedición
		naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de esta.	
Ministerio de Comercio, Industria y Turismo Ministerio de Tecnología de la Información y Comunicaciones	Decreto 1377 del 2012	Reglamenta parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales."[48] Este Decreto facilita la implementación y cumplimiento de la Ley 1581 de 2012 a través de la reglamentación aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales, este último tema referido a la rendición de cuentas.	2012
Superintendencia de Industria y Comercio	Circular 001	Modifica el Capítulo Segundo del Título V de la Circular Única de la Superintendencia de Industria y Comercio Diario Oficial 50051 del 8 de noviembre de 2016.	2016
Superintendencia de Industria y Comercio	Circular 02	Este documento define las disposiciones generales de la Ley 1581 de 2012, para la protección de Datos Personales. Realiza las definiciones, los formatos y la manera como se debe solicitar de manera formal, la Autorización del uso de datos personales.	2015

[48] CONGRESO DE LA REPÚBLICA. Decreto 1377 (27, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Diarios Oficia. Bogotá D.C., 2013. NO. 48834. 10 p.

Organización o entidad emisora	Norma	Descripción	Año de expedición
Superintendencia de Industria y Comercio	Circular Externa No. 005	A través de la cual "fija los estándares de un nivel adecuado para la protección de datos personales en los países receptores de dicha información, así como las condiciones para realizar la transferencia internacional de datos personales, concluye que los países miembros de la Unión Europea y los países que han sido declarados con nivel adecuado de protección por la Comisión Europea. De otra parte, este listado también incluye a México, República de Corea, Costa Rica, Serbia, Perú, Noruega, e Islandia"[49].	2017
Superintendencia de Industria y Comercio	Circular 08	Modifica el numeral 3.2 del Capítulo Tercero del Título V de la Circular Única. Publicada en el Diario Oficial No. 50448 del 15 de diciembre de 2017.	2017
Superintendencia de Industria y Comercio	Decreto 90 de 2018	Por el cual se modifican los artículos 2.2.2.26.1.2 y 2.2.2.26.3.1 del Decreto 1074 de 2015 -Decreto Único Reglamentario del Sector Comercio, Industria y Turismo Diario.	2018
Congreso de la República	Ley 1273	Aquí se define la protección de la información y de los datos y se resguardan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones[50]. Con respecto a lo que indica la ley, se hace una descripción de los ***delitos*** que la ley puntualmente determina y que son realizados a través de la red y que ***afectan directamente los datos personales o sensibles***.	2009

[49] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Circular Externa 005. (En línea), Agosto de 2017. Disponible en: http://www.sic.gov.co/sites/default/files/normatividad/082017/Circular_Externa_005_de_2017.pdf.

[50] CONGRESO DE LA REPÚBLICA. Ley 1273 (5, enero, 2009) Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá D.C., 2009. No 47223.

Organización o entidad emisora	Norma	Descripción	Año de expedición
		● **Artículo 269A: Acceso abusivo a un sistema informático**: "El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes". ● **Artículo 269B:** Obstaculización ilegítima de sistema informático o red de telecomunicación. "El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor". ● **Artículo 269C:** Interceptación de datos informáticos. "El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses." ● **Artículo 269D:** Daño Informático. "El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses	

Organización o entidad emisora	Norma	Descripción	Año de expedición
		y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes." ● **Artículo 269E:** Uso de software malicioso. "El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes." ● **Artículo 269F:** Violación de datos personales. "El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes." ● **Artículo 269G:** Suplantación de sitios web para capturar datos personales. "El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave."	
Superintendencia Financiera de Colombia	Circular Básica Jurídica CE 029/14	Parte I Título I Capítulo VI A través de la cual se definen los lineamientos para el uso de servicio en la nube y orientado, dentro de los requerimientos se involucra la protección de los datos	2014

Organización o entidad emisora	Norma	Descripción	Año de expedición
		personales y teniendo en cuenta que los servicios en nube puede implicar el almacenamiento de datos fuera de Colombia, la Superfinanciera exige que la entidad vigilada verifique que la jurisdicción donde se procesa la información cuente con reglamentación equivalentes o superiores a las definidas en Colombia. Parte I Título II Capítulo I Establece los criterios de seguridad de la información que deben adoptar las entidades vigiladas	

Fuente: Elaboración propia basada en los datos obtenidos en la página web de Diario Oficial, Superintendencia de Industria y Comercio y la Superintendencia Financiera de Colombia.

Modelo de seguridad y privacidad de la información. En el marco de la Estrategia de Gobierno en Línea para el componente de Seguridad y Privacidad de la Información, se establece el Modelo a través del cual pretende preservar la confidencialidad, integridad, disponibilidad y privacidad de la información. El documento recolecta o recopila las mejores prácticas de seguridad de la información a nivel nacional o internacional, permitiendo realizar desde un análisis de la brecha existente [51].

[51] MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES. "Modelo_de_Seguridad_Privacidad" (En línea). (16 marzo de 2020) disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

6. ATAQUES INFORMÁTICOS Y TIPOLOGÍA DE AMENAZAS QUE AFECTAN LOS DATOS PERSONALES EN EL SECTOR FINANCIERO

La protección de los datos personales es resultado de diferentes hechos y documentos a lo largo de la historia de la humanidad, los cuales se han ido actualizando fruto de la incidencia de las tecnologías de la información en el ámbito personal y corporativo, pero también generando brechas por el uso inapropiado de éstas[52].

El auge de las Tecnologías de la Información y las Telecomunicaciones (En adelante TIC) de la mano de su uso en ocasiones desmesurado, permite que los datos personales sean utilizados para fines diferentes para los que originalmente fueron obtenidos, y que sean compartidos con entidades diferentes a las que el propietario o titular de los datos confió la información. Esto evidentemente va en contravía del principio de privacidad de la persona[53]. El acceso a las TIC ha cambiado sustancialmente las cosas; la manera de comunicarse, realizar las transacciones, el comercio electrónico, etc. Esto ya es una realidad y no en vano se habla de la transformación digital y las compañías del sector financiero no quieren quedarse atrás. Como lo menciona Eliana Rodríguez en su artículo: "*América Latina está adoptando la transformación digital tanto en el sector público como en el privado como una forma de mantenerse competitiva en el mercado económico global. Sin embargo, si la ciberseguridad no es una prioridad de las organizaciones, esta transformación es imposible*"[54]. Actualmente lo negativo del asunto es que no se aborda con la misma fuerza la seguridad y así lo reitera Dimitry Bestuzhev, Director del Equipo de Investigación y Análisis para América Latina en Kaspersky Lab, quien señala que "*la seguridad de un banco no es una estrategia estática, sino que necesita evolucionar y adaptarse constantemente, basándose en la inteligencia obtenida sobre las tendencias, las nuevas amenazas y las técnicas de seguridad más recientes para mantener verdaderamente segura la red*"[55].

Con el nacimiento del internet, en los 90´s, nacen los primeros ataques informáticos, luego los ataques empiezan a dirigirse a las herramientas encargadas de proteger la información, en el año 2000. A su vez inicia el fraude en línea; sin embargo, hasta el año 2010 las entidades bancarias inician la implementación de

[52] CONGRESO DE LA REPÚBLICA. Ley 1273 (5, enero, 2009) Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008. Diario Oficial. Bogotá D.C., 2009. No 47223.
[53] Ibid., p. 47.
[54] RODRIGUEZ, Eliana. Ciberseguridad, un componente fundamental de la transformación digital (en línea). 2018 (citado 15-04-2020). Disponible en internet: https://blog.cobiscorp.com/ciberseguridad-transformacion-digital.
[55] Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe (en línea). Washington D.C: Organización de los Estados Americanos (OEA), 2018 (citado 2020-04-15). Disponible en internet: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

planes de sensibilización en seguridad y se busca mayor control sobre la privacidad.

De acuerdo con un estudio realizado en el año 2018 por la Secretaría General de la Organización de Estados Americanos (OEA) que tuvo como objetivo proporcionar información sobre sobre el Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe, los clientes de la banca se vieron afectados principalmente por eventos o incidentes más frecuentes como i) **phishing**, ii) **ingeniería social**, y, iii) **software espía** (malware o troyanos)[56], adicionalmente en este estudio se indica que durante el 2017, el 92% de las entidades bancarias manifiestan haber identificado algún tipo de evento (ataques exitosos y ataques no exitosos) de seguridad digital, presentándose con mayor cantidad los eventos que se relacionan en la tabla 7.[57]

Tabla 7. Eventos identificados contra las entidades bancarias

Tipo de evento	**%**
Código malicioso	80%
Violación de política de escritorio limpio	61%
Spear Phishing	57%

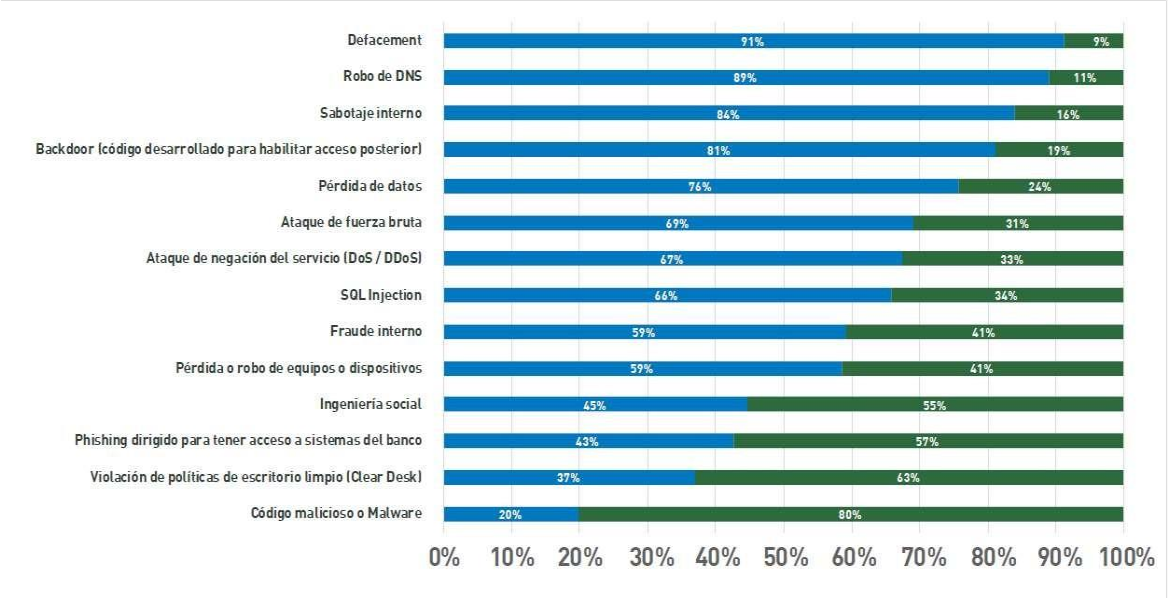
Fuente: Elaboración propia basado en el sitio de OEA Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe {En línea} {25 de septiembre 2019} disponible en internet: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

Adicionalmente se destaca la identificación diaria de malware y phishing dirigido para tener acceso a sistemas del banco (un 24% y 22% de las entidades bancarias los identificaron, respectivamente). En figura 7, se evidencia el resultado de los eventos de seguridad digital contra las entidades bancarias identificados durante el 2017.

