INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO

FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS

ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

METODOLOGÍA DIRIGIDA A COMPAÑÍAS DISTRIBUIDORAS DE TECNOLOGÍA PARA EL MANEJO Y PROTECCIÓN DE LOS DATOS PERSONALES DE TERCEROS DE ACUERDO A LA LEY ESTATUTARIA 1581 DEL 2012 Y EL DECRETO 1377 DE 2013

PRESENTA:

ERIKA LORENA AGUILAR CORREDIN

YONATHAN ARBEY MONTERO MAHECHA

ASESOR TEMÁTICO:

WILMAR JAIMES FERNANDEZ

Marzo de 2018

ÍNDICE GENERAL

TABLA DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

Teniendo en cuenta las leyes que rigen en Colombia en cuanto a la seguridad de la información como lo es la ley 1581 de 2012, todavía existen vacíos en cuanto a las condiciones básicas de seguridad que se deben tener en el manejo y recolección de datos personales en entidades que por su naturaleza deben interactuar con ellos como son los mayoristas de tecnología o distribuidores, el incumplimiento de estas conlleva a sanciones y perdidas económicas, en donde se ve afectada la reputación de la compañía encargada del tratamiento de datos, en este caso las distribuidoras de tecnología. Para ello es necesario realizar un estudio del estado actual de este tipo de compañías y constatar si están cumpliendo con lo establecido en la ley mediante la revisión del decreto 1377 de 2013 en donde se muestra que aspectos importantes deben hacer las empresas en cuanto a la protección de los datos personales y sensibles de terceros. Para ello se realiza una metodología en donde se ejecutará una serie de fases como la investigación, establecimiento de la guía metodológica, establecimiento de buenas prácticas para el tratamiento seguro de datos personales y por último la aplicación de dicha guía sobre una compañía distribuidora de tecnología con el fin de dar un punto de partida de los requerimientos que se deben tener en cuenta para la protección de datos personales.

ABSTRACT

Taking into account the measures that govern in Colombia regarding the security of information as it does in the law 1581 of 2012, there are still in terms of the basic security conditions that must be met in the handling and collection of personal data in entities that by their nature must interact with them, such as technology wholesalers or distributors the breach of these leads to penalties and economic losses, where the reputation of the company responsible for data processing is affected, in this case the technology distributors. For this, it is necessary to carry out a study of the current state of this type of companies and verify if they are complying with the provisions of the law by means of the revision of Decree 1377 of 2013, which shows that companies in terms of protection of personal and sensitive data should do important aspects. To this end, a methodology is carried out in which a series of phases will be executed, such as research, establishment of the methodological guide, establishment of good practices for the safe handling of personal data and finally the application of said guide on a technology distribution company with In order to give a starting point of the requirements that must be taken into account for the protection of personal data.

PALABRAS CLAVE

Datos personales, seguridad, robo de información, regulación, riesgo, cumplimiento.

KEY WORDS

Personal data, security, information theft, regulation, risk, compliance.

INTRODUCCIÓN

La protección de datos personales es una de las principales dolencias para la mayoría de las empresas colombianas hoy en día, esto debido a que el incremento de crímenes cibernéticos como el robo de información confidencial provoca daños importantes tanto económicos como de reputación que pueden llevar a una empresa que se encuentre en producción a cerrar definitivamente su servicio. Colombia quiere evitar este tipo de ataques mediante la aplicación de leyes y normas que son de obligatorio cumplimiento en donde se da a conocer las condiciones básicas de seguridad para la protección de datos confidenciales.

Las empresas no dan un buen manejo a la información sensible ya que no conocen los datos que diariamente manejan y no tienen una clasificación de esta según las áreas de la empresa y su finalidad, no han definido roles y esto permite que todo el personal tenga acceso a la información contenida en los sistemas utilizados. Este caso puede llegar a ser un riesgo potencial que al no tener controles que permitan mitigarlo, las empresas podrían estar siendo atacadas por personas malintencionadas robando así su información, la cual puede ser utilizada con fines dañinos en contra de la compañía y/o en contra del dueño de los datos. Adicional es conveniente que se genere conciencia de que la información que se suministra a las diferentes entidades debe ser protegida y no debe ser disponible según requerimiento de cada persona con previa autorización.

La idea con el desarrollo de este documento es el establecimiento de una metodología para las compañías distribuidoras de tecnología en el manejo y protección de los datos personales de terceros de acuerdo a la ley Estatutaria 1581 del 2012 y el decreto 1377 de 2013, también es conveniente realizar el establecimiento de una serie de buenas prácticas a nivel de seguridad que servirán como posibles controles para ser usados cuando se aborde el tema de tratamiento de riesgos dentro de la guía metodológica a establecer y es necesario que sea puesta en práctica esta metodología para saber si la empresa cumple o o cumple con lo estipulado en las leyes existentes.

En cuanto al alcance del proyecto se enfoca en torno a definir una guía metodológica con la cual puedan tratarse de manera segura los requerimientos que se deben tener en cuenta para el cumplimento de la normativa existente en Colombia de protección de datos personales para las compañías distribuidoras de tecnología teniendo en cuenta la ley 1581 de 2012, el decreto 1377 de 2013 y la ley 1266 de 2008, donde se incluye temas de Habeas

Data. La misma va acompañada de un guía de buenas prácticas o controles los cuales permitirán dar manejo de forma segura a los datos y de esta manera definir los controles para abordar los posibles riesgos. La aplicación de la guía que se va a elaborar se realizara sobre una compañía distribuidora de tecnología a la cual se tiene acceso de nuestra parte a determinada información y que por términos de cláusula de confidencialidad no se entregara en este documento información como nombre real de la compañía. Para ello se dará desarrollo a lo largo de este documento inicialmente a un estado del arte en donde se puede evidenciar lo que se ha trabajado tanto a nivel nacional como mundial en relación con el tratamiento seguro de datos personales, posteriormente se plantea la metodología con la cual se desarrolló el proyecto, a continuación se encuentra el desarrollo de la metodología con las respectivos resultados y conclusiones que se obtuvieron de la ejecución de la misma

PROBLEMÁTICA

La protección de datos personales es una de las principales dolencias para la mayoría de las empresas colombianas hoy en día, esto debido a que el incremento de crímenes cibernéticos como el robo de información confidencial provoca daños importantes tanto económicos como de reputación que pueden llevar a una empresa que se encuentre en producción a cerrar definitivamente su servicio. Colombia quiere evitar este tipo de ataques mediante la aplicación de leyes y normas que son de obligatorio cumplimiento en donde se da a conocer las condiciones básicas de seguridad para la protección de datos confidenciales.

Las empresas no dan un buen manejo a la información sensible ya que no conocen los datos que diariamente manejan y no tienen una clasificación de esta según las áreas de la empresa y su finalidad, no han definido roles y esto permite que todo el personal tenga acceso a la información contenida en los sistemas utilizados. Este caso puede llegar a ser un riesgo potencial que al no tener controles que permitan mitigarlo, las empresas podrían estar siendo atacadas por personas malintencionadas robando así su información, la cual puede ser utilizada con fines dañinos en contra de la compañía y/o en contra del dueño de los datos.

Adicional es conveniente que se genere conciencia de que la información que se suministra a las diferentes entidades debe ser protegida y no debe ser disponible según requerimiento de cada persona con previa autorización.

OBJETIVOS

General

Establecer una metodología y una guía de buenas prácticas para el manejo y protección de datos personales de terceros de acuerdo a la ley estatutaria 1581 de 2012 y decreto 1377 de 2013 para compañías distribuidoras de tecnología.

Específicos

- Plantear una guía metodológica para el tratamiento de datos personales con enfoque seguro.
- Elaborar una guía de buenas prácticas-controles para el tratamiento de riesgos relacionados con el manejo de datos personales.
- Aplicar la guía metodológica diseñada a una compañía de distribución de tecnología

REVISIÓN DE LITERATURA / ANTECEDENTES

Con los avances tecnológicos que rodean el entorno y que a su vez influencian la forma en la cual se manipula la información en muchos aspectos de la vida cotidiana, se observa la necesidad de darle un manejo a estos datos personales de una manera adecuada, pues su mal uso puede llegar a afectar en temas económicos, socio culturales, morales, reputaciones entre otros, lo cual conlleva hacer énfasis en el eje central de la seguridad de la información como lo son los riesgos, dando un vistazo puntualmente a nivel comercial sobre la percepción de los consumidores y sobre los riesgos que se evidencian al compartir información personal con las compañías se plantea la existencia de riesgos:

- Económicos o monetarios
- Físicos
- Psicológicos
- Sociales

“Definimos cada uno de los riesgos de privacidad como los siguientes: (1) el riesgo monetario es el riesgo asociado con la posible pérdida financiera, (2) el riesgo social es el riesgo asociado con las amenazas a la autoestima, la reputación y / o las percepciones de un individuo de otros, (3) el riesgo físico es el riesgo asociado con lesiones corporales, y (4) el riesgo psicológico es el riesgo asociado con posibles emociones negativas, como ansiedad, angustia” [1]

Esa percepción de los consumidores se puede generalizar para indicar que es un aliciente hacia la adopción de las respectivas leyes y decretos para reglamentar el tratamiento de datos personales; a nivel de las compañías permite que se planteen estrategias basadas en buenas practicas que ayuden a cumplir con la normatividad y entregar un parte de tranquilad a las personas que deciden autorizar la entrega de información personal a dichas compañías.

