CREACIÓN E IMPLEMENTACIÓN DE MANUALES Y POLÍTICAS DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES EN LA EMPRESA INFRAROM SAS, EN CUMPLIMIENTO A LA LEY 1581 DE 2012 PARA EL RNBD ANTE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO.

STELLA DIANA RODRÍGUEZ RINCÓN
IVÁN EDUARDO ROMERO VARELA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
BOGOTÁ
2019

CREACIÓN E IMPLEMENTACIÓN DE MANUALES Y POLÍTICAS DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES EN LA EMPRESA INFRAROM SAS, EN CUMPLIMIENTO A LA LEY 1581 DE 2012 PARA EL RNBD ANTE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO.

STELLA DIANA RODRÍGUEZ RINCÓN
IVÁN EDUARDO ROMERO VARELA

Proyecto aplicado para optar al título de:
"Especialista en Seguridad Informática"

Director, MARIANO ESTEBAN ROMERO TORRES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
BOGOTÁ
2019

Artículo 23 de la Resolución No. 13 de Julio de 1946

"*La UNAD Universidad Nacional Abierta y a Distancia, no se hace responsable por los conceptos emitidos por sus alumnos en sus trabajos de tesis. Solo velará por que no se publique nada en contrario al dogma y a la moral católica y porque el proyecto de grado no contengan ataques personales contra persona alguna, antes bien se vea en ellas el anhelo de buscar la verdad y la justicia*."

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, Marzo de 2019

CONTENIDO

pág.

LISTA DE TABLAS

LISTA DE FIGURAS

ANEXOS

Anexo A Recolección de datos responsable del tratamiento

Anexo B Clases de bases de datos

Anexo C Finalidades

Anexo D Formato de recolección de información de base de datos

Anexo F Manual paso a paso del Registro Nacional de Base de Datos

INTRODUCCIÓN

En Colombia se está empezando a crear la cultura de protección de datos personales, dado a un gran número de leyes que tienen como fin crear conciencia de su importancia que van de la mano con derechos fundamentales del ser humano a la honra, al buen nombre y la intimidad, vulnerado cuando no existe una adecuada administración y tratamiento de los datos.

La creación de la ley estatutaria 1581 de 2012 sirve como una herramienta para las empresas que manejan bases de datos personales, puesto que, da las pautas para establecer el tratamiento de datos en todas sus etapas, como también responde a la protección de los derechos fundamentales a la honra, la intimidad y el buen nombre de los empleados, clientes, proveedores y personas que tengan alguna relación comercial con la empresa.

Con esta ley algunas empresas deben realizar el Registro Nacional de Base de Datos en la Superintendencia de Industria y Comercio con un plazo máximo de Enero de 2019. Con este proyecto de grado la empresa Infrarom SAS busca dar cumplimiento a dicha ley.

1. EL PROBLEMA DE INVESTIGACIÓN

Al revisar la ley 1581 de 2012, se identifica que la empresa INFRAROM SAS maneja datos personales de clientes, proveedores y empleados en sus bases de datos y sus políticas de seguridad no se ajustan a las exigidas por la ley, por lo tanto no está lista para realizar el Registro Nacional de Base de Datos ante la Superintendencia de Industria y Comercio.

1.1. DESCRIPCIÓN DEL PROBLEMA

En Colombia se está empezando a dar la importancia requerida a la protección de datos personales, con la aprobación de la Ley Estatutaria 1581 de 2012 que ha servido de instrumento en el avance de la protección integral del derecho a la privacidad. Esta ley va de la mano con el derecho a la honra, al buen nombre y la intimidad, vulnerado cuando no existe una adecuada administración y tratamiento de los datos.

Los avances al nivel del manejo de la información a través de los computadores, facilita la concentración automática de datos referidos a las personas y se convierte en un verdadero factor de poder. Como describe Nelson Remolina (2010 p. 492) estos sistemas de información:

> "se nutren de datos personales, ofrecen innumerables posibilidades para recolectar, almacenar y circular esa información en poco tiempo y de manera imperceptible para las personas a que se refieren los datos, no son absolutamente seguros, evolucionan rápidamente y traspasan las fronteras físicas, lo cual facilita el flujo internacional de la información en mención"

De ahí nace la necesidad de implementar un conjunto de normas y principios que regulen el tratamiento de datos personales en las etapas de recolección, almacenamiento, circulación, publicación y trasferencia de datos.

Con la nueva normativa algunas empresas deben realizar el Registro Nacional de Bases de Datos ante la Superintendencia de Industria y Comercio, la cual impartió instrucciones a los Responsables del Tratamiento de datos personales, sociedades y entidades sin ánimo de lucro que tengan activos totales mayores a 100.000 UVT y personas jurídicas de naturaleza pública, para realizar dicho registro con un plazo máximo de enero del 2019. El Registro de las Bases de Datos debe ir de la mano a la implementación de múltiples normas de seguridad de la información personal, donde se debe asegurar que los datos se encuentran protegidos.

Aunque con la modificación realizada a la ley con el decreto 090 del 18 de enero del 2018 la empresa INFRAROM SAS no está obligada a realizar el RNBD, en su momento se realizó este proceso ya que se considera de gran importancia el manejo adecuado de los datos personales de sus clientes, empleados y proveedores, así como implementar las medidas de seguridad reglamentadas en la ley, por esta razón se identificarán los factores de riesgo que afectan la confidencialidad, integridad y seguridad de los datos personales para poder cumplir con la ley y garantizar la aplicación de las normas y principios que regulen el tratamiento de datos personales en las etapas de recolección, almacenamiento, circulación, publicación y trasferencia de datos.

1.2. FORMULACIÓN DEL PROBLEMA

¿Está preparada la empresa Infrarom SAS, para garantizar a sus clientes, proveedores y a sus empleados, total confidencialidad de sus datos personales, con adecuadas políticas en el manejo de la información y efectividad en los mecanismos de protección, en cumplimiento a los requisitos establecidos en la ley 1581 de 2012?

1.3. SUBPREGUNTAS

¿Se tiene identificadas las bases de datos que manejan información personal de clientes, proveedores y empleados de la empresa Infrarom SAS?
¿Se está manejando de forma adecuada las políticas de seguridad para las bases de datos que contienen datos personales de empleados, clientes y proveedores de la empresa Infrarom SAS?

¿Se cuenta con políticas, manuales y formatos que cumplan con la ley 1581 de 2012, donde se tenga en cuenta el adecuado tratamiento de los datos personales en la empresa Infrarom SAS?