[56] Ibid., p 47.

[57] Ibid., p 47.

Figura 1. Eventos identificados durante el 2017



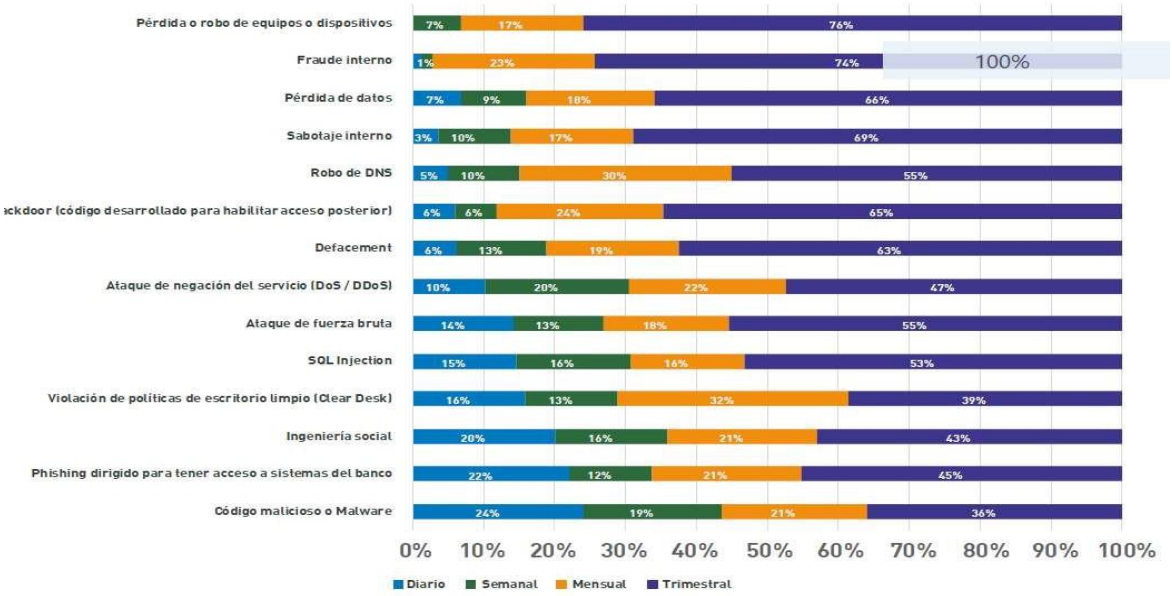
Fuente: Elaboración propia basado en el sitio de OEA Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe {En línea} {25 de septiembre 2019} disponible en internet: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

Según el Informe Global de Riesgos del Foro Económico Mundial 2018, los ciberataques a gran escala y las filtraciones o robos masivos de datos están considerados dentro de los cinco (5) principales riesgos más probables en la próxima década a nivel global. “Los riesgos de ciberseguridad también están creciendo, tanto en su prevalencia como en su potencial disruptivo. Los ataques contra empresas casi se han duplicado en cinco años, y los incidentes que una vez se consideraron extraordinarios se están volviendo cada vez más comunes”[58].

El estudio de la OEA incluyo resultados de la frecuencia con que estos eventos son identificados por las entidades bancarias objeto del estudio, cuyo resultado se evidencia en la figura 2.

[58] The Global Risks Report 2018 (en línea). World Economic Forum, 2018 (citado 2020-04-15). 13th Edition. Disponible en internet: www3.weforum.org/docs/WEF_GRR18_Report.pdf.

Figura 2. Frecuencia en la ocurrencia de eventos de seguridad



Fuente: Elaboración propia basado en el sitio de OEA Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe {En línea} {25 de septiembre 2019} disponible en internet: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

En 2017 la banca tuvo que enfrentar ciberataques a gran escala y amenazas como el Ransomware: *WannaCry* y *Petya;* este mismo año se identificaron 677 millones de ataques cibernéticos entre enero y agosto en América Latina según el fabricante Kaspersky, un aumento de 59% con respecto a los años anteriores, con afecciones principalmente en Brasil, México y Colombia. Hablando puntualmente de Colombia, el cibercrimen aumentó 28,3% en 2017 con respecto a 2016, según el balance del cibercrimen en Colombia del Centro de Cibernético Policial.

El experto en delitos informáticos de Digiware, Andrés Galindo, afirma que hoy en día el impacto financiero y económico del Cibercrimen, es aún mayor que el que genera el narcotráfico; actualmente los *hackers* ya no trabajan de forma independiente ahora trabajan mancomunadamente con grandes bandas o grupos de crimen cibernético organizado con experiencia en sistemas bancarios centrales, metodologías organizadas, técnicas avanzadas, con capacidad de mantener actividad dentro de la red de un banco por varios meses y conformadas en su mayoría por hombres; De acuerdo con la afirmación de este experto, estas bandas están conformadas mayormente por hombres, en la tabla 8 se relaciona la

proporción de los cibercriminales hombres distribuidos por edad, que conforman dichas bandas.

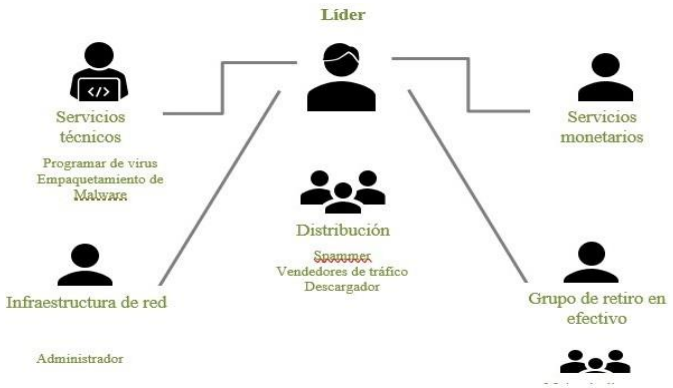
Tabla 8. Edades de los hombres que conforman las bandas cibercriminales

Hombres (representan el 76% de los miembros que conforman una banda cibercriminal)	
14 años en adelante	8%
50 años promedio	11%
35 años promedio	43%

Fuente: Artículo Revista Dinero: “El cibercrimen es un delito más rentable que el narcotráfico. (En línea) (4 de abril de 2020) disponible en https://www.dinero.com/internacional/articulo/principales-cifras-del-cibercrimen-mundo-colombia/213988

De acuerdo a estudios realizados por la empresa Digiware, se afirma que el 76% de los miembros que conforman las bandas de cibercrimen son hombres, donde el 8% son de 14 años en adelante, el 11% tiene un promedio de 50 años y el 43% son de 35 años en promedio. Por lo anterior el 38% restante se ubica en edades menores a 14 años o mayores a 50 años y un 24% corresponde a mujeres de cualquier edad. Estas bandas de delincuentes cibernéticos pueden llegar a conformarse por más de 15 personas de la siguiente manera:

Figura 3. Estructura bandas delincuenciales



Fuente: Elaboración propia basado en el sitio de OEA Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe {En línea} {25 de septiembre 2019} disponible en internet: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

La anterior figura muestra cómo se organizan las bandas delincuenciales a nivel de América Latina, pues se define un Líder General y una estructura de servicios técnicos, monetarios, un esquema de distribución, un esquema para retiro de efectivo, una infraestructura de red y dentro de esta distribución existen especialistas y profesionales para realizar los delitos como programadores, spammer, empaquetado de malware, administradores de redes etc. Es personal con conocimiento para realizar delitos informáticos.

La organización delincuencial Carbanak, conocida como Fin7, ha robado por lo menos USD 1.000 millones a operadores de servicios financieros entre 2013 y 2016 a nivel mundial, operando en más de 20 países.

El país que más sufre de ataques cibernéticos es Indonesia, adicional se indica que uno de los delitos más populares son los ataques focalizados en contra de una persona, previo seguimiento a sus perfiles en redes sociales, cuentas bancarias, vida personal, etc.

Otros tipos de ataques son contra organizaciones con el fin de deteriorar o afectar su imagen o reputación con diferentes tipos de fraudes, se interrumpen servicios, páginas web, correos electrónicos, interceptan llamadas, etc.