Los gobiernos a nivel mundial han tenido que empezar a regular y definir lo que se conoce como derecho habeas data, tal como lo indica Cheng De Qin en su artículo escrito para la Xi'an University of Posts and Telecommunications “Con el rápido desarrollo de la tecnología de la computadora y la red, la violación sin precedentes del derecho a la privacidad individual en el ciberespacio es cada vez más grave, lo que ha obstaculizado el progreso

del comercio electrónico y la economía de red. Fortalecer la protección legal de los datos personales y el derecho a la privacidad en el ciberespacio es una tarea urgente y necesaria que enfrentan los gobiernos de todo el mundo" [2], en donde es claro que a nivel mundial se ha venido trabajando al respecto y existen países que han avanzado bastante con respecto a otros como lo es el caso de España, "existe experiencia de países que se encuentran adelantados en el tema de protección de datos, que una vez creado el sistema jurídico, es necesario la creación de una autoridad que regule el uso de las bases de datos como por ejemplo la agencia española de protección de datos, este ente autónomo cuya finalidad es velar por el cumplimiento de la legislación en cuanto a los derechos de información, acceso, rectificación, oposición y cancelación de datos"[3]. En el caso de Colombia no se ve lejano empezar a implementar este tipo de leyes y a través de la corte constitucional por medio de sentencias consagro respecto a la protección de datos personales que "el habeas data o autodeterminación informática le otorga al titular de los datos personales, la posibilidad de exigir a las administradoras de datos, el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos" [4], por tanto las personas tienen derecho a conocer, actualizar y a rectificar su información personal almacenada en bases de datos, también se ha llegado a una clasificación de los tipos de datos en donde se pueden encontrar los siguientes tipos:

- Privados
- Semipúblicos
- Públicos
- Reservada

A continuación, se realiza una pequeña descripción de cada uno de los anteriores tipos, "datos de Información pública es aquella que puede obtenerse sin reserva alguna, entre ella los documentos públicos" [4]. Información semiprivada "es aquel dato personal o impersonal que, al no pertenecer a la categoría de información pública, sí requiere de algún grado de limitación para su acceso" [4]. Información privada "es aquella que se encuentra en el ámbito propio del sujeto concernido y, por ende, solo puede accederse a ella por orden de autoridad judicial competente y en ejercicio de sus funciones" [4]. Por ultimo información reservada "es aquella que solo interesa a su titular en razón a que se relaciona

estrechamente con la protección de sus derechos a la dignidad humana, la intimidad y la libertad; como es el caso de los datos sobre la preferencia sexual de las personas” [4]

Para los responsables del tratamiento de datos, se estipularon unos deberes mínimos que deben cumplir para el tratamiento de información personal

- **Legitimización de datos y toma de consentimiento**: hace referencia a la legitimidad de los datos que se almacenan es decir si son reales y la obligación de conservar evidencias de que las personas entregaron su consentimiento para realizar el manejo.
- **Legalización de las bases de datos**: la obligación que tienen de registrar las bases de datos que poseen información personal frente al registro nacional.
- **Protección y seguridad de las bases de datos**: sobre las condiciones de seguridad que se deben garantizar con las bases de datos, además del cumplimiento en los principios como la finalidad de la recaudación de información que se dio a conocer a la persona antes de solicitar la aprobación, entre otros principios del habeas data.

Para muchos el tema de la protección de datos personales es violado más por desinformación, esto debido a que como nos dice el reportaje “la privacidad se trata menos de lo que se hace con la información que lo que no se hace con ella” [7], las personas que dan información confidencial a entidades exigen que la recopilen solo para el propósito o finalidad de la empresa y que estos no puedan ser recopilados para fines diferentes, si lo relacionamos con big data la privacidad de convierte en una característica importante y fundamental para que la información no publica sea salvaguardada según las leyes aplicables.

El tratamiento de datos masivos como lo maneja el big data y si hablamos en especial de las bases de datos que contienen información tanto pública como privada de las personas, se debe realizar un importante trabajo que como lo menciona Miguel Recio “Los datos personales masivos y su tratamiento analítico pueden conllevar importantes beneficios, que se concretan tanto en oportunidades de innovación en el caso de servicios electrónicos, por ejemplo las aplicaciones para dispositivos móviles o apps, como de nuevas formas de tratar enfermedades, incluso reduciendo los costos de tratamientos que hoy no son accesibles para todas las personas.” [8], lo digital está inundando al mundo y esto permite que la tecnología valla en aumento y que las regulaciones sean cada vez más estrictas en

el manejo que se deba realizar, muchas aplicaciones manejan sus datos en la nube, pero muchos de ellos no conocen en que datacenter de que país se encuentran almacenados y que en caso de error no garantizan que esa información se recupere; la regulación colombiana en el momento no controla ni rige la información que se encuentra en la nube ni cuales controles son de obligatorio cumplimiento para migrar información, pero es necesario que se empiece a contemplar porque como se revisó anteriormente el mundo está llegando a la Era Digital.

“Cuando el análisis de los datos masivos incluye datos personales, resulta necesario examinar desde el punto de vista del cambio regulatorio y de paradigma las implicaciones que pueda tener para sus titulares pasar de la privacidad por consentimiento a la privacidad a través de la responsabilidad” [8], lo que indica que debe prevalecer la trasparencia del manejo que se tiene a esto datos y su objeto de recolección, identificar qué empresa los está recolectando una entidad pública o del sector privado, quien será el encargado de tratarlos y protegerlos y quien será su usuario final o quien usar esa información y que permisos necesitaría para accederla. La legislación que en el momento se tiene fue pensada en el manejo mínimo de información que podría transportarse, pero en cuanto a tratamientos masivos de información como se está viendo hoy en día no se tuvo recomendación alguna y los que aumentaran en algunos años.

Si hablamos de las leyes que en el país se manejan podemos remitirnos al artículo de Oasis en donde nos dice “Colombia adoptó la Ley 1266 en 2008, con una acción final tomada en octubre de 2012, cuando la privacidad de datos integral. Después la Ley 1581 fue promulgada. Similar a las leyes en Argentina y Uruguay, la nueva ley prohíbe la transferencia de datos a través de las fronteras a los países que no tienen regímenes de protección de datos adecuados según lo determine el regulador colombiano, a menos que el interesado otorgue el consentimiento expreso previo. La legislación secundaria, el Decreto 1377, se emitió en junio de 2013” [9], a través de los años se ha venido actualizando y generando protección a los ciudadanos que aportan sus datos a diferentes entidades; con estas leyes se está proporcionando a los ciudadanos seguridad de que su información está siendo tratada según las leyes y que no serán divulgadas si antes no hay una aprobación o consentimiento en donde se exprese que la persona dio su acceso a información confidencial.

Habeas data

Como indicamos anteriormente Habeas Data es el termino como en Colombia se habla de protección de datos personales, “Este concepto es una noción legal que protege cualquier tipo de información relacionada con el individuo, desde la personal hasta la financiera, dándole de esta manera a la persona el poder de decidir cómo y dónde se pueden utilizar estos datos.” [9], los ciudadanos que den información a entidades tanto públicas como privadas están amparados bajo la ley y protegidos de que la información proporcionada será únicamente utilizada para los fines establecidos por la empresa, en caso que sean usados para otro tipo de solicitudes y enviados a otras entidades se acudirá a leyes y sus respectivas sanciones.

Eficiencia y evolución de las directivas de protección de datos a nivel mundial

A nivel mundial se hacen esfuerzos para que se dé el manejo adecuado a los datos personales pero ¿qué tan eficientes son dichos controles?, en una revisión se evidencio que es necesario contar con adaptabilidad a los cambios constantes de tecnología, por ejemplo la unión Europea en 1995 lanzo una serie de directivas que estaban basadas en el entorno de internet lo que se conoció como Web 2.0, pero más adelante se observó que se debían realizar ajustes por la evolución tecnológica presentada y ya que no se desarrolló en un entorno uniforme en todos los países miembros de la Unión Europea, se consideró hacia el año 2008 que eran anticuadas y tenían debilidades para la protección de datos personales de ese entonces, de esa manera en el 2012 se actualizaron dichas directivas dando cabida a principios de rendición de cuentas y transparencia.

Sobre el principio de transparencia, se considera de vital importancia en la protección de datos personales, como lo indicó la Unión Europea: “El principio de transparencia es particularmente importante en el campo de la protección de datos. Las operaciones de procesamiento no se realizan en público ni se sienten sus resultados inmediatamente por los individuos interesados, para que en consecuencia respondan. Por el contrario, el procesamiento de datos personales tiene lugar a puertas cerradas o más bien dentro de sistemas automatizados, sin las personas cuyos datos se están procesado que está presente o incluso consciente de que tal procesamiento se lleva a cabo. El conocimiento generado sobre un individuo a menudo no es accesible para él, ni ninguna información sobre cómo se produjo. Además, los resultados de dicho procesamiento en la mayoría de los casos no conducen a una acción directa positiva o negativa hacia las personas afectadas, sino que se almacenan en sistemas informáticos para su uso futuro.” [5]. Finalmente, esto gira en torno a la transparencia con la cual se deben tratar los datos

personales por parte del encargado del sistema, la facilidad para el acceso a la información y el lenguaje claro que los datos deben conservar durante el proceso.

Europa es un continente con un alto grado de evolución sobre el tratamiento de datos personales, pero al compararlo con Colombia surge una pregunta ¿está preparado el país o tiene el nivel adecuado de cara a la Unión Europea?, primero hay que entender que se cuenta con una serie de ventajas cuando se cuenta con ese nivel adecuado:

- Aumenta el grado de protección jurídica, porque el modelo europeo es prenda de garantía.
- Generación de escenarios más competitivos en los negocios.
- Es un elemento esencial en las sociedades.

Para responder la pregunta es necesario también entender que significa tener un nivel adecuado según la Unión Europea “un nivel de protección adecuado depende de varios factores, unos de naturaleza regulatoria y otros de carácter instrumental e institucional (requisitos de procedimiento y de aplicación). El primer grosso modo es fruto de la mezcla de derechos en cabeza del titular de los datos y de obligaciones para quienes procesan la información personal o ejercen control sobre ese tratamiento. El segundo comprende, de una parte, la existencia de mecanismos y procedimientos tanto judiciales como no judiciales que garanticen la efectividad de las normas, sancionen su incumplimiento y otorguen a la persona afectada un derecho de reparación frente al tratamiento indebido de su información” [6]

En cuanto a la pregunta propuesta, la respuesta se podría enfocar haciendo énfasis puntualmente sobre la ley 1266 de 2008 que contiene la mayoría de aspectos mínimos como lo son los principios del tratamiento de información, se concluye que no cuenta con los niveles adecuados de protección “porque la ley 1266 de 2008 presenta serias limitaciones y falencias frente a las exigencias del modelo europeo” [6], pues esta ley no regula los datos sensibles que es otro punto a tener en cuenta, tampoco es genérica sino se enfoca principalmente a temas financieros. Pero si se observa en la actualidad podremos ver que a la fecha ya existe una ley genérica de protección de datos, la ley estatutaria 1581 de 2012, donde regula los aspectos a los cuales no llegaba la ley 1266 y desde el punto de vista si cumple con las condiciones mínimas que exige la unión europea.

ESTRATEGIA METODOLÓGICA

Se propone como metodología para el llevar a cabo los objetivos planteados en este documento los siguientes:

- **Investigación**: Se realizará la respectiva investigación y entendimiento de la normatividad nacional relacionada con la protección de datos personales (1581 de 2012, el decreto 1377 de 2013 y la ley 1266 de 2008).

- **Planteamiento de la guía para tratamiento de datos personales con enfoque seguro**: Se planteará la respectiva guía metodológica orientada a la protección de datos personales para empresas distribuidoras de tecnología.