¿La empresa Infrarom SAS, ya realizó el registro nacional de bases de datos ante la superintendencia de Industria y Comercio, para dar cumplimiento a lo establecido en la Ley 1581 de 2012?

1.4. OBJETIVOS

1.4.1. Objetivo General.

Asegurar la integridad y confidencialidad de los datos personales de los clientes, proveedores y empleados de la empresa Infrarom SAS a través del diseño de manuales y políticas de tratamiento y protección de datos que permita dar cumplimiento a los requisitos establecido por la ley 1581 de 2012.

1.4.2. Objetivos específicos.

- Identificar las bases de datos de la empresa Infrarom SAS, que contengan datos personales de sus clientes proveedores y empleados, para revisar qué tipo de dato y la seguridad que se tienen en su tratamiento, de esta manera analizar el cumplimiento de la ley 1581 de 2012.

- Diseñar políticas de seguridad, manuales de procedimientos, recomendaciones y formatos para el tratamiento de datos personales en la empresa Infrarom SAS.

- Implementar las políticas de seguridad y diligenciar los formatos creados para el tratamiento de los datos personales en la empresa Infrarom SAS, incluyendo empleados, clientes y proveedores de quien se maneje o se realice tratamiento de datos personales.

- Realizar el Registro Nacional de Base de Datos ante la superintendencia de Industria y comercio, cumpliendo con la normativa dada en la Ley 1581 de 2012, sobre el tratamiento de los datos personales almacenados en ellas. De esta manera dar cumplimiento a la ley.

1.5 JUSTIFICACIÓN

La protección de datos personales está dado por un conjunto de normas que establecen el tratamiento de los datos en todas sus etapas, recolección, almacenamiento, circulación, publicación y transferencia tanto nacional como internacional, de la mano con los derechos fundamentales a la intimidad, la honra y el buen nombre establecidos en la Constitución Política Colombiana. Busca establecer un punto de equilibrio entre la necesidad de utilizar un dato personal y los derechos integrales de la persona. El habeas data puede entenderse como:

> “el derecho de toda persona a interponer la acción de amparo para tomar conocimiento de los datos a ella referidos y de su finalidad; sea que ellos reposen en registros o bancos de datos públicos, o los privados destinados a proveer informes y, en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos” (Ortiz, 2001 p. 70).

La información, y los datos personales son los activos intangibles con que cuentan las empresas, por tanto, debe existir confianza en el buen manejo de

estos activos que garanticen la efectividad de los mecanismos de protección. El correcto tratamiento de los datos es de vital importancia para la empresa; así como, tomar las medidas necesarias que garanticen al cliente, proveedores y personas que tengan relación comercial con la empresa la total confidencialidad de sus datos para generar y promover confianza en los clientes. Para los ingenieros y personal especializado de la empresa, quienes están en constante capacitación en la adecuada política del manejo de la información, la protección de los datos de sus clientes es su principal objetivo.

La Ley Estatutaria 1581 de 2012 ha servido de instrumento en el avance de la protección integral del derecho a la privacidad. Esta ley va de la mano con el derecho a la honra, al buen nombre y la intimidad, vulnerado cuando no existe una adecuada administración y tratamiento de los datos.

Con la nueva normativa algunas empresas deben realizar el Registro Nacional de Bases de Datos ante la Superintendencia de Industria y Comercio, la cual impartió instrucciones a los Responsables del Tratamiento de datos personales, sociedades y entidades sin ánimo de lucro que tengan activos totales mayores a 100.000 UVT y personas jurídicas de naturaleza pública, para realizar dicho registro con un plazo máximo de Enero del 2019. El Registro de las Bases de Datos debe ir de la mano con la implementación de normas de seguridad de la información personal, donde se debe asegurar que los datos se encuentran protegidos.

Infrarom SAS es una Pyme constituida en abril de 2013 que considera que es importante realizar el RNBD ante la superintendencia y por esta razón se escoge este tema para dar desarrollo al programa integral de documentación exigida por la SIC, implementar documentos internos de políticas y procedimientos, políticas internas de seguridad, políticas web, reconocimiento de seguridad para los empleados, implementación de contratos de confidencialidad, de trasmisión de datos, consentimiento para correos electrónicos, tratamiento de datos personales, de datos sensibles, de datos biométricos, cláusulas de video entre otras.

1.6. DELIMITACIÓN DEL PROYECTO

1.6.1. Alcance

Este proyecto tiene como alcance el diseño del manual y las políticas de Tratamiento de Datos y Protección de Datos Personales, para conocimiento de todos los empleados, así como para todos los clientes, asesores externos, personal temporal e invitados, para la recolección o tratamiento de datos personales ya almacenados en las bases de datos de Infrarom SAS, teniendo en cuenta la normas de la Ley 1581 de 2012 (Ley de Habeas Data).

Al igual que solicitar las autorizaciones para el manejo de datos personales que se tiene en las bases de datos de la empresa y en los documentos físicos de nuestros empleados, clientes, proveedores o personas que han tenido alguna relación con la empresa, así como realizar un formato para futuras autorizaciones que permita cumplir con las políticas de tratamiento de datos personales.

Establecer e implementar documentos internos de políticas y procedimientos, políticas internas de seguridad, políticas web, reconocimiento de seguridad para los empleados, implementación de contratos de confidencialidad, de trasmisión de datos, consentimiento para correos electrónicos, tratamiento de datos personales, de datos sensibles, de datos biométricos, cláusulas de video entre otras.

1.6.2. Delimitación

El proyecto está contemplado para la empresa Infrarom S.A.S., las bases de datos que contengan información personal y la información personal automatizada y física que maneje de clientes, proveedores y terceros que tengan o hayan tenido alguna relación directa con la compañía de nacionalidad o residentes colombianos.

Aplicado a todos los productos y servicios prestados por la compañía para sus clientes, proveedores, empleados y terceros.

El tiempo delimitado para el proyecto es de seis meses para el Registro Nacional de Base de Datos (RNBD) en la Superintendencia de Industria y Comercio fecha límite enero del 2019, seis meses para la implementación de los manuales y políticas de Tratamiento de Datos y Protección de Datos Personales en todos los servicios prestados por la compañía para sus clientes, proveedores, empleados y terceros.