Adicionalmente un estudio adelantado en el 2016, por el Ponemon Institute e IBM Security afirma que para una Compañía el costo por cada registro perdido con información confidencial es mayor a US$141 por registro, además que el sector financiero ocupa uno de los primeros lugares de la lista de industrias en las qué las pérdidas de datos son los más costosos. Dicho estudio también informa que los ataques por **código malicioso** son los de mayor costo; pues el 47% de las brechas de seguridad son generadas por este tipo de ataque, generando un costo de US$156 por registro. El informe del año 2017 reporte una disminución del 10% del costo promedio por la violación de sistemas de información, por lo tanto, el costo promedio de cada registro perdido o robado disminuyó de US$158 a US$141. Sin embargo, el estudio también revela que el incumplimiento es mayor por parte de las compañías.

Mediante ataques informáticos se pueden exponer los datos personales y dado que en la actualidad los delitos o ataques informáticos utilizan mecanismos cada vez más sofisticados, esto conlleva que las compañías colombianas están expuestas a un alto riesgo de pérdida de datos, fuga de información, toda vez que son los objetivos preferidos para los atacantes; ejemplo de ello son casos reconocidos como:

- ***Red social Adult FriendFinder:*** Ataque a las bases de datos, a través de la cual fueron expuestos más de 400 millones de registros.

- ***Fling.com:*** El ataque malicioso expuso 40 millones de datos, incluidas contraseñas y preferencias sexuales de los usuarios.

- ***Equifax:*** Fuga de información como nombres, número de seguridad social, fecha de nacimiento, direcciones.

- ***Facebook:*** Filtración de información (usuario, número de teléfono) de 267 millones de cuentas en el año 2019, de acuerdo al reporte de Comparitech a través de su blog corporativo.

- ***Capital One Financial Corp.:*** En el 2019 esta compañía que emite tarjetas de crédito en Estados Unidos presentó un incidente por robo de la información de más de 100 millones de clientes causado por una ingeniera exfuncionaria de Amazon Web Services.

La falta de concientización en lo que respecta a seguridad informática y la extrema confianza de los usuarios al compartir su información personal en la red, facilitan la tarea a los cibercriminales. Uno de los mecanismos más fáciles y sencillos para el robo de datos es el “Phishing”, de acuerdo con un estudio adelantado por ESET, el robo de información es considerado por un 43% de las empresas como una gran preocupación. Múltiples vectores de ataques permiten que esta sea una de las problemáticas más relacionadas con la confidencialidad y la privacidad de la información. Tanto los códigos maliciosos y la explotación de vulnerabilidades, como el phishing, los empleados disconformes o la sobreexposición de datos en redes sociales son las herramientas iniciales para que los ciberdelincuentes conviertan esta preocupación en un incidente real.

Uno de los errores que más se cometen por las organizaciones y las personas es no tomar las medidas de seguridad respectivas frente al uso de tecnologías, confiarse en que no pasará nada, pues no se toma ninguna medida preventiva.

6.1 DENUNCIAS Y TENDENCIAS DE ATAQUES INFORMÁTICOS A NIVEL COLOMBIA

En Julio de 2018 el Centro Cibernético Policial a través del reporte “Análisis del Estado de Ciberseguridad” se identificaron nuevas amenazas asociadas al cibercrimen de las cuales sobresalen las siguientes:

- Estafa por suplantación de Sim card: SIM Swapping consiste en confundir al operador de celular solicitando una reposición de una Sim card ya rastreada previamente, es decir ya tienen los datos de las cuentas bancarias, cuando esto se logra, realizan movimientos de dinero.

- Tráfico de datos financieros: Vishing consiste en falsos call center, que realizan las llamadas para comercializar o promover productos por medio de engaños y que terminan siendo hurtos telefónicos.

- Fraude por falso WhatsApp: Smiching este fraude hace que al celular lleguen mensajes de texto que direccionan a una link, donde el usuario registra datos de sus cuentas bancarias y lo roban al momento de obtener sus datos.

- Ciberpirámides: Estos son grupos cerrados de WhatsApp hacen invitaciones a hacer aportes de dinero con falsas rentabilidades, esto sin soporte financiero alguno. [59]

Adicionalmente existen amenazas persistentes como:

- Ransomware (código malicioso): WannaCry y Petya.
- *Ataques a entidades gubernamentales*: A través de backdoor o puerta trasera que permitía el uso de herramientas de acceso remoto para ejecutar código malicioso y así lograr realizar actividades como transferencia no permitida de dinero, información y bases de datos.
- *Suplantación del correo electrónico*: Siendo el principal objetivo la suplantación de la dirección de email de colaboradores de las áreas financieras, ventas, bancos, entre otros.
- *Carding*: Para este tipo se encontró que los principales vectores de ataque fueron amenazas como Skimming, cambiazo de tarjetas, ataques en los cajeros automáticos, Phishing y Vishing.
- *Estafas por internet:* Dentro de esta modalidad se destacaron amenazas como Vishing, Smishing, Cartas Nigerianas.
- *Spyware:* Es un tipo de software instalado en un computador, para realizar seguimiento a sus datos personales, bancarios o actividades en línea.

Recientemente el Centro Cibernético de la Policía Nacional informo que durante el año 2018 recibieron 12.014 denuncias por hurto a través de medios informáticos, donde el 55% de éstas tuvieron como objetivo cuentas bancarias [60].

La Superintendencia de Industria y Comercio, el Centro Cibernético Policial, la Fiscalía General de la Nación entre otras entidades vienen reportando desde hace más de 5 años, los delitos cometidos contra ciudadanos por parte de

[59] Rico Torres, Alfonso. ""El dinero no crece en los árboles", recordó el organismo a quienes caen en este tipo de invitaciones" (En línea) (12, febrero, 2019) disponible en: https://www.rcnradio.com/economia/superfinanciera-alerto-sobre-nuevas-piramides-por-redes-sociales

[60] Radio Cadena Nacional S.A.S "Bancos así buscan blindarse ante aumento de ciber robos". (En línea). (3, octubre, 2019) Disponible en: https://www.lafm.com.co/economia/bancos-asi-buscan-blindarse-ante-aumento-de-ciberrobos).

algunas empresas o personas dedicadas a cometer delitos de manera intensional. Estás denuncias fueron realizadas por medio de canales virtuales y corresponde al 45.5% del total de denuncias para el año 2019. De manera presencial se realizan también denuncias a la violación de la Ley de protección de datos personales y corresponde al restante 54.5% los cuales están resumidos en la siguiente tabla:

Tabla 9. Indicadores de delitos informáticos en Colombia

Año	Denuncias
2015	7.523
2016	11.225
2017	15.840
2018	22.524
2019	17.531

Fuente: Cámara Colombiana de Informática y Telecomunicaciones. Informe de las tendencias de Cibercrimen en Colombia 2019-2020. (En línea). (enero a junio 2020) Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

Los principales motivos de multas o sanciones son:

- Envío de correos electrónicos comerciales sin copia oculta.
- Envío de correos electrónicos con fines comerciales, sin la autorización previa del titular del correo.
- Llamadas telefónicas ofreciendo servicios y/o productos sin la autorización del titular
- No atender oportunamente las solicitudes de los clientes de suspender los envíos de correos.

- Recolectar información personal de internet de redes sociales para contactar al titular para ofrecer productos o servicios.[61]

El uso de medios digitales, para realizar transacciones financieras por páginas autorizadas, actualmente se restringe por parte de los usuarios; ya que, al identificar la presencia de riesgos cibernéticos, se puede llegar a tomar la decisión de realizar o no la transacción.

A continuación se relacionan algunos de los casos reportados en el año 2019, por la superintendencia y que afectan los datos personales de los ciudadanos o usuarios. [62]

- **BANCO FALABELLA** por desatender a la solicitud de un usuario de eliminar sus datos de la entidad bancaria y por la tardanza en atender el caso. La multa fue de $496.899.600. La Superintendencia de Industria y Comercio le ordenó a la entidad bancaria adoptar medidas para respetar los derechos de las personas respecto al tratamiento de su información, como lo son, entre otros, el derecho de supresión de sus datos y la atención debida y oportuna de sus solicitudes. Las medidas que debe tomar la entidad bancaria son:

    - Suprimir de manera definitiva y oportuna los datos personales de los titulares que se lo soliciten cuando esa información es utilizada por el banco Falabella para fines comerciales o de marketing.

    - Responder de manera oportuna y de fondo las consultas o reclamos que presenten las personas, eliminando cualquier barrera innecesaria para garantizar los derechos de los titulares.

    - Poner a disposición del titular mecanismos gratuitos y de fácil acceso para presentar la solicitud de supresión de datos o la revocatoria de la autorización otorgada. Éstos deben implementarse a través de los mismos medios o canales mediante los cuales el banco Falabella se contacta o comunica con los titulares de los datos.

---

[61] Escuela de Privacidad. "Consultoría y Asesoría en Protección de Datos Personales." {En línea}. {14 marzo de 2020} disponible en: https://escueladeprivacidad.com/consultoria-y-asesoria-en-proteccion-de-datos-personales/

[62] Superintendencia de Industria y Comercio. "Rappi y Banco Falabella sancionados por incumplir Ley de Protección de Datos" (En línea). (13 marzo de 2008) disponible en: https://www.sic.gov.co/Rappi-y-Banco-Falabella-sancionados-por-incumplir-Ley-de-Proteccion-de-Datos

- Adicionalmente, la entidad bancaria deberá, no sólo implementar un mecanismo de monitoreo permanente respecto de la efectividad de las medidas adoptadas para dar cumplimiento a las anteriores órdenes, sino realizar una auditoría externa enfocada en la verificación de la aplicación de las medidas efectivas y apropiadas para cumplir todo lo ordenado.

☐ **RAPPI SAS** por no atender debidamente la solicitud de un usuario de no usar sus datos para fines comerciales o de marketing fue multada con la suma de $298.121.760. La Superintendencia le ordenó a RAPPI S.A.S. adoptar medidas para proteger los derechos de las personas en cuanto a la suspensión de sus datos y la exigencia de una autorización previa para el tratamiento de estos.

De acuerdo con el **Informe Tendencias del Cibercrimen Colombia 2019-2020** los delitos más denunciados en Colombia se describen en la tabla 10.