- **Planteamiento de guía de buenas prácticas- controles**: en esta fase se realiza el planteamiento de una serie de controles/buenas practicas a nivel de seguridad para dar tratamiento a los posibles riesgos asociados que pueden presentarse durante el tratamiento de datos personales en las empresas distribuidoras de tecnología.

- **Aplicación de la guía metodológica diseñada**: se aplicará la guía metodológica a una empresa del sector seleccionado con el fin de identificar la eficacia de la guía elaborada, a esta empresa se tiene acceso a determinada información que es importante para el estudio, pero por temas de acuerdos de confidencialidad no es posible dar a conocer su nombre o razón social y algunos datos que corresponde a información sensible. Se tendrán en cuenta todos los materiales elaborados para el trabajo y de esta manera se evaluará el cumplimiento de las normas existente para la protección de datos personales.

- **Entrega y sustentación de los resultados**: consiste en la entrega de la documentación elaborada y la respectiva sustentación frente a los jurados.

DESARROLLO E IMPLEMENTACIÓN

Dando desarrollo a la metodología planteada con anterioridad a continuación, se explican los avances de cada una de las fases:

Investigación

En esta fase se llevó a cabo la respectiva investigación sobre la normatividad nacional para el tratamiento de datos personales (ley 1581 de 2012, el decreto 1377 de 2013 y la ley 1266 de 2008) en pro de adquirir los conocimientos necesarios para plasmar una guía

metodológica para el tratamiento de datos personales lo más aterrizada posible y escoger los puntos importantes y fundamentales y de esta forma complementarla con una guía de buenas prácticas/controles que permitan definir controles para la protección de los datos de una manera segura en las compañías distribuidoras de tecnología. La información fuente de investigación se consultó a través de internet, ya que la misma es pública y está disponible en diferentes sitios web como la alcaldía de Bogota y Mintic. Esta investigación permitió identificar que existe en la actualidad una problemática importante a nivel de protección de datos personales la cual debe ser abordada desde este momento debido a que cada día los sistemas como Big Data están ingresando a pasos agigantados al país y si no se toma una medida para protección los datos pueden ser robados de una manera sencilla por atacantes cibernéticos.

Planteamiento de la guía para tratamiento de datos personales con enfoque seguro

La finalidad de la metodología propuesta es definir los requerimientos que se deben tener en cuenta para el cumplimento de la normativa existente en Colombia de protección de datos personales para las compañías distribuidoras de tecnología teniendo en cuenta la ley 1581 de 2012, el decreto 1377 de 2013 y la ley 1266 de 2008 donde se incluye temas de Habeas Data.

1. **Contexto:**

   La metodología que se propone para el cumplimiento de la protección de datos personales se encuentra dirigida a compañías distribuidoras de tecnología las cuales tengan como fin la comercialización de equipos y servicios tecnológicos a terceros ya sean compañías o clientes finales. En algunos casos estas compañías administran los equipos en caso que no tengan el personal adecuado.

2. **Normas utilizadas:**

- *Ley 1581 de 2012: Ley estatutaria del 17 de octubre de 2012 por el cual se dictan disposiciones generales para la protección de datos personales.*
- *Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la ley 1581 de 2012.*

- *Ley 1266 de 2008: Ley estatutaria del 31 de diciembre de 2008 por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de información contenidas en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.*

3. Metodología:

Para proteger los datos personales suministrados a las compañías distribuidoras de tecnología se establece como guía los siguientes pasos:

I. Establecer los procesos de la compañía que reciben o manejan datos de carácter personal de la empresa o de terceros con el fin de enfocar la metodología en lo estrictamente importante, los procesos que se recomiendan son:

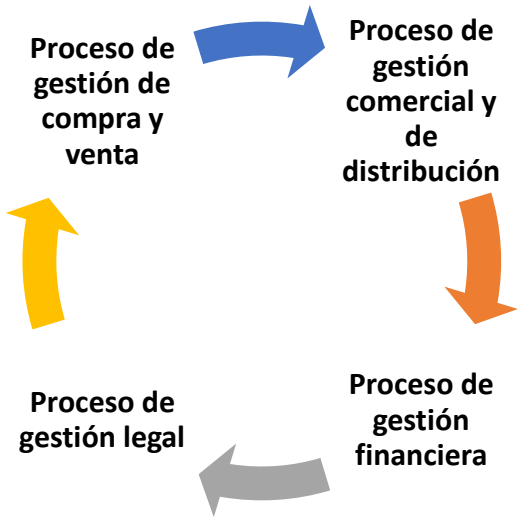

Figura 1.Procesos recomendados para las compañías distribuidoras de tecnología.

II. Después de establecidos los procesos se identificarán las clases de datos que maneja cada proceso, según las leyes que anteriormente se mencionaron se clasifican en:

- **"Dato público:** son datos públicos los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas." [15]

- **“Dato semiprivado:** el dato que no tiene naturaleza intima, reservada, ni publica y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas o la sociedad en general, como el dato financiero y creditico de actividad comercial o servicios.” [15]
- **“Dato privado o sensible:** por su naturaleza intima o reservada solo es relevante para el titular, estos en su divulgación pueden afectar la intimidad del titular o cuyo uso indebido puede generar su discriminación. “ [15]

Para la metodología que se está realizando los datos que se van a tener en cuenta son los **Datos privados** debido a que estos son considerados sensibles y que atentan directamente a la persona implicada.

III. Cuando ya se tenga clasificada la información según los parámetros anteriores, es necesario realizar una identificación de riesgos asociados a los datos privados y sensibles de la organización para, para ello se debe tener en cuenta la siguiente tabla:

TIPO DE RIESGO	CARACTERISTICAS
Datos con riesgos bajo	Esta categoría considera información general tales como: - datos de identificación - contacto - información académica - información laboral - nombre - teléfono - edad - sexo - estado civil - dirección de correo electrónico - lugar y fecha de nacimiento - nacionalidad - puesto de trabajo y lugar de trabajo - idioma o lengua - escolaridad - cédula profesional - información migratoria

Datos con riesgos medios	Contempla los datos que permiten conocer: **La ubicación física de la persona** - la dirección física - información relativa al tránsito de las personas dentro y fuera del país - cualquier otro que permita volver identificable a una persona a través de los datos que proporcione alguien más. Por ejemplo: dependientes, beneficiarios, familiares, referencias laborales, referencias personales, etc. **Inferir el patrimonio de una persona** - los saldos bancarios - estados y/o número de cuenta - cuentas de inversión - bienes muebles e inmuebles - información fiscal - historial crediticio - ingresos - egresos - buró de crédito - seguros - afores - fianzas - sueldos y salarios - servicios contratados, incluye el número de tarjeta bancaria de crédito y/o débito. **datos de autenticación** - usuarios - contraseñas - información biométrica (huellas dactilares, iris, voz, entre otros) - firma autógrafa y electrónica - fotografías - identificaciones oficiales, inclusive escaneadas o fotocopiada **datos jurídicos** - antecedentes penales - amparos - demandas - contratos - litigios - cualquier otro tipo de información relativa a una persona que se encuentre bajo procedimiento administrativo como juicio o jurisdiccional en materia laboral, civil, penal o administrativa
Datos con riesgos altos	**datos personales sensibles**: que de acuerdo a la Ley incluyen: - datos de salud, los cuales se refieren a la información médica donde se documente el estado de salud física y mental, pasado presente o futuro

	- información genética; origen racial o étnico, ideología, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular.
Datos con riesgos mayores	Los datos de mayor riesgo son los que de acuerdo a su naturaleza derivan en mayor beneficio para un atacante, por ejemplo: - Información adicional de tarjeta bancaria que considera el número de la tarjeta de crédito y/o débito - fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal (PIN) de las tarjetas de crédito o débito. - Información de cuentas bancarias, extractos, estados financieros de las empresas, entre otros.

Tabla 1.Riesgos asociados a los datos.

Para la metodología que se está trabajando, se toma consideración en tomar acciones para los riesgos considerados como altos y mayores, debido a que son riesgos que puede afectar tanto al titular dueño de la información y a la empresa que la recolecta, es importante enfocar esfuerzos en mitigarlos y ofrecer una respuesta oportuna en caso que se llegara a materializar alguno. Adicional se deja en consideración que algunos de los riesgos considerados como medios sean tenidos en cuenta debido a que se trata de información que comúnmente se utiliza y que en caso que un atacante los robara también implicaría multas y desprestigio para el titular de la información o para la empresa recolectora.

IV. Ya obtenida la información de los puntos anteriores, es necesario definir los controles de seguridad que permitan ayudar a mitigar los riesgos encontrados, en cuanto a la alineación con la seguridad en los procesos de sistemas de información, la idea es que para dichos procesos ya establecidos no solo se busque garantizar la disponibilidad, integridad y confidencialidad de la información sino que se le dé importancia a la privacidad (derechos que tienen los titulares de los datos personales y los deberes que tienen las entidades en este caso distribuidoras de tecnología de proteger la información

entregada por los titulares), esto último con el fin de garantizar los derechos de intimidad y buen nombre.

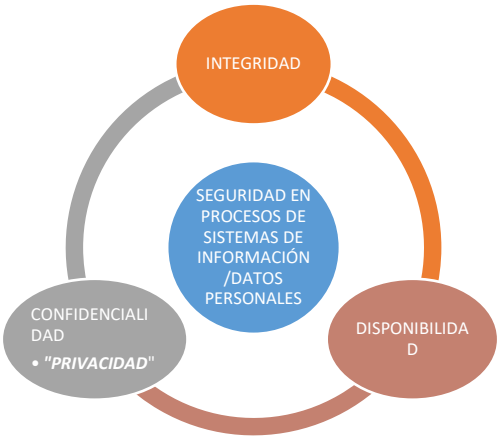

Figura 2. Seguridad en procesos de sistemas de información.

Es necesario como los demás aspectos de seguridad de la información brindarle un enfoque de riesgos e incluir lo relacionado con el tratamiento de datos personales en la metodología utilizada por la compañía para la gestión de riesgos de seguridad de la información, bien sea una metodología del tipo ISO 27005, MAGERIT, NIST 800-30 o una metodología personalizada. Lo ideal es darle un planteamiento que permita identificar y tratar riesgos que lleguen a comprometer la seguridad de los datos personales en torno a su confidencialidad, disponibilidad, integridad y privacidad en el tratamiento de los mismos.

Como control importante es necesario la creación de una **política de tratamiento de datos** la cual deje expresamente claro que información debe ser recolectada de los clientes que se están trabajando y su finalidad, esta política debe ser cumplida por todo el personal que maneja este tipo de información y clasificarla como se indicó anteriormente; se debe divulgar a todos los clientes para que se tenga claridad y en el momento puedan dar el aval o no de si sus datos puede ser tratada como la empresa lo expresa.