2. MARCO REFERENCIAL

2.1. ANTECEDENTES

Dentro de la bibliografía consultada se encontraron diversos artículos que permiten ver amplias investigaciones que se han realizado sobre el tema de las leyes para la protección de los datos personales, una investigación aplicada similar a la que se está realizando, es la que se realizó la Universidad Católica de Colombia titulada “Guía de Implementación y lecciones aprendidas para el proyecto de aplicación de la ley de protección de datos personales. Caso Fiduprevisora” (2017), muestra la importancia de implementar la ley 1581 de 2012 en algunas empresas para dar cumplimiento a la normatividad vigente, en ella el autor busca disminuir los riesgos a los cuales están expuestas las empresas al hacer un mal uso de los datos personales, ya que la ley establece unas sanciones para las empresas que no cumplan con la protección y el tratamiento de los datos, busca también establecer controles y responsabilidades sobre cada una de las bases de datos que contengan datos personales ya sea de empleados, clientes, proveedores.

Esta investigación concluye la importancia de ser asesorado por un experto en la ejecución de la ley, realizando un análisis y recolección de la información para poder determinar una matriz de riesgos de las bases de datos encontradas, para de esta manera organizar políticas para el tratamiento de los datos personales de una forma transversal en la compañía. El cumplimiento de la ley mantiene a la compañía en el mercado dando confianza a sus clientes, empleados y proveedores.

Otra estudio empírico realizado en la Universidad Militar Nueva Granada “La protección jurídica Colombiana al derecho a la intimidad frente al desarrollo tecnológico” (2013) describe como gracias a la tecnología se ha facilitado la recolección, transmisión, almacenamiento de datos personales, poniendo en riesgo los derechos a la intimidad, la buena honra y la protección de los datos

personales, en esta investigación se identifican los vacíos que se encuentran en las leyes, viendo cómo se vulneran los derechos humanos.

Este estudio es una investigación empírica, analítica y comparativa que realiza una reseña histórica, sobre la normatividad que existe sobre la protección de los datos personales y la relación con el desarrollo tecnológico que amenaza constantemente el derecho a la intimidad, dentro de las conclusiones de este estudio está la educación preventiva que se debe realizar a los usuarios de estas nuevas tecnologías para evitar que compartan información personal, de su familia o de menores de edad, a través de redes, lo cual puede generar mala utilización de estos datos para extorsión abuso y otros peligros que vemos en estos tiempo. Muestra la implementación de la ley 1581 de 2012 y la necesidad de adquirir la autorización para el manejo y el tratamiento de los datos personales en las empresas.

Por último un estudio de la Universidad Católica, “Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales” (2014) realizado por Marcela Rojas, muestra la evolución de la normatividad con respecto a la protección de los datos personales tanto a nivel nacional e internacional, se describen artículos internacionales de países latinoamericanos, estadounidenses, y de la unión europea, que tienen relación con las leyes de protección de datos vigentes, identifica los países que cuentan con una adecuada regulación de las leyes de protección de datos, análisis global de las normas, derechos de reglamentación, concluyendo que Colombia es uno de los países latinoamericanos que a través de la ley 1581 de 2012 sobre la protección de datos esta entre el grupo de países que cuenta con una regulación integral sobre el tratamiento de los datos personales ayudando a regular el derecho constitucional a la intimidad, así como el derecho de conocer que información personal se tiene en las bases de datos, actualizarla y rectificarla, mediante la Ley 1581 de 2012, reglamentada parcialmente por el Decreto 1377 de 2013, se regulan aspectos relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados y el ejercicio de los derechos de los titulares de la información.

2.2. MARCO TEORICO CONCEPTUAL

2.2.1. Definiciones

Estas definiciones son tomadas de “LEY ESTATUTARIA 1581 DE 2012 (Octubre 17/2012) Reglamentada parcialmente por el Decreto Nacional 1377 de 2013” Por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 1581 de 2012: Es la ley que complementa la regulación para la protección del derecho fundamental que tiene todas las personas naturales a autorizar la información personal que es almacenada en base de datos.

Dato Personal: información que se puede asociar a una o varias personas naturales.

Dato Personal Público: Son datos que según la Constitución son considerados públicos, por esta razón no se necesita autorización de la persona dueña de la información, entre estos se encuentra teléfono, datos sobre el estado civil, dirección.

Dato Personal Semiprivado: No son datos reservados de una persona, ni datos que deban ser manejados por todas las personas, o sea públicos. Para el tratamiento de este tipo de datos es necesaria la autorización de la persona titular de la información. Por ejemplo datos de un crédito, datos financieros.

Dato Personal Privado: Son datos que solo le interesan a la persona dueña del dato y para su tratamiento requiere la autorización de la persona, ejemplo dato de escolaridad.

Dato Personal Sensible: Estos datos son de suma importancia ya que el mal uso de ellos pueden generar discriminación, no deben ser tratados a menos que sea requerido para alguna emergencia vital del titular o este se encuentre incapacitado y su obtención haya sido autorizada expresamente. Entre estos datos encontramos raza, orientación política, religión, datos biométricos, datos de salud.

Encargado del Tratamiento: Esta persona puede ser jurídica o natural, privada o pública, encargada de realizar el tratamiento de datos personales y es adjudicado como el responsable de los datos.

Política de Tratamiento: Documento que contiene la política del tratamiento de datos personales aplicada a una empresa, que debe cumplir con los lineamientos de la legislación vigente en la materia.

Proveedor: Persona jurídica o persona natural que presta algún servicio a la empresa en virtud de una relación contractual/obligacional.

Responsable del Tratamiento: persona que decide sobre la base de datos y el tratamiento, para implementar la política, será el responsable, en principio, la empresa.

Titular: Persona dueña de los datos personales que van a ser tratados, puede ser un proveedor, un cliente, un empleado, o un tercero que por relaciones comerciales o jurídicas, proporciones los datos personales a la empresa.

Trabajador: Persona que brinde un servicio a la empresa a través de un contrato laboral.

Transferencia: hace referencia al envío de datos personales manejados por la empresa a un tercero ya sea persona natural o jurídica, siempre teniendo en cuenta la política y autorizaciones para el tratamiento efectivo de datos personales.

Trasmisión: hace referencia a la comunicación de datos personales por parte de la persona responsable de tratar los datos personales.

Tratamiento: Hace referencia a las operaciones que se realicen con los datos personales, ya sea de recolección, almacenamiento, uso, circulación o supresión.

2.2.2. Ley 1581 de 2012 protección de datos personales

En Colombia la protección de datos es un derecho que se encuentra documentado en las diferentes leyes que se han formulado para una reglamentación administrativa; sin embargo, todavía no se tiene una cultura empresarial sobre la responsabilidad del tratamiento de datos con respecto a la protección y seguridad, las empresas manejan los datos personales de sus clientes, proveedores, empleados, como si fueran de su propiedad, sin la debida autorización de los titulares de la información.