Tabla 10. Delitos más denunciados en Colombia

Cantidad	Tipo de delito
31.058	**Hurto por medios informáticos**
8.037	**Violación de Datos Personales (robo de identidad)**
7.994	**Acceso abusivo a un sistema Informático**
3.425	**Transferencia no consentida de Activos**
2.387	**Uso de Software Malicioso**

Fuente: Telecomunicaciones. Informe de las tendencias de Cibercrimen en Colombia (2019-2020).(En línea). Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf. p. 9-10.

De acuerdo al estudio realizado en el primer trimestre del 2020 y a las denuncias ya reportadas por los diferentes organismos de control, en Colombia, los delitos que más generan afectación tanto a las compañías como a los usuarios son el *hurto por medios informáticos* y aquí se hace referencia a la ***suplantación de sitios web*** o ***phishing***, luego está en segundo lugar la *violación de datos personales* y aquí podemos identificar la ***suplantación de identidad*** y la ***ingeniería social***, posteriormente y en tercer lugar, está el ***acceso abusivo a un sistema de información***, la transferencia no consentida de activos y el uso de software malicioso o el llamado ***Malware***.

6.2 TIPOLOGÍA DE AMENAZAS QUE AFECTAN LA SEGURIDAD DE LOS DATOS PERSONALES EN EL SECTOR FINANCIERO

La seguridad informática no es un tema estático, las organizaciones tienen que estar en constante desarrollo e innovación para evitar consecuencias catastróficas como daños a la reputación de los bancos y entidades crediticias perdida y confianza de la lealtad de los clientes y severas sanciones legales y regulatorias.

Para afrontar las amenazas a los servicios financieros es necesario armonizar la legislación de la región para combinar las experiencias, recursos y no limitar el intercambio de ideas también desarrollar más profesionales en diversos sectores como en las fuerzas de la ley; los servicios financieros y las telecomunicaciones, entre otros y sensibilizar a los profesionales de servicios financieros sobre la importancia de la seguridad cibernética.

Otro de los aspectos mencionados en el estudio nos permite identificar las estrategias usadas por los delincuentes: [63]

- Buscar las debilidades del software para ingresar al sistema IT
- Atacar contraseñas (spear-phising)
- Atacar sitios web para infectar a los usuarios con software malicioso
- Colocar software que bloquea a los usuarios fuera de sus propios sistemas (ransomware).

Para combatir con las estrategias usadas por los delincuentes el estudio propone, en primera instancia, que las autoridades gubernamentales sean más efectivas en la investigación y judicialización de los ciberdelincuentes e internamente las entidades bancarias deben capacitar periódicamente a sus empleados por medio de conferencias, debates, regulación y exposición de casos reales.

[63] SG/OEA. "Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe" (En línea) (2018) disponible en: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

Debido a la falta de efectividad gubernamental, muchas entidades no reportan oportuna ni adecuadamente los casos de incidentes de seguridad digital.

En cuanto al presupuesto estimado para la seguridad digital (seguridad de la información, ciberseguridad y prevención del fraude) se encuentra entre el 1% y 5% del Ebitda, incluyen plataformas y medios tecnológicos, recursos humanos, servicios tercerizados, capacitaciones. [64]

“Los profesionales de la seguridad citan el presupuesto, la interoperabilidad y el personal como sus principales limitaciones a la hora de administrar la seguridad (...). La falta de personal capacitado también se menciona como un desafío para la adopción de tecnología y procesos de seguridad avanzados.” [65]

[64] Ibid. p. 9.
[65] Centro Criptológico Nacional, “Ciberamenazas y Tendencias 2019” (En línea) (4, octubre, 2019) Disponible en: https://www.ccn-cert.cni.es/

7. PERTINENCIA DE LA SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE DATOS PERSONALES

7.1 QUÉ ES SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD INFORMÁTICA

Toda vez que el conocimiento y la información se ha convertidos en uno de los activos más valiosos del siglo XXI, los esfuerzos para mantener la información segura se han vuelto cada vez más importante.

La seguridad de la información se puede definir como el conjunto de prácticas aplicadas para mantener los datos seguros frente a accesos o alteraciones no autorizados durante todo su ciclo de vida, es decir, en reposo, procesamiento o cuando se transmiten de una equipo de cómputo, dispositivo de almacenamiento o ubicación física a otra. Cuando se habla de prácticas se hace referencia a controles organizativos o técnicos tales como: procesos, políticas, metodologías, soluciones tecnológicas que se diseñan e implementan para proteger la información del acceso no autorizado, uso inadecuado, divulgación no autorizada, destrucción o modificación.

Seguridad informática es un subconjunto de seguridad de la información y se entiendo como el conjunto de soluciones o herramientas tecnológicas, procedimientos y políticas aplicadas sobre la infraestructura tecnológica sobre la cual se crean, procesan, almacenan o trasmiten los datos; en otras palabras se hace referencia a la seguridad de los datos a nivel de hardware, software y redes, esto incluye, pero sin limitarse a: equipos de cómputo, servidores, redes de telecomunicaciones (equipos activos y pasivos de red, aplicaciones o software

Por otro lado es importante entender que la información o los datos tienen principalmente tres atributos o propiedades básicas y que usualmente se conoce como la tríada CIA (por su siglas en inglés confidentiality, integrity, and availability): Confidencialidad, Integridad y Disponibilidad. Y son precisamente estos atributos los que se pretenden proteger a través de la gestión de seguridad de la información. La gestión de seguridad de la información y seguridad informática tiene como columna vertebral la **gestión de riesgos**.

Más que aplicar una normatividad y seguir unos controles de acuerdo a los procesos del negocio, para comenzar a reconocer la pertinencia de la tecnología, el hardware y software al tema de Seguridad de la Información no solo en el sector financiero sino en cualquier entidad que requiera aplicar seguridad y privacidad a sus activos de información, es necesario mencionar que si no se tiene un sistema de control de riesgos enfocado a la privacidad y seguridad de la información, es imprescindible definirlo y para esto se debe comenzar con alinear los recursos humanos con los objetivos y la misión de cada organización. Sin este compromiso humano, lo técnico se vuelve innecesario, pues el factor humano debe tener el compromiso y la conducta adecuada en la protección de los datos.

La gestión de seguridad de la información y privacidad se apoya en normas, estándares, marcos de gestión y buenas prácticas que existen en el mercado para la gestión de seguridad de la información. En el siguiente recuadro se relacionan alguna de ellas que son referentes dentro de las Compañías en Colombia, incluidas las del sector financiero:

Tabla 11. Estándares más reconocidos en el mercado

Norma/Estándar	Descripción	Disponible en
ISO 27001	Estándar de seguridad de la información para la definición, implementación, operación y mantenimiento de un sistema de gestión de seguridad de la información.	No aplica
ISO 27032	Marco de gestión de ciberseguridad.	No aplica
ISO 27035	Mejores prácticas para la gestión de incidentes de seguridad de la información	No aplica
NIST Framework Cybersecurity	Marco que incluye estándares, directrices y mejores prácticas para gestionar el riesgo de ciberseguridad.	https://www.nist.gov/
NIST SP800-30	Guía para la evaluación de riesgos	https://www.nist.gov/
NIST SP800-53	Controles de seguridad para organizaciones y sistemas de información federales.	https://www.nist.gov/
NIST SP800-61	Guía para la gestión de incidentes de seguridad informática	https://www.nist.gov/
CIS	Entidad sin ánimo de lucro e integrado por una comunidad global de TI. Dentro de esta comunidad se encuentra CIS Controls y CIS Benchmarks que son un estándar global y de buenas prácticas para la protección de infraestructura tecnológica	https://www.cisecurity.org/
OWASP	Proyecto abierto de seguridad en aplicaciones web. Dentro de este proyecto se generan herramientas y documentación referente a seguridad en aplicaciones. El proyecto más conocido es el OWASP Top 10 y el cual consisten en la publicación periódica de las 10 principales vulnerabilidades en las aplicaciones web.	https://owasp.org/

Fuente: Elaboración propia.

7.2 IMPACTO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES EN EL DERECHO A LA PRIVACIDAD E INTIMIDAD

Internet y las nuevas tecnologías

El uso de las TIC en el país ha incrementado tal como lo manifiesta el ministro de las TIC, David Luna, quien en entrevista con la revista Enter.co indica que durante el año 2016 se tenían más de 15 millones de conexiones a internet, siete veces más que en el 2010[66]. La masificación del servicio de internet, la evolución del IoT, la aparición del Big Data, el uso cada vez mayor de redes sociales, trae consigo beneficios para la sociedad tales como fácil acceso a la información, fácil comunicación, almacenamiento de grandes cantidades de información, automatización de actividades, entre otros. Sin duda con las nuevas tecnologías los datos personales han adquirido un gran valor económico para las compañías toda vez que a través de la recolección de esta información se pueden establecer sus modelos predictivos de comportamiento de los clientes y sacar una ventaja económica.

Sin embargo, todo ello también conlleva a riesgos sobre la *confidencialidad*, *integridad* y *disponibilidad* de la información; estos riesgos como fraudes por internet, fuga de información, suplantación de identidad, ciberacoso, etc. Todo esto hace necesario tomar medidas preventivas de carácter técnico y organizacional.

7.3 IMPACTO POR INCUMPLIMIENTO DEL MARCO LEGAL Y REGULATORIO EN COLOMBIA

La protección y seguridad de la información personal radica en que es un derecho fundamental de cada persona el autorizar o no su información personal, porque se debe tener en cuenta temas de privacidad de los datos, intimidad, buen nombre y protección de datos personales[67].