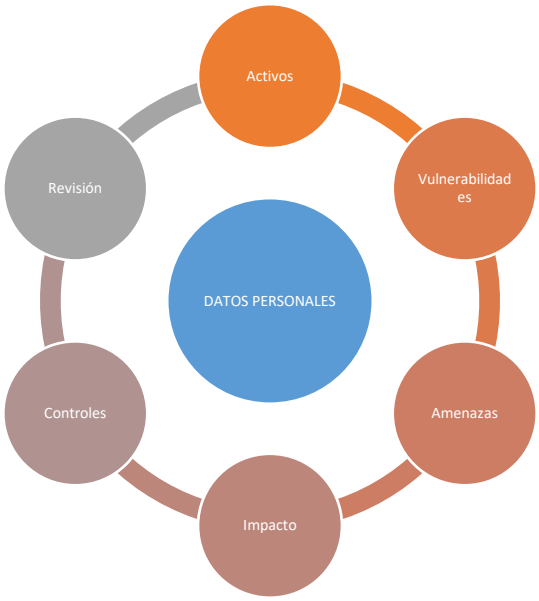

Figura 3.Gestión de riesgos en el tratamiento de datos personales.

Adicional para los controles también se entrega una guía de buenas prácticas, en donde se pueden tomar aquellos que se consideren pertinentes de los indicados para el tratamiento de los riesgos encontrados, la compañía podrá optar por aplicar otros controles que no estén incluidos en dicha guía si así lo considera. La implementación de los controles no se aborda en esta metodología ya que quedará sujeta a los recursos con los cuales cuente lo compañía (recurso humano, tiempo, dinero).

V. Posteriormente se deben fortalecer las responsabilidades del manejo y tratamiento de la información recolectada, para ello es necesario conocer según la ley los deberes de los responsables y asignar una persona que se encargara que velar porque se cumplan.

Con el fin de dar cumplimiento a los deberes anteriormente mencionados es necesario asignar un responsable, para eso es necesario los siguientes datos:

Datos de identificación del responsable del tratamiento

- Nombre
- Dirección
- PBX y FAX
- Línea Gratuita de atención al cliente
- Correo
- Portal Web

VI. Adicional a lo anteriormente mencionado se debe establecer un aviso de privacidad en el cual a las personas que están entregando sus datos tengan claro el objeto por el cual se está recolectando esta información, los datos principales para este aviso es:

- Nombre o razón social y datos del responsable del tratamiento de los datos
- El tratamiento al cual serán sometidos la información suministrada y su finalidad
- Los derechos del titular de la información
- Los mecanismos dispuestos por la entidad para que el titular conozca la Política para el Tratamiento de Datos Personales y los cambios sustanciales que se produzcan en ella o en el Aviso de Privacidad.
- Información sobre consulta y acceso a la Política para el Tratamiento de Datos Personales.

VII. Las finalidades de la recolección de información en las compañías distribuidoras de tecnología pueden ser:

- Para los fines administrativos propios de la entidad.

- Caracterizar canales y usuarios finales para adelantar estrategias de mejoramiento en la prestación del servicio.
- Dar tratamiento y respuesta a las peticiones, quejas, reclamos, denuncias, sugerencias y/o felicitaciones presentados a la entidad.
- Alimentar el Sistema de Información.
- Adelantar encuestas de satisfacción de usuarios.
- Envío de información de interés general.
- Recopilar información de ciudadanos asistentes a capacitación desarrolladas por la entidad.

NOTA: La recolección de los datos personales son para el desarrollo de las funciones propias de la entidad. Cualquier otro tipo de finalidad que se pretenda dar, deberá ser informado previamente en el aviso de privacidad y en la respectiva autorización otorgada por el titular del dato, y siempre teniendo en cuenta los principios rectores para el tratamiento de los datos personales, establecidos por la Ley.

VIII. Como titular de los datos, los clientes tienen derechos sobre la información que fue suministrada a las compañías las cuales son:

- "Conocer, actualizar y rectificar sus datos personales. Este derecho se podrá ejercer también, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- Solicitar prueba de la autorización otorgada a la entidad a la cual fue suministrada la información para el tratamiento de sus datos personales.
- Ser informado del uso y tratamiento dado a sus datos personales, previa solicitud elevada a través de los canales de servicio.

- Revocar la autorización y/o solicitar la supresión de uno a más datos cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.” [13]

IX. Las compañías distribuidoras de tecnología deben realizar un formato de autorización que debe ir firmado por el titular de la información y adjunto en el momento del envío de los datos, **básicamente debería llevar**:

- Realizar un formato propio para cada empresa con el logo.
- Nombrar las normas aplicables que en este caso es la ley 1581 de 2012, la ley 1266 de 2008 y el decreto 1377 de 2013 y su objeto.
- Realizar un texto donde se autoriza el uso de la información suministrada indicando la finalidad y el tratamiento que tendrá.
- Debe estar resaltado las palabras Autorizo, explícitamente, inequívoca e informada que la información enviada hará parte de la base de datos de la compañía.
- Deben estar indicados los derechos del titular de la información.
- Debe indicar la fecha en la que fue firmada la autorización.
- Debe ir firmada por el titular y el responsable del tratamiento.

X. Después de solicitar esta autorización el responsable del tratamiento debe **eliminar los datos de los clientes** que no enviaron dicho formato diligenciado e informar que fueron eliminados y los que no son requeridos para la finalidad de la empresa.

XI. Se deben establecer canales de atención a los clientes en donde puedan pedir requerimientos respecto a los datos que suministraron tales como:

- “Consultas: Los titulares o representantes podrán consultar la información personal del titular que repose en cualquier base de datos lo que quiere decir que las compañías distribuidoras de tecnología son responsables del

tratamiento, suministrará a éstos, toda la información contenida en el registro individual o que esté vinculada con la identificación del titular.” [13]

- “Reclamos: Los titulares que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley y demás normas que la desarrollan, podrán presentar un reclamo con la siguiente información:
  - Identificación del titular del dato.
  - Descripción precisa de los hechos que dan lugar al reclamo.
  - Datos de notificación, dirección física y/o electrónica.
  - Los demás documentos que se quiera hacer valer.” [13]
- Acceso a los datos: se debe garantizar el derecho de acceso a los datos personales, una vez se haya verificado la identidad del titular y/o representante poniendo a disposición de éste, los respectivos datos personales.
- Actualización y rectificación de datos: como responsable del tratamiento de los datos, las compañías distribuidoras de tecnología deberán rectificar y actualizar a solicitud del titular toda información que de éste resulte ser incompleta o inexacta. Para estos efectos, el titular señalará las actualizaciones y rectificaciones a que dieran lugar, junto a la documentación que soporte su solicitud.
- Eliminación de datos: Los Titulares podrán en todo momento y cuando consideren que los datos no están recibiendo un tratamiento adecuado o los mismos no son pertinentes para la finalidad para la cual fueron recolectados mediante el envío de un reclamo.

Para este tipo de requerimientos es necesario registrar canales de atención en donde los titulares puedan instaurar la petición del tipo que se vio anteriormente, para ello mínimo debe tener.

Canales de servicio:

- Escrito:
  - Dirección física
  - Correo electrónico de servicio al cliente
  - Formulario PQR que debe estar en la página web de la compañía
- Presencial
  - Dirección de la compañía
- Telefónico
  - Conmutador de la compañía
  - Línea gratuita nacional
- Virtual
  - Redes sociales
  - Chat general ubicado en la página web

Cualesquiera de los canales de comunicación anteriormente mencionados pueden ser utilizados por los titulares para imponer cualquier requerimiento y son legalmente constituidos.

Planteamiento de guía de buenas prácticas- controles

De acuerdo a lo estipulado en la página web de la superintendencia de industria y comercio (http://www.sic.gov.co/preguntas-frecuentes-rnbd), para el registro nacional de bases de datos se deben registrar bases de datos que se encuentren en **medios físicos** como el papel igualmente en **medios electrónicos** (archivos, listas, bases de datos, entre otros);

esto permite plantear una serie de controles de seguridad que de acuerdo a los resultado del análisis de riesgos realizado a la compañía según competa se tendrá en cuenta o no su aplicación en pro de dar cumplimiento a lo establecido en los artículos **17 y 18 de la ley 1581 de 2012.**

Artículo 17, sobre los deberes del responsable del tratamiento. Apartado D)" Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento" [16]

Artículo 18, sobre los deberes del encargado del tratamiento. Apartado B) "Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento" [16]

Dando cumplimiento a dichos requerimientos normativos y en busca de preservar la integridad, disponibilidad y confidencialidad de los datos personales tratados por las compañías distribuidoras de tecnología, se plantea la siguiente plantilla con los principales aspectos a tener en cuenta como controles y/o buenas prácticas durante el transcurso del tratamiento de datos, en la metodología planteada se hace referencia en el **punto IV** que esta guía puede servir para seleccionar algunos controles y también queda en indisposición de la organización poder definir otros controles según considere:

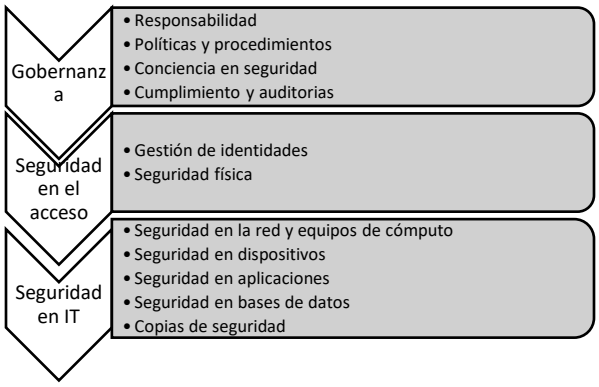

Figura 4. Buenas prácticas en seguridad de datos personales. Diseño propio

En cuanto a la gobernanza, se considera un punto clave en la seguridad de la información y más cuando se habla de protección de datos personales, en donde es necesario que desde la alta dirección se brinde el respectivo apoyo para llevar a cabo el tratamiento de la información de una manera adecuada con las respectivas condiciones de seguridad, por tanto, se plantea considerar:

- La **responsabilidad** que debe mostrar la alta dirección con el apoyo activo e interés marcado, enfocado a la protección de la información y jugando el papel de integradora, debido a que en este tema no solo le compete al área de IT sino debe ser un componente transversal al negocio.