Con la implementación de la ley 1581 de 2012 se quiere implementar y fomentar el derecho a conocer, actualizar y rectificar la información personal que se encuentren en diferentes bases de datos, además, se va a exigir una autorización del titular del datos para el tratamiento del mismo.

En la actual sociedad la protección de algunos derechos humanos se encuentran comprometidos ante el inadecuado uso de la tecnología que hace de la información un recurso muy accesible. Estos derechos se encuentran, relacionados con la protección de datos como son el derecho a la información, al buen nombre y a la intimidad. Estos derechos los reconoce la propia Corte Constitucional en su pronunciamiento:

> "La honra y el buen nombre de las personas, (...), constituyen, junto con el derecho a la intimidad los elementos de mayor vulnerabilidad dentro del conjunto de los que afectan a la persona a partir de publicaciones o informaciones erróneas, inexactas o incompletas".

La Constitución Política de Colombia ha otorgado el derecho del hábeas data al titular de los datos personales, lo cual les da derecho a exigir a los administradores de estos, el acceso, inclusión, exclusión, adición, corrección, actualización y certificación de los datos, como también limita la posibilidad de divulgarlos, publicarlos o cederlos, conforme a los principios que regulan el proceso de administración de datos personales que manejen las empresas. Este derecho tiene naturaleza autónoma y relación con los derechos a la intimidad y a la información. (Galvis, 2012)

Para dar cumplimiento a la norma, el tratamiento de los datos personales ya sea hecho por persona privada, pública, jurídica o natural, debe cumplir con las reglas establecidas en la ley de tratamiento de datos personales, solo puede realizarse con la autorización del titular de los datos garantizando ante todo la confidencialidad y reserva de la información.

La información que se tiene almacenada en las bases de datos debe ser completa, actualizada, comprobable, veraz y comprensible, y debe darse acceso al titular de la información.

Para dar cumplimiento a la ley, se encargó a la Delegatura para la Protección de Datos Personales que pertenece a la Superintendencia de Industria y Comercio (SIC), como autoridad para vigilar y controlar su tratamiento.

Para poder establecer el buen manejo de las base de datos personales la Superintendencia de Industria y Comercio creó el Registro Nacional de Base de Datos (RNBD), donde algunas empresas deben registrar las bases de datos que tengan información personal y nombrar un responsable para su tratamiento, El RNBD es el directorio público administrado por la Superintendencia de Industria y Comercio, estas bases de datos tendrán Políticas de Tratamiento que estarán sujetas a la aplicación de la norma.

No se aplica la ley 1581 de 2012 a las bases de datos que contengan: “información de uso personal o doméstico, información que tiene por finalidad la seguridad y defensa nacional, información que tiene por finalidad la prevención, detección, monitoreo y control del lavado de activos y financiación del terrorismo, información que tiene por finalidad de inteligencia y contrainteligencia”. (Remolina, 2010)

Por otra parte la ley 1581 contempla una protección especial para el tratamiento de los datos personales de los menores de edad, este podrá realizarse siempre y cuando no se ponga en peligro o vulnere algún derecho fundamental promoviendo su desarrollo armónico integral y la protección de sus intereses. Las personas que autorizan el tratamiento de los datos personales de los

menores de edad deben ser su representantes legales quienes se harán responsables de su uso.

Según la Ley 1581 de 2012 los derechos de los titulares de los datos personales son: “conocer, actualizar y rectificar sus datos personales, solicitar la prueba de su autorización para el tratamiento de sus datos personales, ser informado respecto del uso que se le da a sus datos personales, revocar la autorización y/o solicitar la supresión de sus datos personales de las bases de datos o archivos cuando el titular lo considere, presentar quejas ante la entidad administrativa encargada de la protección de los datos personales”. (SERVINCOOP, S.F.)

Las empresas deben crear un formato de autorización expresando la finalidad para la cual se necesitan los datos personales, debe ser previa, informada y expresa por el titular; esta autorización la pueden obtener de forma escrita, física o electrónica, y permitir ser consultada en cualquier momento.

La ley 1581 de 2012 determina que no es necesaria la autorización del titular cuando: “se trata de datos personales públicos, los datos personales son requeridos por una entidad pública en ejercicio de sus funciones, se está frente a casos de urgencia médica o sanitaria, son tratados para fines históricos, estadísticos o científicos, el dato se relaciona con información contenida en el registro civil”.

Las empresas deben nombrar un responsable y encargados del tratamiento de los datos, esta persona puede ser de carácter privado, público; natural o jurídica, quien tiene como función decidir sobre el tratamiento de la base de datos, debe indicar la finalidad del recaudo del dato personal al titular, informar sus derechos, los medios por los cuales el titular puede ejercer sus derechos, informar que los datos que requieran autorización no está obligado a suministrarlos.

Otros deberes de los responsables del tratamiento de los datos personales son: “informar y garantizar el ejercicio de los derechos de los titulares de los datos personales, tramitar las consultas, solicitudes y reclamos, utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran, respetar las condiciones de seguridad y privacidad

de información del titular, cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente". (Ley 1581 de 2012)

La entidad encargada de la vigilancia y el cumplimiento de la ley de protección de datos personales es la SIC, a través de la Delegatura para la Protección de Datos Personales quienes estarán a cargo del registro nacional de base de datos cuya información es de interés para las autoridades de vigilancia, posteriormente servirá para orientar la política pública sobre el tema; los responsables del tratamiento deben reportar el tipo de datos almacenados, las medidas de seguridad sobre los mismos, su procedencia, los reclamos interpuestos por los titulares, los incidentes de seguridad y las políticas de tratamiento de datos personales que aplican.

La Circular No. 02 de 3 de noviembre de 2015 expedida por la SIC, "estableció como plazo máximo para el registro inicial de las bases de datos, el 9 de noviembre de 2016; sin embrago, mediante decreto 1759 de 2016, se amplió el plazo al 30 de junio de 2017 en lo que concierne a personas jurídicas de naturaleza privada y sociedades de economía mixta, la última modificación realizada en el decreto 090 de enero del 2018 no obliga a las sociedades y entidades sin ánimo de lucro y personas naturales a realizar el RNBD ante la superintendencia de Industria y comercio, con el objetivo de disminuir la cantidad de empresas vigiladas, ampliando como último plazo para las empresas que están obligadas para el 31 de enero de 2019.

La ciudadanía en general se encuentra desinformada del derecho constitucional del Habeas Data, es importante trabajar educándolos en sus derechos y exigiendo a las empresas el cumplimiento de su deber ante el tratamiento y la protección de los datos personales.