De acuerdo con el Artículo 23 de la Ley 1581 de 2012, la SIC puede imponer sanciones a los responsables y encargados del tratamiento de los datos personales, estas sanciones podrán ser:

- Sanción económica de carácter personal e institucional hasta por un monto de 2.000 SMMLV.
- Suspensión de las actividades relacionadas con el tratamiento de los datos,

[66] GONZALES, Jeffrey. ¿Cómo se perfila la industria TIC en Colombia para 2017? (En línea). Febrero de 2017. Disponible en: http://www.unipamplona.edu.co/unipamplona/portalIG/home_15/recursos/01_general/09062014/n_icontec.pdf

[67] CONGRESO DE LA REPÚBLICA. Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá D.C., 2012. No 48587. p. 197.

hasta por seis (6) meses.
- Cierre temporal de las operaciones relacionadas con el tratamiento de los datos, esto en caso de haber trascurrido la suspensión sin haber adoptado las medidas correctivas ordenadas por la SIC.
- Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos personales sensibles.

Pese a que en Colombia existe regulación para la protección de datos personales como la Ley 1266 y la Ley 1581 de 2012, va en aumento las sanciones interpuestas por la SIC, durante el 2015 interpuso sanciones por 385.351 millones de pesos por incumplimiento a la Ley 1581, lo cual representa un aumento de un 51% más en multas interpuestas en el 2014 ($199.810)[68]. Y de acuerdo con la noticia publicada el 8 de junio del 2017 estas sanciones incluyen divulgación de datos en internet, hurto y/o pérdida de información contenida en bases de datos, entre otras razones[69].

La Superintendencia de Industria y Comercio, en ejercicio de sus funciones de inspección, vigilancia y control del régimen de protección de datos personales, ha impuesto multas que superan los $21 mil millones de pesos, además se han impuesto más de 610 sanciones desde el 2010, con respecto al tema de protección de datos personales en Colombia. Las sanciones aplicadas se relacionan con violaciones del habeas data financiero, reportes a centrales de riesgo que no corresponden con la realidad, no actualización oportuna de información o por no avisar al deudor antes de hacer el reporte a las centrales de riesgo; esto se acerca al 80% del total de sanciones impuestas[70].

Finalmente, la Superintendencia de Industria y Comercio ha impartido 1094 órdenes para que se corrijan, actualicen o eliminen datos en las bases de datos de las empresas y de esta manera generar un impacto directo e inmediato en beneficio del ciudadano, de su vida íntima y de su privacidad[71].

7.4 IMPACTO DE LOS DELITOS INFORMÁTICOS

Según estudios realizados por empresas de seguridad como ESET (ESET es una compañía de seguridad informática establecida en Bratislava, Eslovaquia) [72]actualmente, no solo en Colombia sino a nivel mundial los delitos informáticos aumentan a un nivel significativo, estos delitos involucran desde la venta de armas, venta de drogas, inducción al suicidio, estafas, pornografía infantil, hurto a cuentas

[68] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Informe de Gestión 2015. Bogotá. p.5.
[69] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Multas por violaciones de datos personales, (En línea)(8 de junio de 2017). Disponible en: http://www.sic.gov.co/noticias/por-violaciones-de-datos-personales-superindustria-ha-impuesto-sanciones-por-mas-de-21-mil-millones-de-pesos.
[70] Ibid. p.1
[71] Ibid. p.1
[72] Enjoy Safer Technology. ESET (En línea) (2018) disponible en: https://www.welivesecurity.com/

bancarias y tarjetas de crédito, extorsiones sexuales, suplantación de identidad, pirámides', Estos son solo algunos de los muchos delitos que se reportan a través de internet por una aplicación de la policía nacional que permite denunciar todo tipo de abusos y delitos presenciales e informáticos que se cometen en el país y su crecimiento es constante. Podemos decir que estos delitos, es una nueva modalidad de crimen organizado [73].

Según datos de la fiscalía y la policía nacional, el incremento por delitos informáticos ha tenido un aumento del 31%, desde el 2016; sin embargo, las denuncias con respecto al mismo periodo del año anterior aumentaron en un 201% esto es una cifra preocupante y que enciende alarmas en todos los aspectos de la vida.

Por otro lado, Symantec a través de su Informe indica que: En el año 2013 "solamente en Brasil, los costos de los delitos cibernéticos alcanzaron los USD 8,000 millones, seguidos por México con USD 3,000 millones y Colombia, con USD 464 millones. A nivel mundial, una de cada ocho violaciones de datos dio como resultado la exposición de 10 millones de identidades"[74].

Un reciente estudio realizado por Legal Hiel en alianza con LEGIS arrojó que las empresas del sector financiero y solidario son las más preocupadas por respaldar la información personal de sus clientes (35%); seguida por el sector educativo, principalmente universidades (25%) y, en tercer lugar, las empresas de servicios públicos (25%). "El sector salud, a pesar de tener el mayor riesgo por la cantidad de datos sensibles que maneja, apenas alcanza el 15% en la intención a registrar y proteger la información personal de los usuarios[75].

7.5 PELIGROS Y AMENAZAS DEL NUEVO ENTORNO

En efecto, la tecnología y su aplicación a sistemas de comunicación cada vez más avanzados, pone en evidencia la necesidad de controlar y regular el movimiento creciente de bases de datos de contenido personal, en algunas áreas sensibles de la sociedad, como lo son: el sistema financiero, la salud, la educación y lo judicial [76].

[73] El tiempo. "Denuncias por delitos informáticos crecieron el 31 % el año pasado" (En línea). (14 marzo de 2020) disponible en: http://m.eltiempo.com/justicia/delitos/denuncias-por-delitos-informaticos-crecieron-en-2017-172294

[74] SYMANTEC. Tendencias de seguridad cibernética en América Latina y el Caribe. (En línea). Junio de 2014. Disponible en Internet: https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf.

[75] CARACOL RADIO. Sector salud el menos preocupado por resguardar los datos personales de sus clientes. (En línea). 15 de septiembre de 2017. Disponible en Internet: http://caracol.com.co/programa/2017/09/15/sanamente/1505506347_788925.html.

[76] CALLE, Sol Beatriz. Apuntes jurídicos sobre la protección de datos personales a la luz de la actual norma de habeas data en Colombia. (En línea), Enero de 2009. Disponible para consulta en: http://www.icesi.edu.co/revistas/index.php/precedente/article/view/1459.

Sin embargo, dado el desarrollo de servicios en Internet y del comercio electrónico genera nuevas amenazas para la privacidad e intimidad de los usuarios, toda vez que, a través de las páginas se recolecta información, ya sea para comprar o no, dada la facilidad para su recolección y análisis, sin informar para qué se requiere y cuál es su finalidad, los mecanismos de protección ni los derechos que tiene el usuario sobre su información.

Sumado a esto, cuando el usuario navega por Internet, desconoce que su navegación puede ser grabada por mecanismos de seguimiento. Las compañías de comercio electrónico utilizan numerosos métodos para identificar y efectuar seguimientos de los consumidores en la red. Uno de los métodos más conocidos, actualmente, consiste en la utilización de las denominadas “cookies”. Estas consisten en que los sitios donde se visita dejan una pista en el disco duro (“cookie”) del usuario, esta pista permite al sitio conocer las veces que el consumidor visita al sitio y hacer seguimiento de la actividad del consumidor, pudiéndose crear así un perfil de gustos de éste. El titular del sitio puede negociar, con determinadas empresas, la transmisión de los datos; que luego, será utilizado en campañas publicitarias dirigidas a seguros potenciales consumidores.

Solo el hecho de grabar pistas en el disco duro del consumidor ya es una flagrante violación a la privacidad. Aunque el consumidor puede fijar el nivel de seguridad de los “cookies”, lo cierto es que, la mayoría de los consumidores, no tienen conocimiento sobre ellos, por lo tanto, aceptan niveles bajos de protección de “cookies” sin conocer lo que son, ni sus implicaciones. por otro lado, muchos sitios web requieren, para que puedan acceder a ellos, el permiso para grabar “cookies”, de lo contrario, no permiten que los consumidores accedan a sus páginas. Al menos, en estos casos, se le está haciendo saber al consumidor la posible grabación de “cookies”, y es decisión de él si acepta o no. Pero como se dijo antes, la mayoría de los consumidores desconocen qué son, para qué sirven y sus consecuencias.

7.5 CONTROLES ORGANIZATIVOS, OPERATIVOS Y TÉCNICOS

Durante el desarrollo de los capítulos anteriores se ha evidenciado la relevancia a del derecho a la privacidad, que de manera general lo que busca es impedir la vulneración de un derecho fundamental como el uso o almacenamiento de los datos personales de forma no autorizada, el abuso en el uso de estos o la divulgación no autorizada de los datos.

Para obtener una protección de datos, es necesario no solo toda la plataforma jurídica o normativa que se construya para este propósito, también se hace

perentorio adherir una serie de mecanismos o controles técnicos o tecnológicos que contribuyan a asegurar la privacidad y seguridad de los datos personales en el ámbito de los sistemas informáticos.

Las medidas de seguridad para la protección de datos personales se concentran principalmente en mecanismos, sistemas y metodologías de índole informático que facilitan el cumplimiento de los principios básicos de la protección de datos personales así como de la legislación.

Según el abogado Velasco Melo, en su artículo sobre derecho informático y la gestión de la seguridad de la información, "la trascendencia de la seguridad de la información en las organizaciones públicas o privadas radica en que: (i) el volumen de información crece día a día; (ii) la información es un intangible con un valor bastante apreciable en la economía actual; (iii) la información es una ventaja estratégica en el mercado, que la convierte en algo atractivo para la competencia, como elemento generador de riqueza, (iv) la frecuencia de los ataques a los activos de una organización es cada vez mayor, cualquiera que sea el medio al que se acuda, y (v) no existe una cultura de seguridad en los usuarios de la información, lo que conduce a que las organizaciones empiecen a incorporar prácticas seguras de protección de la información, advirtiendo que este proceso habrá de impactar la cultura de la organización; aspecto que requiere de tiempo y compromiso, empezando por la dirección de la misma"[77].