- Es importante la existencia de **políticas y procedimientos documentados** en pro de la protección de datos personales principalmente para el área de IT pero sin limitarse a esta última, ya que los datos personales no siempre se encuentran en medios digitales sino también se pueden encontrar en medios físicos. Además es conveniente establecer una política de usuario final en donde se recalque el debido uso de las aplicaciones de la compañía que procesen datos personales. Por último y no menos importante se encuentra las revisiones periódicas que se deben realizar a las políticas y procedimientos para validar que los mismos se encuentren acorde a los requerimientos actuales de la compañía.

- Como los demás aspectos de seguridad de la información no es ajeno al tratamiento seguro de datos personales que se lleve a cabo el respectivo **entrenamiento a nivel de seguridad** en donde se tenga en cuenta:

- Que se incluya todo el personal de la compañía, empleados, contratistas, colaboradores.
- El entrenamiento deberá ir enfocado a **crear conciencia** en el personal, dando a conocer la **importancia de las prácticas de seguridad en el tratamiento de datos personales**, además sus responsabilidades y la importancia de evitar todo tipo de prácticas que vayan en contra de sus obligaciones en cuanto a la privacidad de la información.
- La capacitación debe ser actualizada a la realidad de la compañía y debe darse regularmente a los empleados, contratistas y colaboradores con una periodicidad acordada con la alta gerencia.
- Es conveniente recalcar el correcto uso en el día a día como usuarios finales de las aplicaciones y/o documentos cuyo contenido sean datos personales.

- En cuanto a las **auditorias,** son de gran importancia en el tratamiento de datos personales de manera segura, ya que permiten conocer **el cumplimiento de las medidas de seguridad** establecidas. Se recomienda abordar:
  - Revisión de logs de los diferentes sistemas en donde permitan evidenciar posibles accesos sin autorización a los datos contenidos en aplicaciones, bases de datos u archivos, además del seguimiento a las bitácoras en donde se observe el movimiento de información en físico si el caso lo amerita
  - Realización de pruebas de vulnerabilidades a nivel técnico, de las cuales en caso de encontrarse la existencia de las mismas es recomendable se apliquen las respectivas remediaciones sobre los activo objeto del estudio
  - Revisión del cumplimiento de políticas y procedimientos según lo establecido por la compañía, tomar acciones correctivas si compete

- Un componente primordial cuando se realiza tratamiento de datos por medio electrónico de forma segura es la **gestión de identidades** en donde se aconseja abordar temas como:
    - Autenticación con múltiple factor sobre sistemas o plataformas que se involucren con el tratamiento de los datos personales.
    - Establecer el número de intentos fallidos de autenticación en los sistemas antes del bloqueo de la cuenta.
    - Transmisión y almacenamiento seguro de claves por medio de hash/cifrado.
    - Políticas de contraseñas donde se incluya longitud mínima, la no repetición de claves anteriores, contemplando complejidad de las mismas.
    - Entrenamiento hacia los empleados, contratistas y colaboradores sobre la relevancia de usar claves fuertes.
    - Buscar la eliminación de usuarios genéricos o compartidos
    - Definición de política de control de acceso y de roles, con los respectivos permisos según competa sobre los datos personales, bien sea para información física o electrónica.
    - Realizar depuración de cuentas y permisos en los sistemas de información
    - Almacenar logs sobre los accesos e intentos realizados a los sistemas de información con contenido o manipulación de datos personales

- Un aspecto de seguridad olvidado por muchas compañías es la **seguridad física**, cuando se habla de datos personales no es ajeno a ello, por tanto se recomienda abordar:
    - Medidas de control de acceso a los sitios considerados como críticos por la información personal tratada en los mismos.
    - Segregación física entre dependencia de la compañía.

- Privacidad y seguridad tanto entre dependencias como en los puestos de trabajo de los empleados.
- Existencia de política de escritorio limpio.
- Existencia de medidas de protección de información con datos personales en físico ubicados en archivo, RRHH y otra área de la compañía.
- Existencia de política para el control de visitantes a la compañía.

- La seguridad a nivel de los **equipos de cómputo y de redes** se debe tener en cuenta cuando se habla de protección de datos personales, por tanto se considera importante:
  - Tener segregación a nivel de red.
  - Hacer uso de modelo de capas en la red.
  - Realizar zonificación a nivel de firewall.
  - Realizar hardening sobre los servidores.
  - Uso de protocolo seguros para transmisión de datos personales.
  - Monitorear la red para detectar intentos de acceso sin autorización.
  - Disponer de filtrado de contenido e IPS (sistema de prevención de intrusos) en la red.
  - Contemplar el uso de Data Leak Prevention sobre la red, como control de fuga de información.
  - Contemplar el uso de cifrado a nivel de disco sobre los equipos de cómputo.
  - Uso obligatorio de software antimalware en los equipos de cómputo.
  - Protección a nivel de correo con antispam.
  - Disponer de un sistema de copias de seguridad sobre servidores e información de usuario final.
  - Uso de políticas de dominio para controlar los permisos a nivel de usuario final.

- Existencia y divulgación de política de seguridad relacionada con el uso de la red en general.

- El uso de diferentes **dispositivos** como medios de almacenamiento extraíble, impresoras multifuncionales y fax deben ser supervisados meticulosamente cuando se pretenda asegurar el tratamiento de datos dentro de la compañía. Se recomienda:
  - Minimizar al máximo el uso de medios de almacenamiento extraíble principalmente en áreas identificadas como críticas para el tratamiento de datos personales.
  - Reglamentar el uso y acceso de medios de almacenamiento extraíbles en la compañía, dispositivos de impresión, escáner, impresoras, celulares con cámara y fax.
  - Evaluar la opción de implementar desactivación de puertos físicos en los equipos de cómputo para evitar conexión de dispositivos extraíbles.
  - Tener presente la existencia del procedimiento de destrucción de información tanto lógica como física, el cual debe estar enmarcado en el ciclo de vida de la información definido por la compañía.
  - Contar con procedimientos a nivel de IT para borrado seguro de información en dispositivos de almacenamiento.
- Cuando se habla de protección de datos a nivel de **aplicación** se puede abordar desde el enfoque de aplicaciones de escritorio y aplicaciones web, a continuación un listado de buenas prácticas en pro de la protección de datos personales:

  Para **aplicaciones de escritorio**:

- Usar software preferiblemente con las últimas versiones previamente validadas considerando que dicha versión no llegue a tener componentes intrusivos con la privacidad de los datos.
- Remover aplicaciones y desactivar características de sistema operativo que no se usen en los equipos de usuario y servidores.
- Mantener actualizados los navegadores web.
- Evitar abrir correos con adjuntos sin antes ser inspeccionados por un antivirus o un antispam.
- Existencia de política de antivirus y uso de aplicaciones, dándola a conocer a los empleados, contratistas y colaboradores que hagan uso de recursos de cómputo.

Para **aplicaciones web** se debe hacer énfasis principalmente a los desarrollos propios:

- Realizar validaciones en formularios de entrada de datos de usuario.
- Realizar escaneo de vulnerabilidades siguiendo guías como las de OWASP.
- Hacer uso de protocolos seguros en la transferencia de información personal entre cliente y servidor.
- Evitar el listado/publicación de archivos con datos personales en servidores web.
- No permitir que se usen datos personales de un ambiente de desarrollo en otro, principalmente de producción a pruebas.
- Realizar correcta validación de cookies/sesiones frente a la URL del sitio publicado.

- Quizás el punto más crítico a la hora de hablar de aseguramiento en el tratamiento de datos personales son las **bases de datos**, ya que son los espacios donde se almacena de manera estructurada la información, ya una vez obtenido el acceso a

la misma la privacidad de dicha información queda en las manos de quien tenga el acceso, por tanto se plantean las siguientes prácticas que conducirán a darle un manejo adecuado a la protección de los datos personales contenidos en dichas bases:

- Utilizar cifrado de los datos bien sea parcial de solo la data más sensible o todos los datos en general que se almacenen en la base de datos.
- No es conveniente que las bases de datos estén expuestas en servidores publicados directamente a internet.
- Realizar copias de seguridad periódicamente a las bases de datos, estableciendo los respectivos procedimientos para ello.
- Realizar validación de logs para determinar posibles intentos de acceso sin autorización a la información.
- Establecer roles y privilegios para quienes tengan acceso a la gestión de la base de datos.
- cuando se habla de información o planillas en físico que no son propiamente bases de datos sino listas que contienen datos personales se debe tener establecido los procedimientos para su manipulación y control de cambios sobre los mismos.
- Si es posible implementar alta redundancia.
- Contar con un adecuado plan de contingencia.

- Como contingencia en caso de ocurrencia de incidentes de seguridad, en donde se llegue a ver comprometido los datos personales contenidos en bases de datos, archivos de usuario, aplicaciones son las **copias de seguridad**, llevar una gestión eficiente es lo más conveniente, por tanto se plantea:

  - Contar con una política de copias de seguridad y retención.

- Validar que la información a respaldar sea la indicada.
- Verificar periódicamente que los datos contenidos en las copias de seguridad sean recuperables en caso de emergencia.
- Contar con los respectivos procedimientos para garantizar el correcto uso y protección de las copias de seguridad.
- En caso de manejar listas de datos en físico es conveniente también contar con las respectivas copias mantenidas en un lugar seguridad y bajo el
- control del personal competente.

Aplicación de la guía metodológica diseñada

A continuación, se plantea el desarrollo de la metodología propuesta, para ello se tomó como referencia una de las compañías distribuidoras de tecnología que se encuentran en Colombia y la cual accedió a brindar cierta información mediante firma de acuerdo de confidencialidad no se puede entregar información ni divulgar el nombre de la empresa según los eventos encontrados.

La compañía distribuidora de Colombia hace parte de una multinacional que tiene presencia a nivel de norte américa y Latinoamérica, en Colombia tiene su centro de operación en la ciudad de Bogotá, desde donde se prestan los servicios de distribución de soluciones tecnológicas a nivel de telecomunicaciones, distribuyendo productos y servicios de diferentes fabricantes especializados en seguridad del mercado.

1. **Procesos que manejan datos de carácter personal**

La empresa en estudio tiene estipulado los procesos de acuerdo con el nicho del negocio al que pertenecen, sus áreas más críticas con Comercial y Operaciones esto debido a que toda su labor está enfocada en la venta y entrega de soluciones. Adicional está el área de finanzas la cual es la encargada de la revisión de métricas del negocio en cuanto a margen

de ventas y maneja información altamente importante para la organización.Dentro de los procesos que realizaremos el estudio están:

- **Gestión de Alianzas**: Proceso encargado de la creación de los clientes (entiéndase por cliente canal y fabricante) que se construirá un nivel de confianza dentro de la compañía.
- **Gestión de compras y pedidos**: Proceso encargado de la realización de la compra ya sea a los clientes (entiéndase por cliente canal y fabricante), realización de facturación y procesos de entrega.
- **Gestión de proyectos**: Proceso encargado de dirigir proyectos elaborados directamente por el distribuidor a sus clientes.