Las empresas que dentro de su labor necesiten administrar, recoger, manejar, almacenar cualquier datos personales de sus trabajadores, clientes, contratistas, proveedores, debería estar obligado a realizar el registro nacional de bases de datos y crear las políticas de tratamiento en conformidad con la ley 1581 de 2012, quienes están obligados, al no hacerlo tendrá que asumir una

multa de hasta dos mil salarios mínimos mensuales legales vigentes y el cierre temporal o suspensión de la actividad.

El Gobierno Nacional amplió el plazo para que los responsables del tratamiento de la información personal en Colombia inscriban sus bases de datos en el Registro Nacional de Bases de Datos ante la Superintendencia de Industria y Comercio y deberán realizar la inscripción de las bases de datos que manejen a más tardar el treinta (30) de enero del 2019. (Decreto N° 090 del 18 de enero de 2018). Este procedimiento se realiza de forma sencilla y rápida y puede hacerse a través de la página web de la Superintendencia de Industria y Comercio www.sic.gov.co, algunas empresa deben inscribir cada una de las bases de datos que manejen, en el RNBD. Este trámite no tiene ningún costo, y excluye a las sociedades y entidades sin ánimo de lucro y personas naturales.

2.3. MARCO CONTEXTUAL

Infrarom S.A.S. es una empresa pequeña que fue fundada en el año 2013 que vio la necesidad de prestar un servicio de excelente calidad a micro empresas y Pymes que no tuvieran acceso o presupuesto para tener un área de tecnología, pero que aun así necesitaran los servicios de licenciamiento, correo empresarial, chat empresarial, alquilando los servidores en la nube, prestando todo tipo de soporte tecnológico que requiera.

Es una empresa dedicada a la ingeniería de información, que cuenta con diferentes áreas de trabajo, dispuestos a ofrecerle atención las 24 horas del día los 365 días del año. En Infrarom S.A.S. se cuenta con la más alta tecnología y calidad para el desarrollo de Software y mantenimiento de sus servidores y equipos.

Infrarom SAS, tiene como misión “brindar soluciones eficaces e inteligentes para gestionar los cambios necesarios para la tecnología y desarrollo de su empresa, así mismo desea contribuir a mejorar las capacidades productivas de su empresa tanto en la industria como en el sector en el que se encuentra y así ayudarle a

potenciar el mercado y la demanda de sus productos o servicios" (Infrarom, 2014), el alcance de este proyecto es ambicioso pero adecuado, ya que la empresa es una Pyme que en el momento cuenta con poco tiempo de constitución, se cuenta con diez clientes y 12 personas con contrato laboral con la empresa, lo cual hace posible y facilita la recolección de los datos personales, la recopilación de las bases de datos de nuestros clientes y la recopilación de los datos personales de nuestros empleados y de los profesionales que han tenido y tienen relación con la empresa. Todo esto hace posible lograr el objetivo de dar la mayor seguridad de los datos que maneja la empresa en cada uno de sus procesos y servicios. Aunque somos una micro empresa y de acuerdo con la última modificación no estaríamos obligados a realizar el RNBD, para Infrarom SAS es de vital importancia el manejo de los datos personales y la implementación de manuales y políticas de seguridad.

Cerda Gutiérrez (1996) dice que si el proyecto es de origen institucional, tiene enorme importancia el marco general de la entidad por la gran utilidad de la información que se aporta sobre la organización responsable del proyecto. Cuando el proyecto se efectúa en la misma institución la información es obvia. Es muy útil tener en cuenta la información que tiene que ver con las políticas y prioridades de la organización y las relaciones que tenga con otras instituciones.

2.4. MARCO LEGAL

Para la protección de datos personales solo existía la ley 1266 de 2008, que era exclusiva para los datos de carácter comercial y financiero y los reportes en centrales de riesgo; esta ley sigue vigente para los datos personales crediticios, financieros, comerciales y de servicios registrados en un banco de datos.

Con la expedición de la ley 1581 de 2012 se amplió la protección de los datos aplicado a todas la bases de datos de entidades privadas y públicas que utilicen y almacenen datos personales, excepto las bases de datos de uso doméstico, las de inteligencia, las de contra inteligencia, las de seguridad nacional, la de

censos y las de contenido periodístico estas excepciones se dan para prever conflictos que se puedan presentar en el uso de los derechos de libre expresión, protección de orden público y otros.

Según la alcandía de Bogotá los documentos para Habeas Data, Regulación y documentación son los descritos en la Tabla 1.

Tabla 1 Documentos, Regulación y Reglamentación

Documentos para HABEAS DATA : Regulación y Reglamentación		
Año	**Documento**	**Restricto**
2008	Ley 1266 de 2008 Nivel Nacional	En esta ley se encuentran las leyes generales del hábeas data regulando el manejo de la información contenida en bases de datos personales, en especialmente la crediticia, financiera, comercial, de servicios.
2009	Decreto 1727 de 2009 Nivel Nacional	Da indicaciones de como los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios deben presentar la información de los titulares.
2010	Decreto 2952 de 2010 Nivel Nacional	Reglamenta los artículos 12 y 13 de la Ley 1266 de 2008 "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países".
2012	Ley 1581 de 2012 Nivel Nacional	Desarrolla el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar la información que se hayan recogido sobre ellas en bases de datos o archivos, definiendo su ámbito de aplicación, sus principios rectores, las categorías especiales de datos, forma de realizar el tratamiento de los datos, derechos de los titulares de la información, en que situaciones es necesaria la autorización del titular y cuando no, los deberes de información del titular, el derecho a corregir la información, deberes de los responsables del tratamiento de los datos, la Superintendencia de Industria y Comercio, será la autoridad de velar por los deberes de los responsables del tratamiento de datos.