De acuerdo con lo anterior y toda vez que es deber de las Compañías la adopción de esta legislación, cobra relevancia e importancia para éstas el contar con mecanismos técnicos, operativos y organizacionales para la protección de datos durante todo su ciclo de vida, por lo tanto, es aquí donde se hace relevante la seguridad de la información, incluida la seguridad informática. Para este propósito un punto de partida es la implementación del SGSI, toda vez que la ISO 27001 garantiza la privacidad de la información, no solo desde el punto de vista técnico, sino organizacional.

Por lo tanto, definir, implementar y mejorar continuamente la gestión en seguridad de la información dentro de la Compañía representa un beneficio en materia de competitividad, confianza y cumplimiento legal. De manera que algunas de las medidas que se pueden implementar para el manejo y tratamiento seguro de los Datos Personales es la implementación de controles como los propuestos en el Anexo A de la norma ISO 27001 o los propuestos por el NIST a través de su publicación SP 800-53, los cuales disponen controles desde la perspectiva organizacional (recurso humano, políticas, procedimientos, etc.) y técnica

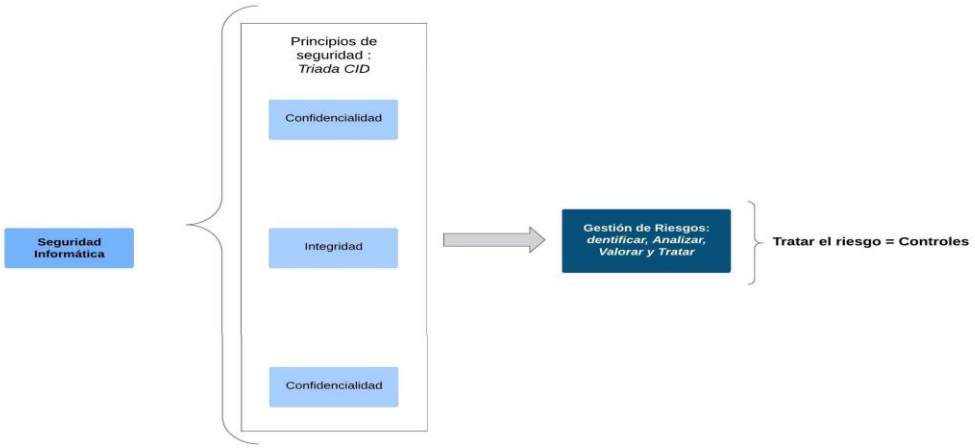
[77] VELASCO, Arean Hernando. El Derecho Informático y la Gestión de la Seguridad de la Información una perspectiva con base en la norma ISO 27001. (En línea), Junio de 2008. Disponible para consulta en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-86972008000100013.

(Hardening o aseguramiento de la plataforma crítica, seguridad perimetral, gestión de vulnerabilidades técnicas, cifrado de la información, entre otros).

De hecho La regulación europea en esta materia y la cual entró en vigor a partir de mayo del 2016 y que es de obligatorio cumplimiento a partir de mayo de 2018, establece nuevos controles de seguridad. Estos controles incluyen el cifrado (Artículo 32), doble factor de autenticación. Es de resaltar que esta normatividad menciona como otros sujetos obligados ubicados fuera de la Unión Europea que dirijan sus servicios a usuarios de países miembros o que reciban datos personales desde Europa.

De lo descrito con anterioridad, se puede deducir que las medidas de seguridad informática **correctamente implementadas y gestionadas aportan un adecuado nivel de seguridad y protección de los da**tos frente a los posibles ataques informáticos. Esto se resume de la siguiente manera:

Figura 4. Relación seguridad informática y protección de datos personales



[78]

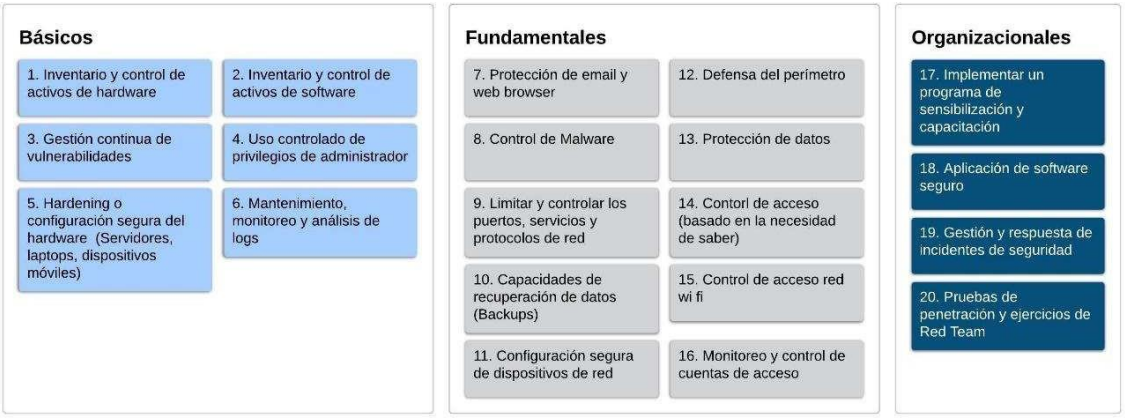
Fuente: Elaboración propia.

Los diferentes estándares de seguridad proponen controles que sirven como referencia para la seguridad y protección de los datos, por ejemplo la ISO 27001 en su anexo A establece 114 controles agrupados en 14 dominios, la NIST SP800-53 define 18 familias de controles. Sin embargo el CIS (Center for Internet Security) es

[78] Enjoy Safer Technology. ESET Security Report Latino América 2017. (En línea) (2018) disponible en: https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

una organización independiente sin fines de lucro cuya misión es desarrollar buenos ejemplos de soluciones de ciberseguridad y ha priorizado los controles que colectivamente permiten la defensa y protección de la información contra los ataques más comunes, esto se debe a la participación de una comunidad de expertos en TI que aplican su experiencia de primera mano como defensores cibernéticos para crear estas mejores prácticas de seguridad aceptadas globalmente. Los controles CIS se sustentan de información de ataques reales y defensas efectivas y el conocimiento combinado de expertos de cada parte del ecosistema (empresas, gobiernos, individuos); en la figura 5 se presentan los controles del CIS por prioridad, desde los controles básicos hasta los más avanzados.

Figura 5. Controles CIS



Fuente: Elaboración propia.

7.6 MEJORAS EN LA SEGURIDAD DE LOS DATOS EN EL SECTOR FINANCIERO

7.6.1 Enfoque preventivo. Las capacidades preventivas deben fortalecerse y madurar, esto implica no solo ser reactivos ante eventos o incidentes.

7.6.2 Nuevos mecanismos de monitoreo. El volumen de transacciones que las entidades financieras manejan a través de sus canales digitales y no digitales dificulta su revisión a través de mecanismos o herramientas tradicionales. Por esta razón, es pertinente que incorporen nuevas tecnologías basadas en Machine learning que les permita controlar, buscar, analizar, visualizar y tomar decisiones sobre flujos masivos de datos en tiempo real; dicho en otras palabras, identificar en

tiempo real operaciones sospechosas, actividades fraudulentas, análisis y correlación de eventos, entre otros.

Las tecnologías basadas en Machine learning permiten interpretar y aprender de los datos colectados permitiendo generar una análisis deductivo y predictivo.

7.6.3 Nuevas capacidades. Es importante que las entidades financieras coordinen los esfuerzos dentro de sus áreas para responder a los ataques cibernéticos. Por otro lado el enfoque tradicional de las compañías ha sido la protección y detección, sin embargo dadas las frecuentes amenazas emergentes y evolutivas hace necesario que mejoren e incorporar nuevos mecanismos de detección, respuesta y recuperación, inclusive soluciones o tecnologías de predicción de sucesos y ataques.

7.6.4 Evitar el enfoque único al cumplimiento normativo. La seguridad debe ser vista como un habilitador de negocio, no solo enfocarse en el cumplimiento regulatorio, sino fortalecer las capacidades internas para la gestión de riesgos que le permita reducir su nivel de exposición.

8. CONCLUSIONES

- Hoy la transformación de la era digital ha tenido un avance significativo sobre todo en las redes sociales, el internet de las cosas y en la tecnología móvil, sin embargo por este tipo de tecnologías es muy frecuente encontrar ofertas y servicios de fácil acceso y que llaman la atención de los usuarios a estas tecnologías, sin embargo; por este tipo de actividades es que se cometen actos delictivos, que amenazan el robo de información personal, sensible y que puede llevar a pérdidas financieras significativas. El exceso de confianza y obstinación de los usuarios de compartir su información personal.

- El desarrollo del internet, las comunicaciones y la construcción de computadoras personales, hace que toda esta infraestructura tecnológica no necesariamente estén pensados o creados en pos de la seguridad de la información, por lo tanto se genera lo que hoy llamamos vulnerabilidades, es por eso que en comparación con la normatividad de protección de datos personales es necesario tener los controles que sean necesarios para preservar la confidencialidad, la disponibilidad y la integridad, esto significa que las medidas y controles que se realizan realmente aseguran que los datos son accedidos únicamente por el personal debidamente autorizado y autenticado y con los respectivos permisos; adicionalmente, que la información solo sea actualizada por personal autorizado y que realmente se encuentre disponible cuando se necesite. Para lograr todo esto, es necesario tener en cuenta aspectos tanto técnicos, físicos y administrativos. Sin embargo, la seguridad solo comienza cuando todos los niveles jerárquicos en una organización son conscientes de su importancia y se toman las medidas necesarias para dar la seguridad suficiente. Al faltar tan solo uno, a esos controles y medidas ya no hay seguridad.

- En la actualidad, las instituciones están haciendo frente a diferentes tipos de presión, tales como:
    - Atraer nuevos clientes y competidores emergentes (por ejemplo las startup Fintech), implica la adopción de nuevos sistemas y modelos ágiles, exponiéndose a mayores riesgos.
    - Un entorno de amenazas dinámico, donde los atacantes innovan de manera mucho más rápida.
- Con el entorno tecnológico cambiante y el boom de la transformación digital es pertinente que las compañías del sector financiero reexaminen sus estrategias de ciberseguridad y las acople con esta nueva realidad.