2. Datos privados que manejan cada proceso

Los datos personales como cualquier dato se encuentran relacionados con algunos activos ya que los mismos no se encuentran y no tienen sentido por si solos para la compañía, a continuación se mencionan los activos objeto de estudio:

- **Gestión de Alianzas:**
    - Base de datos de los canales que pueden distribuir las soluciones y los productos de la organización.
    - Base de datos de los fabricantes que distribuye la empresa.
- **Gestión de compras y pedidos**:
    - Órdenes de compra de los canales con los datos del cliente final.
    - Órdenes de compra generadas del distribuidor al fabricante
    - Facturas realizadas al canal respecto a la orden de compra enviada
- **Gestión de proyectos**
    - Contratos y soportes de proyectos que se ejecutaron y los que se ejecutaran.

3. Clasificación de los riesgos asociados a los datos privados

ÍTEM	ACTIVO	DATOS PERSONALES CONTENIDOS	VULNERABILIDADES	AMENAZAS	RIESGO	IMPACTO	TRATAMIENTO
1	Base de datos de clientes (digital)	-Datos con riesgos Medios -Datos con riesgos Altos	Se puede ver afectada por el mal uso de parte de las personas en cuanto a la información contenida en la base de datos. Permite conexiones múltiples con un mismo usuario, es una característica de muchos motores de bases de datos	Manejo indebido de la información proporcionada por los clientes. Acceso no autorizado a la información Robo y divulgación de la información a terceros.	Económico debido a que los clientes al identificar que la información no está bien protegida no vuelven a comprar, además de multas establecidas por la ley. Reputacional debido a que no hay confianza en el intercambio de información sensible.	ALTO	**Plan de tratamiento 1**
2	Base de datos de fabricante (digital)	-Datos con riesgos Medios -Datos con riesgos Altos	Se puede ver afectada por el mal uso de parte de las personas en cuanto a la información contenida en la base de datos. Permite conexiones múltiples con un mismo usuario, es una característica de muchos motores de bases de datos .	Manejo indebido de la información proporcionada por los clientes. Acceso no autorizado a la información Robo y divulgación de la información a terceros.	Económico debido a que los fabricantes eliminan su relación con el distribuidor y puede llegar a quitar su fábrica del portafolio. Reputacional debido a que no hay confianza en el intercambio de información sensible.	ALTO	

3	facturas (físico-digital)	-Datos con riesgos Medios -Datos con riesgos Altos.	Dependen del uso que le den las personas lo que las hace susceptible al mal uso de los datos contenidos en las mismas.	Adulteración de los datos contenidos en la factura tanto de las empresas como de los precios contenidos en ella. Falsificación de la información con el fin de generar daño al cliente.	Económico debido a que al adulterar datos de la factura puede cambiar precios y afectar el flujo de la empresa, además de multas establecidas por las leyes aplicables. Reputacional debido que al no tener confianza los clientes no vuelven a comprar y el negocio empieza a decrecer.	ALTO	**Plan de tratamiento 2**
4	órdenes de compra clientes (físico-digital)	-Datos con riesgos Medios -Datos con riesgos Altos.	Las personas le pueden dar una incorrecta manipulación a la información contenida en las mismas.	Falsificación de la orden de compra con fines dañinos para la empresa o cliente. Robo de información por parte de los	Económico debido a que al no coincidir la información se puede adquirir productos o servicios que en realidad no fueron adquiridos.	ALTO	

				empleados o terceros como competencia. Información no valida sobre la orden de compra que se emite al cliente.	Reputacional debido a que al mal uso de la información puede caer en manos de la competencia y además de perder el negocio se pierde el cliente.		
5	Órdenes de compra fabricas(fisico-digital)	-Datos con riesgos Medios -Datos con riesgos Altos.	Mal uso de la información contenida en la orden de compra con fines dañinos.	Falsificación de la orden de compra con fines dañinos para la empresa o fabricante. Robo de información por parte de los empleados o terceros como competencia.	Económico debido a que al no coincidir la información se puede adquirir productos o servicios que en realidad no fueron adquiridos. Adicional el fabricante no apoyaría al crecimiento del distribuidor y bajaría sus ventas de manera considerable	ALTO	
6	contratos y soportes de proyectos (digital)	-Datos con riesgos Medios -Datos con riesgos Altos.	Susceptible al acceso no autorizado a la información contenida de contratos y soportes de los proyectos que se estén realizando en el momento y los pasados. Se pueden ver afectados por el uso no adecuado de la información contenida en los contratos ejecutados y por ejecutar.	Robo de información contenida en los contratos y soportes de los proyectos por personal interno de la organización o por terceros que obtienen acceso no autorizado a estos documentos. Divulgación de los negocios que se están ejecutando o por ejecutar a la competencia por	Económico debido a que se efectuaran multas establecidas por la ley por divulgación de información sensible. Reputacional debido que en el mercado no está bien visto que una empresa divulgue información confidencial de sus negocios.	ALTO	**Plan de tratamiento 3**

			Uso de la información para fines que no estén consultados previamente con el dueño de los datos.	desconocimiento de los empleados. Tratamiento no adecuado de la información según las leyes establecidas.			

Tabla 2. Riesgos identificados

4. Definición de los controles de seguridad

Según los riesgos identificados en el ítem anterior se plantean los siguientes planes de tratamiento que permitirán dar un mejor a nivel de seguridad de la información a los datos personales contenidos en dichos activos, para ello se usó de la guía de buenas prácticas.

Plan de tratamiento 1

Contexto

Actualmente la compañía está permitiendo el uso de usuarios genéricos, donde solo existe un usuario diferente al administrador con el cual se hacen diferentes acciones sobre las bases de datos de clientes y de la base de datos de fabricantes, en donde las credenciales de acceso son compartidas por los empleados del proceso de gestión de alianzas, esto se realizó por practicidad en la operación pero no se tuvo en cuenta la brecha de seguridad que se genera con ello, actualmente no hay trazabilidad sobre las acciones realizadas por cada usuario en las bases de datos, adicional se puede presentar que las credenciales caigan en manos de personas no autorizadas y se extraiga o se elimine datos personales; lo que puede llevar a que se materialicen los riesgos mencionados en la tabla de riesgos.

Plan sugerido

Lo ideal es generar un usuario para cada uno de los empleados del proceso de Gestión de Alianza que debe tener acceso a cada una de las bases datos (clientes y fabricantes), para ello se sugiere el siguiente plan que gira entorno a la **no presencia de usuarios genéricos** en dichas bases de bases de datos.

ÍTEM	ACCIÓN	TIEMPO ESTIMADO PARA EJECUTAR	RESPONSABLE
1	Realizar levantamiento de información de las personas que deben tener acceso a las bases de datos en cuestión y definir los privilegios que deben tener	8 días	coordinador del proceso de gestión de alianza
2	Plantear esta propuesta al área de IT para que soliciten las respectivas autorizaciones y se generen las correspondientes solicitudes dentro del área	15 días	coordinador del proceso de gestión de alianza
3	Una vez obtenidas las autorizaciones se deben generar cada uno de los usuarios, esto por parte del administrador encargado de las bases de datos, este procedimiento es soportado por el motor de bases de datos	2 días	Administrador de bases de datos Área de IT
4	Entregar las credenciales de acceso a cada uno de los empleados a los cuales se le genere el usuario en las respectivas bases de datos, el administrador debe hacer uso de	1 día	Administrador de las bases de datos

	cifrado de las credenciales al interior de la base de las bases de datos		
5	Inculcar la cultura dentro del proceso de Gestión de alianza sobre el uso de los usuarios principalmente sobre estas base de datos, dándole entender a los empleados la razón del cambio	2 días	Coordinador área IT
6	Eliminar usuario tipo genérico (compartido) de las bases de datos	1 día	Administrador de las bases de datos
7	Realizar seguimiento para establecer si se presentaron intentos no autorizados con el usuario genérico a las bases de datos (clientes y proveedores)	7 días	Administrador de bases de datos
8	Generar reporte entregando estadísticas sobre los accesos realizados, intentos de accesos no autorizados, mensualmente, para evaluar el comportamiento de los accesos a las bases de datos	1 día	Administrador de las bases de datos- Coordinador de IT

Tabla 3.Plan 1

Observación:

** Como sugerencia para la compañía es conveniente se evalué la existencia de más usuarios genéricos o compartidos en otros aplicativos y /o bases de datos, debido a que no es una buena práctica, adicional es conveniente dentro de la política de seguridad se realicen las respectivos ajustes sobre las consideraciones con relación a los usuarios genéricos si así lo decide la compañía.

Plan de tratamiento 2

Contexto

En el proceso de **gestión de compras y pedidos** se cuenta con un espacio físico adecuado como archivo en el cual se almacena documentación en físico (papel) relacionada con facturas, órdenes de compra clientes y órdenes de compra fabricantes, en dichos activos tal como se evidencia en la tabla de riesgos se puede observar que contienen datos personales los cuales al versen afectados se generaría un impacto alto tanto para el proceso como para la compañía como tal, a nivel de acceso físico existe una brecha de seguridad ya que una vez obtenido acceso a las instalaciones en las cuales se encuentra dicho proceso se tendría acceso directo al archivo que se encuentra en un cuarto al interior de la misma, solo se lleva control por medio de una bitácora donde se registra las personas que acceden a dicho cuarto y el motivo por el cual ingresa, aunque existen cámaras de video en el sitio es conveniente mejorar el **control de acceso físico** a dicho sitio y reducir al máximo se llegue a materializar una amenaza.

Plan sugerido

El plan consiste en la adición de un **control de acceso físico** para mejorar la protección en el archivo donde reposan activos tan importantes que contienen datos personales que se deben proteger al máximo para evitar materialización de amenazas.