Tabla 1. (Continuación)

2012	Sentencia 458 de 2012 Corte Constitucional	Solicitud para que el certificado de antecedentes judiciales. Que dice: "registra antecedentes, pero no es requerido por autoridad judicial" sea eliminación de dicha anotación ya que se considera que se vulnera los derechos al habeas data, a la intimidad, al buen nombre, a la honra, a la igualdad, al debido proceso, al mínimo vital y al trabajo. Desde la ley se considera los antecedentes penales como datos personales en la medida en que, asocian una situación determinada con una persona natural. Estos datos personales son propios y exclusivos de la persona. En este sentido el habeas data faculta al sujeto a conocer, actualizar, rectificar, autorizar, incluir, excluir, etc., su información personal cuando se encuentre en una base de datos.
2013	Decreto 1377 de 2013 Nivel Nacional	Es una reglamentación parcial de la Ley 1581 de 2012, en ella se encuentran generalidades sobre la protección de datos personales. "Asimismo, señala lo relacionado con el tratamiento de datos en el ámbito personal o doméstico, definiciones, autorización, políticas de tratamiento, ejercicio de los derechos de los titulares, transferencias y transmisiones internacionales de datos personales y responsabilidad demostrada frente al tratamiento de datos personales".
2014	Decreto 886 de 2014 Nivel Nacional	Reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al RNBD, Se debe realizar la inscripción de todas las bases de datos que contengan datos personales así sean personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano o fuera de él, en este último caso, siempre que al Responsable del Tratamiento o al Encargado del Tratamiento se le apliquen las leyes colombianas en virtud de normas y tratados internacionales. En esta ley se establecen reglas sobre la obligación ante el tratamiento de los datos personales, consulta por parte del titular, información mínima, responsables, encargados, canales para ejercicio de derechos, nombre y finalidad, formas y política de tratamiento, plazos de inscripción, sanciones, entre otras disposiciones.
2018	Decreto 090 de 18 de enero	Disminuye la cantidad de empresas vigiladas, excluyendo las empresas y sociedades sin ánimo que sean micro y pequeñas empresas así como personas naturales, aumenta el plazo máximo del RNBD hasta el 31 de enero del 2019.

Fuente: http://www.alcaldiabogota.gov.co/sisjur/listados/tematica2.jsp?subtema=20798

3. METODOLOGÍA

3.1. TIPO DE INVESTIGACIÓN

Este proyecto utiliza la Investigación Aplicada en el análisis de los datos personales que maneja la empresa Infrarom SAS, y el método descriptivo, el cual se utiliza para recoger, organizar, presentar, analizar los resultados de las observaciones de las bases de datos y documentos físicos, para clasificar de esta manera los datos que se consideran personales, sensibles o de tratamiento especial. Este método implica la recopilación y presentación sistemática de los datos para dar la idea clara de la situación expuesta en la Ley 1581 de protección de datos personales. La ventaja que tiene este estudio es que la metodología es fácil de corto tiempo y económica.

3.2. DISEÑO DE INVESTIGACIÓN

El diseño utilizado en esta investigación aplicada, práctica con enfoque diagnóstico, según Sampieri (2007), donde se utiliza los conocimientos adquiridos en la Especialización de Seguridad de la Información, en beneficio de la seguridad de los datos personales de clientes, proveedores y empleados de la empresa INFRAROM SAS, esta investigación se realiza a través de entrevistas, formatos de recolección y cuestionarios, donde se establece la problemática del tratamiento de los datos por falta de buenas prácticas en seguridad, y es motivo de estudio de esta investigación.

Los pasos a seguir en el diseño de la investigación para la implementación de la Ley 1581 de 2012 y el posterior RNBD son, recolección de información sobre los datos personales manejados en las bases de datos digitales y físicos de la empresa INFRAROM SAS, clasificación y etiquetado en sensibles, privados, semi-privados y públicos, determinando las políticas de seguridad que se requieren para cada tipo de dato; creación e implementación de políticas, manuales, formatos y actas que garanticen la seguridad de la información y por

último Registro de las bases de datos ante la Superintendencia de Industria y Comercio.

3.3. POBLACION DE MUESTRA

La población de muestra será toda la empresa Infrarom SAS, ya que es una empresa pequeña que cuenta con 12 empleados incluyendo administrativos y operativos, es una población pequeña que permite realizar el proyecto con facilidad.

3.4. FUENTES DE INVESTIGACIÓN

La información primaria utilizada en esta investigación se obtuvo a través de los datos recolectados por medio de entrevistas y diligenciamiento de formatos para identificar los datos personales de clientes, proveedores y empleados que se encuentran en las bases de datos tanto físicas como digitales de la empresa INFRAROM SAS.

Las fuentes secundarias que se utilizaron en esta investigación fueron obtenidas de investigaciones anteriores en temas relacionados a la protección y tratamiento de datos personales, tema que en la actualidad ha adquirido una gran importancia para defender los derechos a la intimidad, la dignidad y el buen nombre. Estas investigaciones fueron tomadas de fuentes confiables como investigaciones de universidades, tesis, revistas relacionadas con la temática y leyes que existen en Colombia sobre el tema.

3.5. TECNICAS E INSTRUMENTOS DE RECOLECCIÓN DE LA INFORMACIÓN

Se utilizarán los siguientes formatos para la recolección de la información que luego será analizada y clasificada para el manejo de datos personales de la

compañía y de este modo poder establecer el manual y las políticas de Tratamiento de Datos y Protección de Datos Personales.

La técnica utilizada será la entrevista.

Los formatos que se van a utilizar para la recolección de los datos se reúnen en las Tabla 2, donde se recopila los datos personales de los empleados, que serán utilizados para cláusulas de contratos de privacidad, creados para la posterior firma, en la Tabla 3 se identificarán todos los responsables del tratamiento de datos, en ellos podemos identificar personas naturales o jurídicas que tienen accesos a las bases de datos que contienen información personal de empleados, clientes o proveedores.

Tabla 2 Identificación de empleados de la empresa

DATOS EMPLEADOS INFRAROM		
Nombres_Empleado	Número de Documento	Tipo de Documento

Fuente: El Autor

Tabla 3 Identificación del Responsable de tratamiento de los Datos

RESPONSABLES DEL TRATAMIENTO DE DATOS					
Nombre Encargado	Tipo	N° Documento	Departamento	Ciudad	Dirección

Fuente: El Autor

3.4. METODOLOGÍA DE DESARROLLO

En el Anexo A “Recolección de Datos para la adaptación a la Ley de Protección de datos”, se recolectará información para la creación de las políticas, manuales

y contratos que serán creados, como logo de la empresa, razón social, responsable del tratamiento de datos, Nit, información general de la empresa, correo electrónico que será usado para recibir o enviar información acerca de la protección de datos, actividad económica, canales de atención para el tratamiento de los datos entre otros.

Después de recolectar los datos principales de la empresa entramos a determinar las bases de datos que se tienen, para clasificarlos podemos ver las distintas bases de datos en el Anexo B “Clases de Bases de Datos” se encuentra un listado de las bases de datos más comunes encontradas en las empresas, donde se puede determinar que bases utiliza la empresa para clasificar la información.

Cuando ya se tiene identificados los datos personales que tiene la empresa, y clasificadas en las diferentes bases de datos se debe determinar la finalidad con la que se recolectó el dato para poder pedir la autorización de su tratamiento de acuerdo a la finalidad determinada, en el Anexo C “Finalidades para las bases de datos según la SIC” se encuentran un listado de finalidades que pueden ayudar a identificar cuales sirven en cada caso.