- Por otro lado, el sector financiero tiene retos en cuanto a ciberseguridad dado las nuevas soluciones emergentes como: servicios en nube, el internet de las cosas y sumado a ello la falta de personal especializado en

ciberseguridad.

- Dicho lo anterior, es vital que las compañías maduren sus procesos de gestión de riesgos de manera que incluyan la revisión de las tendencias en amenazas y vulnerabilidades, incorporar la gestión de riesgos desde la planeación de nuevos proyectos independiente de su naturaleza, identificar minuciosamente los flujos de información para enfocar sus esfuerzos en la protección de la información confidencial o sensible

9. RECOMENDACIONES

Por lo anterior y de acuerdo a tecnologías actuales es importante la adaptación de tecnologías que involucren Machine Learning; ya que esto permite de manera automática obtener tendencias, patrones y relaciones con la información y los datos[79], indicadores que permiten a las organizaciones ser proactivos ante las situaciones que se presentan. Aquí se puede hablar de soluciones SIEM (por ejemplo: Splunk, Elastic Stark) y complementarlas con tecnologías de análisis de comportamiento e identidades (UBA/UEBA) y tecnologías para la orquestación y automatización (SOAR), de manera que le permita a la Compañía tener visibilidad completa sobre su postura de seguridad y reducir los tiempos de respuesta de los incidentes de seguridad de la información.

Es necesario que las compañías empiecen a robustecer sus procesos de gestión de incidentes, de manera que documenten y prueben planes de respuesta a incidentes para cada tipo o categoría de incidente (malware, Denegación de servicio, etc.) lo cual acompañados de soluciones SOAR reducirán considerablemente los tiempos de contención, erradicación, recuperación y por ende el impacto que trae consigo un incidente.

El uso de móviles y correos corporativos y personales por parte de ejecutivos y personal de confianza hace necesario la definición de pautas y normas de uso, que establezcan seguridad, confidencialidad y responsabilidad.

En la comunicación con los clientes, también es necesario la definición en la seguridad, privacidad y confidencialidad de las relaciones, pues cualquier tipo de comunicación que detrás no contenga una norma o procedimiento de seguridad, hace que pueda existir una ruptura y una oportunidad de fraude, que obviamente conlleva a la pérdida de dinero, tiempo y lo más importante de información financiera y de la empresa. Aquí es necesario considerar los mecanismos de seguridad perimetral de la organización y sus relaciones comerciales.

No menos importante es pertinente no dejar de lado los programas de sensibilización y capacitación para todos los colaboradores y terceros de la entidad financiera, puesto que usualmente un incidente es originado por una persona de forma accidental o premeditada y para ello no existen tecnologías. Cada vez es más relevante, generar una cultura de seguridad y esto se logra con sensibilización.

[79] CLEVERDATA. "¿Qué es Machine Learning?" (En línea) (2020) disponible en: https://cleverdata.io/que-es-machine-learning-big-data/

BIBLIOGRAFÍA

CONGRESO DE LA REPÚBLICA. Constitución Política de Colombia. Bogotá. (4, julio, 1991). Gaceta Constitucional número 114. 1991. (s.f.).

CONGRESO DE LA REPÚBLICA. Decreto 1115, (29, junio, 2017). Por el cual se modifica el artículo 2.2.2.26.3.1 del Decreto número 1074 de 2015 - Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Bogotá D.C., 2017. No 50279. 38 p. (s.f.).

CONGRESO DE LA REPÚBLICA. Decreto 1727 (16, agosto, 2012) Por la cual se determina la forma en la cual lo operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la provenientes de terceros países, deben presenta. (s.f.).

CONGRESO DE LA REPÚBLICA. Decreto 2952 (6, agosto, 2010) Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008. Diario Oficial. Bogotá D.C., 2010. No 47793. 16 p. (s.f.).

CONGRESO DE LA REPÚBLICA. Ley 1266 (31, diciembre, 2008). Por la cual se dictan las disposiciones generales sobre el hábeas data. Diario Oficial. Bogotá D.C., 2008. No 47219. 11 p. (s.f.).

CONGRESO DE LA REPÚBLICA. Ley 1273 (5, enero, 2009) Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que u. (s.f.).

CONGRESO DE LA REPÚBLICA. Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá D.C., 2012. No 48587. 197 p. (s.f.).

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO 1995 L 281. (s.f.).

LAZPITA GURTUBAY, María. 1994. Análisis comparado de las legislaciones sobre protección de datos de los Estados miembros de la Comunidad Europea. Informática y Derecho 6-7 (La protección de datos personales en la L.O.R.T.A.D y derecho comparado): Mérida, . (s.f.).

OERTING, Troesls y DOYLE, Sean. Foro Económico Mundial: El panorama de la amenazas a la ciberseguridad en los Bancos de América Latina y el Caribe. Citado por CONTRERAS, Belisario, et al. Estado de la Ciberseguridad en el Sector Bancario en América Latina. (s.f.).

PEREZ-LUÑO. Enrique César. El procedimiento de Habeas Data. El derecho procesal ante las nuevas tecnologías. Madrid: DYKISON, S.L. 336 p. ISBN 978-84-91-48-231-4. (s.f.).

Warren, Samuel, Brandeis Louis, El derecho a la intimidad, Editorial Civitas S.A., Madrid 1995, p. 25. (s.f.).

WEBGRAFIA

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS. “Resolución 217 A (III) Declaración Universal de Derechos del Hombre [en línea]. (10 de diciembre de 1948)) París, Naciones Unidas. 1948. Disponible en: https://www.un.org/es/universal-declaration-human-rights/inde. (s.f.).

Cámara de Diputados del H. Congreso de la Unión. "Ley Federal de Protección de Datos Personales en Posesión de los Particulares" (En línea). (5, julio, 2010) disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf. (s.f.).

Cano, Lucero Galvis. "Protección de datos en Colombia, avances y retos". Revista Lebret 4, n.º 4 (1 de enero de 2012): 195-214. (En línea). (13 marzo de 2008) disponible en: https://doi.org/10.15332/rl.v4i4.336 p.199. (s.f.).

CARACOL RADIO. Sector salud el menos preocupado por resguardar los datos personales de sus clientes. (En línea). 15 de septiembre de 2017. Disponible en Internet: http://caracol.com.co/programa/2017/09/15/sanamente/1505506347_788925.html. (s.f.).

CARACOL RADIO. Sector salud el menos preocupado por resguardar los datos personales de sus clientes. (En línea). 15 de septiembre de 2017. Disponible en Internet: http://caracol.com.co/programa/2017/09/15/sanamente/1505506347_788925.html. (s.f.).

Centro Criptológico Nacional, “Ciberamenazas y Tendencias 2019” (En línea) (4, octubre, 2019) Disponible en: https://www.ccn-cert.cni.es/. (s.f.).

CLEVERDATA. "¿Qué es Machine Learning?" (En línea) (2020) disponible en: https://cleverdata.io/que-es-machine-learning-big-data/. (s.f.).

COLOMBIA. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. "Por violaciones de datos personales, Superindustria ha impuesto sanciones por más de $21 mil millones de pesos" (En línea) (8, junio, 2017) Colombia. Disponible en: https://www.sic.gov.co/noticias/por-v. (s.f.).

COLOMBIA. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. “Protección de Datos Personales” {En línea}. {diciembre 2016} Disponible en: https://www.sic.gov.co/proteccion-de-datos-personales. (s.f.).

DIARIO OFICIAL DE LA FEDERACIÓN. "Ley Federal de Protección de Datos Personales en Posesión de los Particulares" (En línea). (5 julio de 2010) disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf. (s.f.).

El Tiempo. "Denuncias por delitos informáticos crecieron el 31 % el año pasado" (En línea). (14 marzo de 2020) disponible en: http://m.eltiempo.com/justicia/delitos/denuncias-por-delitos-informaticos-crecieron-en-2017-172294. (s.f.).

ENATIC. “Nuestros datos personales, fuente de negocio y actividades de profiling” (En línea) (17 de octubre de 2019) disponible en: https://www.abogacia.es/2016/09/21/nuestros-datos-personales-fuente-de-negocio-y-actividades-de-profiling/. (s.f.).

Enjoy Safer Tecnology. ESET (En línea) (2018) disponible en: https://www.welivesecurity.com/ . (s.f.).

Escuela de Privacidad. "Consultoría y Asesoría en Protección de Datos Personales." {En línea}. {14 marzo de 2020} disponible en: https://escueladeprivacidad.com/consultoria-y-asesoria-en-proteccion-de-datos-personales/. (s.f.).

ESPAÑA. WORLD ECONOMIC FORUM. "La cuarta revolución industrial-Klaus Schwab" (En línea)(diciembre 2016) Disponible en: http://40.70.207.114/documentosV2/La%20cuarta%20revolucion%20industrial-Klaus%20Schwab%20(1).pdf. (s.f.).

Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe [en línea]. Washington D.C: Organización de los Estados Americanos (OEA), 2018 [citado 2020-04-15]. Disponible en internet: https://www.oas.org/es/sms/cicte/sectorbancariospa. (s.f.).

GONZALES, Jeffrey. ¿Cómo se perfila la industria TIC en Colombia para 2017? [En línea]. Febrero de 2017. Disponible en: . (s.f.).

Norton. “¿Qué es la ingeniería social?” (En línea) (15 de diciembre 2018) disponible en: https://mx.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html .(s.f.)

https://www.dinero.com/internacional/articulo/principales-cifras-del-cibercrimen-mundo-colombia/213988, R. D. (s.f.).

La Vanguardia. Madrid “España y 20 países firman protocolo para el Convenio de Protección de Datos”. (en línea)(10 de Octubre 2018). Disponible en: https://www.lavanguardia.com/politica/20181010/452291023498/espana-y-20-paises-firman-protocolo-para-el-con. (s.f.).