ÍTEM	ACCIÓN	TIEMPO ESTIMADO PARA EJECUTAR	RESPONSABLE
1	Realizar cotización de materiales para implementar acceso con lector de tarjeta al archivo y generar propuesta a la dirección para recibir la respectiva aprobación, además se debe cotizar la mano de obra	15 días	Jefe de seguridad Física- Jefe del proceso de gestión de compras y pedidos
2	Presentar la propuesta a la dirección con la respectiva justificación relacionada con los riesgos evidenciados y los posibles impactos que trae para la compañía en caso de la materialización de una amenaza sobre alguno de los activos en mención, incluir en la propuesta el personal que sería autorizado	2 días	Jefe de seguridad Física- Jefe del proceso de gestión de compras y pedidos

	para ingresar a dicho sitio, aclarando que no es necesario adquirir más tarjetas de tipo NFC ya que todos los empleados cuentan con una de estas.		
3	En caso de recibir aprobación proceder con la ejecución de la propuesta adquiriendo los materiales y contratando el personal encargado para la adecuación, en caso que la compañía decida aceptar el riesgo y no implementar ningún control se debe dejar la respectiva evidencia de la notificación y la acción que decidió la dirección	10 días	Jefe de seguridad Física
4	Solo si se va a implementar el control es necesario realizar concientización para el personal que hace parte del proceso y de esta manera dar a entender el porqué del cambio, explicando cómo entra a operar dicho	2 días	Jefe del proceso de gestión de compras y pedidos

	acceso al sitio, documentado los procedimientos correspondientes		
5	Solo si es implementado el control es necesario realizar las respectivas pruebas, validando que solo tenga acceso el personal autorizado	5 días	Jefe de seguridad física
6	Validar los intentos no autorizados posterior a la implementación y generar reporte	30 días	Jefe de seguridad física- Jefe del proceso de gestión de compras y pedidos

Tabla 4.Plan 2

Plan de tratamiento 3

Contexto

A nivel digital los **contratos y soportes de proyectos** se manejan por medio de un aplicativo de desarrollo propio de la compañía, el cual es accesible a través de vía web, el mismo no se encuentra publicado hacia internet, solo es accesible internamente, la información de contratos se transmite desde las estaciones de trabajo de los gerentes de proyecto al servidor IIS (Internet Information Server), por la red interna se trasmite dicha información en donde están incluidos datos personales contenidos en los contratos y proyectos, se realiza backup de los archivos almacenados en dicho servidor a diario, pero existe una mala práctica que es transmitir la información por un protocolo no seguro (http),

si algún atacante llega a interceptar la comunicación al interior de la red puede capturar información valiosa de la compañía, tal como se muestra en la tabla de riesgos. Por tanto se plantea el uso de **protocolos seguros en la transmisión de información** para ello se plantea el siguiente plan de tratamiento.

Plan sugerido

Hacer uso de **comunicación segura** a través de https y certificados digitales SSL, de esta manera adicionar seguridad en la comunicación por donde se trasmite información con datos personales desde el navegador web al servidor, para ello se diseña el siguiente plan:

ÍTEM	ACTIVIDAD	TIEMPO ESTIMADO PARA EJECUTAR	RESPONSABLE
1	Diseñar propuesta para presentar al área de IT sobre el uso de certificados digital SSL para la conexión hacia dicha aplicación	15 días	Administrador de aplicación
2	Presentar propuesta y obtener aprobación. A nivel económico no tiene implicación alguna ya que el certificado puede ser auto firmado pues es de uso interno	2 día	Administrador de aplicación
3	Aprobar el cambio solicitado entendiendo el porqué de dicho	1 día	Jefe de Gestión de proyectos-Jefe del área de IT

	cambio y los riesgos que se están tratando con ello.		
4	Una vez aprobado proceder a ejecutar el procedimiento para cargar certificado y permitir el uso de protocolos seguros en dicha aplicación web: 4.1 Generar el CSR (Certificate Signing Request) desde el servidor para el certificado SSL 4.2 Firmar el CSR con la CA (Certificate Authority) Entidad Certificadora en este caso Interna 4.3 Generar el certificado y cargar sobre el servidor según el request generado 4.4 Realizar ajustes sobre la carpeta de la aplicación en el servidor 4.5 Desplegar el certificado en los equipos que requieren acceso a la aplicación web es decir los equipos de los gerentes de proyectos	7 días	Administrador de aplicación

	4.5 Validar el correcto acceso a la aplicación desde el navegador web 4.6 Si ocurre algún inconveniente es necesario realizar rollback (devolver los cambios) **para el procedimiento más detallado se entrega el siguiente enlace (https://support.microsoft.com/es-es/help/324069/how-to-set-up-an-https-service-in-iis)		
5	Si el cambio es exitoso realizar la respectiva capacitación a los usuarios de la aplicación sobre el cambio realizado y la importancia del mismo	2 días	Administrador de aplicación
6	Monitorear el correcto funcionamiento de la aplicación una vez realizado el cambio	30 días	Administrador de aplicación

Tabla 5.Plan 3

5. Asignación de las responsabilidades para el cumplimiento normativo

Con el fin de dar seguimiento a la metodología propuesta se evidencia que la compañía no cuenta con personal especializado en el tratamiento de los datos personales proporcionados por los clientes o fabricantes que manejan. Este es un riesgo importante

debido a que la información está siendo manipulada sin los controles especializados y está siendo transportada de manera deliberada, el nivel de confianza entre los empleados es bastante alta, pero es necesario que se tenga un grupo de trabajo que se encargue de la manipulación de esta información que es confidencial y que debe contar con un nivel de seguridad alto, el rol debe cumplir con:

- Conocimiento especializado en clasificación de información sensible.

- Tener experiencia en tratamiento de información perteneciente a datos personales o de carácter privado.

- Contar certificaciones laborales que constaten el trabajo realizado y la eficiencia con la que lo realizo.

Existen más características que debe tener este personal que depende de cada empresa y la finalidad que le darán al área. Las más importantes son las que se nombraron anteriormente para logra cumplir las leyes que en la actualidad se encuentran en Colombia.

Es necesario que los planes de tratamiento anteriormente mencionados sean vigilados en su ejecución por el personal responsable del tratamiento, esto debido a que ellos son las personas que trabajaran con este tipo de información y son los encargados que no exista fuga o robo de información, ellos son el principal encargado de la protección de dichos datos.

6. Aviso de privacidad

Para Colombia la compañía no cuenta con un aviso de privacidad explícitamente establecido para que los titulares conozcan las políticas de tratamiento de datos personales que ha establecido la misma, por tal motivo se plantea el siguiente modelo el cual puede

ser publicado en la página web o sea registrado en un medio visible para los clientes y fabricantes.

AVISO DE PRIVACIDAD:

Dando cumplimiento a la normatividad establecida de acuerdo a la Ley 1581 de 2012 y el Decreto 1377 de 2013 y como responsable del tratamiento de datos personales la compañía (distribuidora de tecnología) ubicada en la ciudad de Bogotá con los siguientes datos de contacto, los cuales son puestos a disposición de los titulares:

- NIT: 111.111.111-1
- Dirección: Calle X # X – X oficina X
- Teléfono: +57 17366034 Ext 1234

Finalidad

La finalidad de la recolección de los datos solicitados es con el fin de alimentar la base de datos de los clientes que maneja la compañía distribuidora de tecnología para tenerlos en cuenta en eventos, capacitaciones y compras de los diferentes fabricantes que se manejan en el portafolio. *(Se debe especificar el motivo de la recolección de la información solicitada y los fines para los cuales será utilizada, en caso quesean utilizadas para procedimientos diferentes puede llegar a sanción según lo estipula la ley).*

Derechos del titular

Para ejercer los derechos aquí mencionados se deberá llevar a cabo por los canales que (compañía distribuidora de tecnología) disponga para tal fin:

- Conocer, actualizar y rectificar sus datos personales.
- Solicitar prueba de la autorización.

- Ser informado del uso y tratamiento dado a sus datos personales

- Revocar la autorización y/o solicitar la supresión de uno a más datos cuando en el tratamiento no se respeten los principios.

- Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

Sobre la política de tratamiento, la misma estará disponible en el sitio web de la compañía (debe ser cargada en el sitio web) (https://www.XXXXX.com.co)

7. Finalidad

En la revisión de la empresa, se verifico que no existe una finalidad en donde se exprese para que serán usados los datos que están proporcionando, en el momento de solicitarlos de manera telefónica o presencial se habla del tema, pero según la ley debe haber un documento firmado con autorización en donde el dueño de la información sede los derechos de privacidad para los fines que la entidad los solicita. Un ejemplo seria:

La finalidad de la recolección de los datos solicitados es con el fin de alimentar la base de datos de los clientes que maneja la compañía distribuidora de tecnología para tenerlos en cuenta en eventos, capacitaciones y compras de los diferentes fabricantes que se manejan en el portafolio. (Se debe especificar el motivo de la recolección de la información solicitada y los fines para los cuales será utilizada, en caso quesean utilizadas para procedimientos diferentes puede llegar a sanción según lo estipula la ley).

8. Los derechos de los titulares

La compañía distribuidora de tecnología tiene definidos los derechos de los titulares del tratamiento de datos, siguiendo la normatividad establecido por la ley, más los mismos no

son correctamente divulgados, aquí se mencionan los derechos establecidos y los cuales deben ser contenidos en el aviso de privacidad y/o en la política del tratamiento de datos:

- Conocer, actualizar y rectificar sus datos personales.
- Solicitar prueba de la autorización.
- Ser informado del uso y tratamiento dado a sus datos personales
- Revocar la autorización y/o solicitar la supresión de uno a más datos cuando en el tratamiento no se respeten los principios.
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

9. formato de autorización

La compañía no tiene un formato en donde pida la autorización de la utilización de los datos personales que son solicitados, este es un tema importante tanto para las personas que envían la información como para aquellos que la reciben debido a que, si los datos son usados para fines diferentes no hay una constancia escrita en donde se especifique la finalidad y esto infringiría la ley y se aplicaran las sanciones y multas establecidas.

Este formato puede ser elaborado en formato de la empresa dando a conocer:

- Escribir a nombre propio de la persona.
- Finalidad de la recolección.
- Identificación de los datos solicitados.
- Validez y tiempo de tratamiento de los datos proporcionados.
- Derechos y deberes de los dueños de la información.

- Línea de atención para quejas, reclamos e información.

También puede ser un pie de nota en algún formato de registro del canal en donde se indique:

Dando cumplimiento a la normatividad establecida de acuerdo a la Ley 1581 de 2012 y el Decreto 1377 de 2013 y como responsable del tratamiento de datos personales la compañía XXX manejara los datos contenido en este archivo para fines de alimentación de la base de datos de la empresa. Este documente debe ir firmado por la persona que permite el tratamiento de los datos.