Identificando las bases de datos y las finalidades que se tienen para la recolección del dato, se inicia a diligenciar el formulario de cada base de datos identificando si la información está automatizada o física y número de titulares de la base de datos, información que contiene cada una de las bases de datos y responsable del tratamiento de datos, finalidades y seguridad implementada para los datos recolectados. Este formulario se encuentra en el Anexo D “Formato de recolección de información de bases de datos.”

4. RESULTADOS

4.1. BASES DE DATOS EMPRESA INFRAROM SAS

Después de realizar la recolección de la información en la empresa Infrarom SAS, se diligenció la información sobre las bases de datos encontradas en la empresa.

El objetivo principal de este trabajo es cumplir con el artículo 4 literal g) de la Ley Estatutaria 1581 de 2012, de Protección de Datos, donde INFRAROM SAS, es el directo responsable del tratamiento de datos personales, para dar cumplimiento con la norma, se debe implementar diferentes medidas administrativas, técnicas y humanas que garanticen la seguridad de los datos personales, evitando de esta manera el fraude, la adulteración o el uso para discriminación y violación de la integridad.

Para poder realizar el registro se debe cumplir con las normas de seguridad que se establecen en este trabajo. Las normas de seguridad las podemos clasificar en cuatro niveles según si los datos son públicos, semiprivado, privado o sensible. Cada nivel debe ser cumplido de forma acumulativa y será descrito en la siguiente tabla. (Tabla 4)

Tabla 4 Tipos de Datos y Niveles de Seguridad

Tipos de Datos	Descripción	Nivel de Seguridad
Público	Se consideran públicos los datos que se encuentran en documentos que puede acceder todo el mundo como sentencias judiciales que no se encuentran en reserva y el estado civil de las personas.	Público – semiprivado
Semiprivado	Dentro de los datos semiprivados se encuentra la información crediticia, comercial, financiera y de servicios (reportes positivos y negativos)	Público – semiprivado

Tabla 4 (Continuación)

Privado	Son aquellos datos que por su carácter reservado e íntimo le interesa solo al titular como son correos electrónicos y números de teléfono personal; datos laborales, datos financieros y entidades gestoras, seguridad social, bases de datos de patrimonio, créditos, evaluaciones de personalidad, etc.	Privado
Sensible	Son aquellos datos personales de especial protección por lo que pueden afectar la intimidad del titular y generar discriminación entre ellos tenemos: datos biométricos, huellas, iris, datos sindicales, creencias e ideologías, religión, raza, etnia, vida sexual, datos que sean recogidos sin consentimiento para fines policiales, entre otros.	Sensible

Las bases de datos que se encuentran en la empresa pueden ser automatizadas, se encuentran en computadores o servidores y físicas las que tenemos en archivos de la empresa dependiendo de esto se adoptan diferentes medidas de seguridad.

En la Tabla 5 se muestra los niveles de seguridad y el de tratamiento de las bases de datos almacenas en INFRAROM SAS.

Tabla 5 Bases de Datos y Nivel de Seguridad

Base de datos	Seguridad	Sistema de tratamiento	Registros
EMPLEADOS ACTIVOS	Sensible	Computador Archivo propio Interno	12
CLIENTES ACTIVOS	Privada	Computador. Archivo propio Interno	10

Tabla 5 (Continuación)

PROVEEDORES	Privada	Computador. Archivo propio Interno	25
EMPLEADOS RETIRADOS	Sensible	Computador. Archivo propio Interno	6
CLIENTES INACTIVOS	Privada	Computador. Archivo propio Interno	11
CLIENTES PROSPECTO INTRANET	Público	Computador Comercial	100
CLIENTES PROSPECTO OTROS	Público	Computador Comercial	450
CORREOS CORPORATIVOS	Semi privado	Computador Administrativo	8

Al tener recopilado los datos que maneja la empresa INFRAROM SAS se establecen las medidas de seguridad que se deben tener en cuenta para el almacenamiento de todo tipo de datos ya sean privados, semiprivados, públicos y sensibles.

En soportes y gestión de documentos se deben tomar normas de seguridad que nos garantice que no hay recuperación o acceso indebido a datos eliminados, destruidos o borrados., se deben contar con medidas que no permitan el acceso al lugar donde se encuentran los archivos con los datos, se debe contar con formatos para la salida de documentos ya sean físicos o electrónicos, crear un sistema de identificación o etiquetado del tipo de información.

Con relación al control de acceso debe ser específico a los datos que necesita el usuario para el desarrollo de su trabajo, por esto se debe mantener actualizados los usuarios y el perfil de cada uno con los accesos autorizados, se debe implementar mecanismos de control de acceso a los sitios donde se

encuentre la información, archivadores ubicados en áreas de acceso con llave u otras medidas de seguridad, definición de perfiles de usuarios, cifrado de datos, registro de accesos y controles del responsable de administrar la base de datos

Cuando ocurre una incidencias se debe registrar identificando tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras, procedimiento de notificación y gestión de incidencias, registrar los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados, datos grabados manualmente, tener la autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.

Se elabora e implementa el manual interno de seguridad de cumplimiento obligatorio para el personal, teniendo en cuenta el ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, identificación de los encargados del tratamiento y controles periódicos de cumplimiento

Se establecen políticas de archivo, almacenamiento y custodia de documentos, siguiendo procedimientos que garanticen una correcta conservación, localización y consulta y permitan el ejercicio de los derechos de los titulares, dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas, contra con registro de entrada y salida de documentos y soportes; fecha, emisor y receptor, número, tipo de información, forma de envío, responsable de la recepción o entrega.

Identificación y autenticación usuarios para acceder a los sistemas de información y verificación de su autorización, se debe tener mecanismos de identificación y autenticación; contraseñas: asignación, caducidad y almacenamiento cifrado, todos los acceso a datos deben realizarse mediante redes seguras, mecanismos que limiten el número de intentos reiterados de acceso no autorizado.

Se deben realizar auditorías ordinarias (interna o externa) cada dos meses, auditoria extraordinaria por modificaciones sustanciales en los sistemas de información, realizar un informe de detección de deficiencia y propuestas de corrección y realizar un análisis y conclusiones del responsable de seguridad y del responsable del tratamiento

Responsable de seguridad de la información designación de uno o varios responsables de administra las bases de datos, designación a uno o varios encargados del control y la coordinación de las medidas del manual interno de seguridad, prohibición de delegación de la responsabilidad del responsable del tratamiento en los responsables de administrar las bases de datos.