MEXICO. CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN. "Ley Federal de Protección de Datos Personales en Posesión de los Particulares" (En línea). (5, julio, 2010) disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf. (s.f.).

MEXICO. DIARIO OFICIAL DE LA FEDERACIÓN. "Ley Federal de Protección de Datos Personales en Posesión de los Particulares" (En línea). (5 julio de 2010) disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf. (s.f.).

MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES. “Modelo_de_Seguridad_Privacidad” (En línea. (16 marzo de 2020) disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf. (s.f.).

PARIS. ASAMBLEA GENERAL DE LAS NACIONES UNIDAS. “Resolución 217 A (III) Declaración Universal de Derechos del Hombre [en línea]. (10 de diciembre de 1948)) París, Naciones Unidas. 1948. Disponible en: https://www.un.org/es/universal-declaration-human-righ. (s.f.).

Radio Cadenal Nacional S.A.S “Bancos así buscan blindarse ante aumento de ciber robos”. (En línea). (3, octubre, 2019) Disponible en: https://www.lafm.com.co/economia/bancos-asi-buscan-blindarse-ante-aumento-de-ciberrobos). (s.f.).

Rico Torres, Alfonso. ""El dinero no crece en los árboles", recordó el organismo a quienes caen en este tipo de invitaciones" (En línea) (12, febrero, 2019) disponible en: https://www.rcnradio.com/economia/superfinanciera-alerto-sobre-nuevas-piramides-por. (s.f.).

RODRIGUEZ, Eliana. Ciberseguridad, un componente fundamental de la transformación digital [en línea]. 2018 [citado 15-04-2020]. Disponible en internet: https://blog.cobiscorp.com/ciberseguridad-transformacion-digital. (s.f.).

Superintendencia de Industria y Comercio. "Rappi y Banco Falabella sancionados por incumplir Ley de Protección de Datos" (En línea). (13 marzo de 2008) disponible en: https://www.sic.gov.co/Rappi-y-Banco-Falabella-sancionados-por-incumplir-Ley-de-Protecci. (s.f.).

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Circular Externa 005. [En línea], Agosto de 2017. Disponible en: http://www.sic.gov.co/sites/default/files/normatividad/082017/Circular_Externa_005_de_2017.pdf. (s.f.).

SUPERINTENDENCIA FINANCIERA DE COLOMBIA. "Circular Básica Jurídica (C.E. 029/14) Parte I Título II Capítulo I" (En línea). (16 diciembre 2019) disponible en: https://www.superfinanciera.gov.co/publicacion/10102519. (s.f.).

SYMANTEC. Tendencias de seguridad cibernética en América Latina y el Caribe. (En línea). Junio de 2014. Disponible en Internet: https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf. (s.f.).

Tribunal Europeo de Derechos Humanos. “Convenio Europeo de Derechos Humanos (CEDH)" (En línea) (4, noviembre de 1950) disponible en: https://www.echr.coe.int/Documents/Convention_SPA.pdf. (s.f.).

VELASCO, Arean Hernando. El Derecho Informático y la Gestión de la Seguridad de la Información una perspectiva con base en la norma ISO 27001. (En línea), Junio de 2008. Disponible para consulta en: http://www.scielo.org.co/scielo.php?script=sci_arttext&p. (s.f.).

VELASCO, Arean Hernando. El Derecho Informático y la Gestión de la Seguridad de la Información una perspectiva con base en la norma ISO 27001. (En línea), Junio de 2008. Disponible para consulta en: http://www.scielo.org.co/scielo.php?script=sci_arttext&p. (s.f.).

Fecha de Realización: 26/04/2020
Título: SEGURIDAD INFORMÁTICA: RELACIÓN E IMPACTO FRENTE A LA LEY DE PROTECCIÓN DE DATOS PERSONALES (LEY 1581 DE 2012)
Autor: RUIZ GARZON, Marcela Patricia - AGUIRRE OLMOS, Diana Paola
Palabras Claves: Seguridad, Información, informática, Habeas data, Datos, Intimidad, Acción de Tutela, Derechos y deberes, Protección de Datos.
Descripción: Este documento intenta mostrar las referencias a tener en cuenta como parte de la recopilación de información que se quiere analizar, para realizar el desarrollo del trabajo de grado; es un documento que establece y define conceptos y aspectos de la Ley de Protección de Datos Personales.
Fuentes:

CONGRESO DE LA REPÚBLICA. Constitución Política de Colombia. Bogotá. (4, julio, 1991). Gaceta Constitucional número 114. 1991. (s.f.).

CONGRESO DE LA REPÚBLICA. Decreto 1115, (29, junio, 2017). Por el cual se modifica el artículo 2.2.2.26.3.1 del Decreto número 1074 de 2015 - Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Bogotá D.C., 2017. No 50279. 38 p. (s.f.).

CONGRESO DE LA REPÚBLICA. Decreto 1727 (16, agosto, 2012) Por la cual se determina la forma en la cual lo operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la provenientes de terceros países, deben presenta. (s.f.).

CONGRESO DE LA REPÚBLICA. Decreto 2952 (6, agosto, 2010) Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008. Diario Oficial. Bogotá D.C., 2010. No 47793. 16 p. (s.f.).

CONGRESO DE LA REPÚBLICA. Ley 1266 (31, diciembre, 2008). Por la cual se dictan las disposiciones generales sobre el hábeas data. Diario Oficial. Bogotá D.C., 2008. No 47219. 11 p. (s.f.).

CONGRESO DE LA REPÚBLICA. Ley 1273 (5, enero, 2009) Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que u. (s.f.).

CONGRESO DE LA REPÚBLICA. Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá D.C., 2012. No 48587. 197 p. (s.f.).

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO 1995 L 281. (s.f.).

LAZPITA GURTUBAY, María. 1994. Análisis comparado de las legislaciones sobre protección de datos de los Estados miembros de la Comunidad Europea. Informática y Derecho 6-7 (La protección de datos personales en la L.O.R.T.A.D y derecho comparado): Mérida, . (s.f.).

OERTING, Troesls y DOYLE, Sean. Foro Económico Mundial: El panorama de las amenazas a la ciberseguridad en los Bancos de América Latina y el

Caribe. Citado por CONTRERAS, Belisario, et al. Estado de la Ciberseguridad en el Sector Bancario en América Latina. (s.f.).
PEREZ-LUÑO. Enrique César. El procedimiento de Habeas Data. El derecho procesal ante las nuevas tecnologías. Madrid: DYKISON, S.L. 336 p. ISBN 978-84-91-48-231-4. (s.f.).
Warren, Samuel, Brandeis Louis, El derecho a la intimidad, Editorial Civitas S.A., Madrid 1995, p. 25. (s.f.).

Contenido del documento:

Metodología:
En este documento se utiliza una metodología de tipo explicativa, donde se recopila información del mismo tema a nivel nacional y mundial y es con respecto a la protección de datos personales, lo cual genera un resultado con base en diferentes tipos de investigaciones y estudios. El enfoque utilizado es mixto, pues se basa en diferentes indicadores e informes de investigación y adicional se analiza el sector financiero de manera cualitativa.

Conceptos nuevos: Phishing, Incidente de Seguridad, Riesgo de Seguridad, Malware, Vulnerabilidad, NIST, CIS, OWASP, Machine Learning, SIEM

- **Conclusiones:** Hoy la transformación de la era digital ha tenido un avance significativo sobre todo en las redes sociales, el internet de las cosas y en la tecnología móvil, sin embargo por este tipo de tecnologías es muy frecuente encontrar ofertas y servicios de fácil acceso y que llaman la atención de los usuarios a estas tecnologías, sin embargo; por este tipo de actividades es que se cometen actos delictivos, que amenazan el robo de información personal, sensible y que puede llevar a pérdidas financieras significativas. El exceso de confianza y obstinación de los usuarios de compartir su información personal.
- El desarrollo del internet, las comunicaciones y la construcción de computadoras personales, hace que toda esta infraestructura tecnológica

no necesariamente estén pensados o creados en pos de la seguridad de la información, por lo tanto se genera lo que hoy llamamos vulnerabilidades, es por eso que en comparación con la normatividad de protección de datos personales es necesario tener los controles que sean necesarios para preservar la confidencialidad, la disponibilidad y la integridad, esto significa que las medidas y controles que se realizan realmente aseguran que los datos son accedidos únicamente por el personal debidamente autorizado y autenticado y con los respectivos permisos; adicionalmente, que la información solo sea actualizada por personal autorizado y que realmente se encuentre disponible cuando se necesite. Para lograr todo esto, es necesario tener en cuenta aspectos tanto técnicos, físicos y administrativos. Sin embargo, la seguridad solo comienza cuando todos los niveles jerárquicos en una organización son conscientes de su importancia y se toman las medidas necesarias para dar la seguridad suficiente. Al faltar tan solo uno, a esos controles y medidas ya no hay seguridad.

- En la actualidad, las instituciones están haciendo frente a diferentes tipos de presión, tales como:
    - Atraer nuevos clientes y competidores emergentes (por ejemplo las startup Fintech), implica la adopción de nuevos sistemas y modelos ágiles, exponiéndose a mayores riesgos.
    - Un entorno de amenazas dinámico, donde los atacantes innovan de manera mucho más rápida.
- Con el entorno tecnológico cambiante y el boom de la transformación digital es pertinente que las compañías del sector financiero reexaminen sus estrategias de ciberseguridad y las acople con esta nueva realidad.
- Por otro lado, el sector financiero tiene retos en cuanto a ciberseguridad dado las nuevas soluciones emergentes como: servicios en nube, el internet de las cosas y sumado a ello la falta de personal especializado en ciberseguridad.

AUTOR: Diana Paola Aguirre Olmos, Marcela Patricia Ruiz Garzón.