10. Eliminación de datos personales de clientes que no entregaron autorización

La compañía distribuidora de tecnología no cuenta con un procedimiento establecido para eliminar los datos personales de clientes que no entregan autorización, pues no existe la autorización formal (como se puede observar en el Ítem anterior) de parte del titular, de esta manera el personal encargado de realizar el tratamiento de datos al interior de la compañía deberá hacer expreso en su política de tratamiento de datos que al no recibir autorización dicha información será eliminada, además a nivel procedimental debe quedar establecido el mismo:

Nombre del Procedimiento	**Eliminación de datos que no cuentan con autorización del titular o que no se encuentren dentro de la finalidad establecida por la compañía.**
Propósito	Validar que se tenga la autorización para el tratamiento de datos recolectados en caso de no ser así eliminar los mismos,

Alcance	verificación de la autorización tomando como acción la supresión en caso de contar con la misma
Proceso	1. El personal asignado por la compañía como responsable del tratamiento de datos debe validar que se cuente con la evidencia de la autorización por parte del titular. 2. en caso de no contar con la autorización proceder a contactar a la persona por medio telefónico o vía correo electrónico en donde se le suministre el formato de autorización y el tiempo máximo que tiene para responder 3. El titular recibe el formato de autorización, lo firma y lo hace llegar en un plazo de una semana como máximo a la compañía 4. Si no se recibe la autorización, la compañía distribuidora de tecnología eliminara los datos personales con los cuales cuenta, ya que no se existe la autorización. Esto lo debe realizar el personal asignado por parte de la compañía.

	5. Paralelamente el personal asignado por la compañía para ejercer las funciones del tratamiento de datos deberá validar que los datos captados sean los requeridos para la cumplir con la finalidad del tratamiento, en caso de encontrarse datos no que sean requeridos se deberán eliminar los mismos pues no está autorizado su tratamiento.

Tabla 6.Procedimiento eliminación de datos que no cuenten con autorización

11. Establecimiento de canales

La empresa cuenta con una línea general de quejas y reclamos de todo lo relacionado con el Core de negocio, pero no cuenta con una línea especializada para este tipo de requerimientos, las personas que contestan este conmutador son especializadas en ventas de seguridad, pero desconocen el procedimiento de quejas y reclamos con respecto a mala utilización de los datos proporcionados por el cliente.

Como se indicó en la metodología es necesario que existan varios canales de atención con el fin de dar información especializada en cuanto a este tipo de información y que el cliente sienta que se está cumpliendo con la reglamentación existente en el país, para ellos se recomienda:

- Dirección física en donde el cliente de manera escrita pueda solicitar aclaraciones de la información sensible enviada.

  Calle X # X – X oficina X

- Un correo de servicio al cliente en donde puedan de manera digital enviar solicitudes y que se respondan con SLA menores a 3 horas debido a la importancia.

  Servicioclientes_proteccion@xxxx.com

- Formulario de PQR ubicado en la página WEB de la empresa para que sea más sencillo para el cliente.

  HTTPS://www.XXXX.com/servicio/cliente/PQR

- Chad en la página WEB con el fin de comunicar inconformidades y que sea atendido en la mayor brevedad posible.

  HTTPS://www.XXXX.com/Chat

- Teléfono fijo en donde se indique la extensión del área encargada de la protección de los datos proporcionados.

  +57 17366034 Ext 1234

• **Entrega y sustentación de los resultados**: consiste en la entrega y sustentación del formato de entrega final con los resultados obtenidos.

RESULTADOS

Una vez llevadas a cabo las diferentes fases de la estrategia metodológica utilizada para abordar la temática planteada en este documento se observa que en la **fase de investigación** se evidencio la existencia de una problemática importante a nivel de protección de datos personales la cual debe ser abordada desde este momento, debido a que cada día los sistemas como Big Data están ingresando a pasos agigantados al país y si no se toma una medida para protección los datos pueden ser robados de una manera sencilla por atacantes cibernéticos.

En la fase de **Planteamiento de la guía para tratamiento de datos personales con enfoque seguro,** se llegó al establecimiento de una guía con 11 pasos, la cual va enfocada al tratamiento de datos personales de una manera segura por parte de las compañías distribuidoras de tecnología siguiendo por un lado la normatividad vigente y por otro el enfoque de riesgos que se debe contemplar en cualquier aspecto de seguridad de la información.

En la fase de **Planteamiento de guía de buenas prácticas-controles,** se llegó al establecimiento de una serie de buenas prácticas que giran en torno a las medidas de seguridad que son convenientes, tomar para el tratamiento de riesgos que se encuentren sobre los activos que tengan relación con datos personales de terceros en el caso de las compañías distribuidoras de tecnología, los mismos van desde temas relacionados gobernanza, seguridad en el acceso y seguridad en IT.

Por ultimo en la fase de **Aplicación de la guía metodológica diseñada,** se observó que la compañía distribuidora de tecnología que fue objeto de estudio presenta varias deficiencias en el manejo de datos personales de terceros, pues no cuenta con la definición de varios de los requisitos establecidos en la guía la guía metodológica diseñada, en cuanto a los activos de información que están relacionados con datos personales se encontraron algunas vulnerabilidades que pueden ser explotadas por algún atacante y lograr la materialización de las amenazas generando posibles afectaciones para la compañía, para ello se realizó el planteamiento de unos posibles tratamientos para estas últimas (tomando como base la guía de buenas prácticas establecida la fase anterior).

CONCLUSIONES Y TRABAJO FUTURO

Con el desarrollo de este proyecto se reúne una serie de requisitos básicos que se recomiendan tener en cuenta en las compañías distribuidoras de tecnología, para el tratamiento de datos personales de terceros de una manera segura con un enfoque de riesgos y con base en el cumplimiento de la normatividad nacional vigente en cuanto a este se refiere todo reunido en una guía metodológica cuyo propósito es, tratar riesgos relacionados con el incumplimiento de las leyes vigentes y el incorrecto manejo de los datos personales a cargo. Estos riesgos de los que se hablan durante todo el trabajo y que se ven plasmados en el desarrollo trae consigo impactos económicos, sancionatorios e inclusive afectación en la reputación las compañías, tal como ha sucedido con varias compañías de otros sectores que se han visto afectadas por no dar un manejo adecuado a los datos personales lo de los cuales son responsables.

Este tipo de proyectos permiten al estudiante llevar de la teoría a la práctica y evidenciar lo que en realidad está pasando en las diferentes empresas, permite que se lleve más allá del conocimiento y se conozca a cabalidad los diferentes problemas que se están teniendo en cuanto a la seguridad de la información que es el foco de la especialización que está siendo objeto de estudio y permite dar soluciones concisas a los diferentes riesgos existentes.

Para una futura oportunidad y como continuación del proyecto se evaluará la opción de que se amplié el alcance no solo con dirección hacia compañías distribuidoras de tecnología sino a los sectores más críticos en Colombia, en donde se pueda evaluar el enfoque de riesgos y cumplimiento de la normatividad establecida para el tratamiento de datos personales de forma segura y ofrecer ayudas prácticas para ayudar y evitar sanciones.

REFERENCIAS

[1] Milne, G. R., Pettinico, G., Hajjat, F. M., & Markos, E. (2017). Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing. Journal Of Consumer Affairs, 51(1), 133-161. doi:10.1111/joca.12111

[2] De Qin, Cheng. (2005). Personal Data Protection in Electronic Business. Xi'an University of Post and Telecommunications, 893-895

[3] Leon Carvajal, Maria C. (2010). Las tecnologías de la información, la comunicación y la protección de datos personales. Universidad de Cuenca, 1-51.

[4] Monsalve Caballero, Vladimir. (2017). LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LOS CONTRATOS ELECTRÓNICOS CON CONSUMIDORES: ANÁLISIS DE LA LEGISLACIÓN COLOMBIANA Y DE LOS PRINCIPALES REFERENTES EUROPEOS. Prolegómenos, 20(39), 163-195. https://dx.doi.org/10.18359/prole.2729

[5] de Hert, P., Papakonstantinou, V., Wright, D., & Gutwirth, S. (2013). The proposed Regulation and the construction of a principles-driven system for individual data protection. Innovation: The European Journal Of Social Sciences, 26(1/2), 133-144. doi:10.1080/13511610.2013.734047

[6] Remolina-Angarita, Nelson. (2010). ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?. 16 International Law, Revista Colombiana de Derecho Internacional, 489-524.

[7] Wilson, S. (2015). Big data held to privacy laws, too. Nature, 519(7544), 414. https://doi.org/10.1038/519414a

[8] Recio, M., & De Reflexión, A. (2017). Big Data: Hacia La Protección De Datos Personales Basada En Una Transparencia Y Responsabilidad Aumentadas, (17). https://doi.org/10.15425/redecom.17.2017.09

[9] Parraguez Kobek, L., & Caldera, E. (2016). Cyber Security and Habeas Data: The Latin American response to information security and data protection. Oasis, (24), 109. https://doi.org/10.18601/16577558.n24.07

[10] Didier, M. M., Romero, E. J. I., & Parini, N. F. (2016). Registro de objetores de conciencia: implicancias de los derechos a la igualdad y a la protección de datos personales. Revista Persona Y Derecho, 0(73), 231–259. https://doi.org/10.15581/011.73.231-259

[11] Vegazana, C. De. (2012). Códigos tipo: derecho a la información y protección de datos personales.

[12] Ordoñes, A. L. (2010). Universidad de cuenca facultad de jurisprudencia escuela de derecho "utilización de la firma dijital para la protección de datos personales como medio de seguridad en las transacciones electronicas.," 1(95), 1–95.

[13] Departamento Administrativo de la Función Pública. (2016). Instructivo de la Política para el Tratamiento de Datos Personales, 10–11. Retrieved from

http://www.funcionpublica.gov.co/documents/418537/1512450/InstructivoPolitica_Datos.pdf/f7d7cbe2-6739-46de-9f76-ee147cf1aa60.

[14] Alcaldía mayor de Bogotá (2012). Ley 1581 de 2012 Nivel Nacional, ley estatutaria. Retrieved from http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981.

[15] Secretaria del senado (2008). Ley estatutaria 1266 del 31 de diciembre de 2008. Retrieved from http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html.

[16]. Ley 1581 de 2012 Nivel Nacional. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981. Consultado 30/03/2018

Guide to securing personal information, 2015. Australian Goverment. Recuperado de https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information#part-a-circumstances-that-affect-assessment-of-reasonable-steps. Consultado 07/04/2018

Alcaldía mayor de Bogotá (2013). Decreto 1377 de 2013 Nivel Nacional, Decreto protección de datos personales. Retrieved from http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646.

Larios Olivos, Y. J. (2014). Guía metodológica para la protección de datos en la utilización de la computación en la nube, 1–82. Retrieved from http://repositorio.cuc.edu.co:80/xmlui/handle/11323/237.

Alvarado. J. A. R. (2015). Implementación de la protección de datos personales en el SGC basado en la ley1581 para una institución privativa de la libertad. Tesis de Grado, 1. Retrieved from https://www.umng.edu.co/repositorio/tesis/especializacion.