A continuación, se exponen y describen las medidas de seguridad mínimas implantadas por INFRAROM SAS que están recogidas y desarrolladas en su Manual Interno de Seguridad.

Las bases de datos encontradas en Infrarom SAS se describen a continuación, como responsable del tratamiento de datos quedo la persona jurídica Infrarom SAS, con dirección establecida en cámara y comercio como Diagonal 128B Bis No. 56D -20 Oficina 101, de Bogotá, el teléfono que quedó radicada es el número fijo de la empresa 3819905. Como Oficial de Protección de Datos quedo la señora Paula Yamile Sarmiento Gamboa, identificada con C.C. 52498781 cuyo cargo es directora administrativa, el correo creado para cualquier solicitud referente a protección de datos es: protecciónde datos@infrarom.com

Dentro de las bases de datos identificadas en Infrarom SAS, encontramos las siguientes:

1. Empleados Activos: esta base de datos está constituida por 12 registros que son las empleados con los que cuenta la compañía en estos momentos, contiene diversa información del empleado, como datos de menores (hijos), número de cédula, todos los datos que reunimos para la contratación del empleado, en donde podemos destacar que la finalidad de tener esta información es

administrativa, para afiliaciones y de recursos humanos para procesos de selección del empleado, esta maneja datos de tipo sensible por lo cual se deben tener unas medidas de seguridad de la información más estrictas que con otras bases de datos, esta información se encuentra digitalizada en el equipo administrativo y física en archivador bajo llave.

2. Clientes Activos esta base de datos contiene la información de nuestros clientes que se encuentran en este momento contando con nuestros servicios, tiene 10 registros y la principal finalidad de esta base de datos es comercial y de fidelización de clientes, la información que se maneja en ellas es de tipo pública, semi – privada y privada, se encuentra de forma digital en el equipo de la dirección operativa y comercial; además física que se encuentra en archivador bajo llave en la oficina administrativa.

3. Proveedores esta base de datos contiene 25 registros que contienen la información más importante de nuestros proveedores, esta información fue recolectada para fines principalmente comerciales, la información que se maneja es de tipo privada y se encuentra en archivo digital en el equipo administrativo.

4. Empleados retirados: esta base de datos contiene 6 registros con información sensible que se recolecto con finalidad administrativa, recursos humanos, gestión de nómina y gestión de personal; la información que se maneja en esta base de datos es de tipo sensible ya que posee fotografías, huellas, información de menores de edad entre otras, esta información se encuentra en el equipo de cómputo de administración y en un archivo físico bajo llave.

5. Clientes Inactivos esta base de datos contiene la información de nuestros antiguos clientes que ya no se encuentran en este momento con nuestros servicios, tiene 11 registros y la principal finalidad de esta base de datos es comercial y de fidelización de clientes, la información que se maneja en ellas es de tipo pública, semi – privada y privada, se encuentra de forma digital en el equipo de la dirección operativa y comercial; además física que se encuentra en archivador bajo llave en la oficina administrativa.

6. Clientes Prospecto intranet esta base de datos contiene 100 registros, es información que se ha recolectado a través del área comercial, contiene datos públicos de personas jurídicas como NIT, representante legal, teléfono de la empresa, dirección de la empresa, la principal finalidad de la recolección de esta información es comercial, se encuentra de forma digital en el equipo de comercial.

7. Clientes Prospecto esta base de datos contiene 450 registros, es información adquirida en Cámara y Comercio para el grupo comercial, contiene datos públicos de personas jurídicas como NIT, representante legal, teléfono de la empresa, dirección de la empresa, la principal finalidad de la recolección de esta información es comercial, se encuentra de forma digital en el equipo de comercial.

8. Correos corporativos esta base de datos contiene 8 registros de los correos asignados a los empleados de la empresa, la información se considera semi-privada, contiene nombre, correo y algunos datos del usuario, esta información se encuentra digital en equipo de cómputo del área operativa.

Después de la recolección de la información de las bases de datos donde se contenga información personal de empleados, clientes, proveedores; analizando el tipo de información que contienen sea sensible, privada, semiprivada o pública; se procede a realizar una matriz de riesgos encontrados en la empresa, esto se realiza a través de una encuesta realiza al personal de la empresa Infrarom SAS, que se encuentra en el Anexo E identifican los riesgos encontrados el peligro, la evaluación del riesgo y las medidas de control tomadas.

Entre los riesgos encontrados en la empresa están los siguientes, los cuales representan un peligro bajo pero del cual se deben tomar medidas de control.

- No se cuenta con unas directrices claras acerca del control documental de la organización.
- Falta de capacitación al personal para manejo de datos y documentos.

- No se conoce los requisitos legales aplicables a los documentos y tratamiento de datos.
- No se cuenta con canales de comunicación adecuados
- Los documentos y datos no son controlados por un colaborador que tenga una responsabilidad definida para velar por la adecuada distribución, acceso, confidencialidad y restricciones de los mismos.
- No se tiene documentado cuales son las personas que deben conocer el documento o la información.
- No se controla el acceso a los documentos físicos a través de archivadores con llaves u otro mecanismo que garantice la restricción del acceso a la información y documentos en las diferentes oficinas, despachos e instalaciones.
- Diferentes funcionarios de cada oficina distribuyen a su criterio, información, comunicaciones y documentos

4.2. DISEÑAR POLÍTICAS DE SEGURIDAD, MANUALES DE PROCEDIMIENTOS Y RECOMENDACIONES

4.2.1. Políticas internas de seguridad (Infrarom SAS)

Objetivo

Fijar controles en las actividades que se desarrollan en INFRAROM SAS para que los involucrados en la operación garanticen el uso adecuado de los sistemas de información a los que tienen acceso.

También establecer las medidas de control que deben tener los empleados y personas que tienen acceso a la información de INFRAROM SAS, permitiendo establecer niveles de seguridad que mantienen la información de forma confiable, integra y disponible, construyendo las políticas de seguridad aplicadas al sistema de información, instalaciones, redes y y lugares donde se realiza el proceso, almacenamiento y transmisión.

De acuerdo con los estándares internacionales de seguridad (ISO 27001:2013), la Ley 1581 de 2012 y los aspectos establecidos por la Superintendencia de Industria y Comercio por medio de la guía para la implementación del principio de responsabilidad.

La empresa cuenta con factores de riesgo asociados a las faltas de medidas de seguridad que pueden ocasionar fraudes o acciones de personas maliciosas que pongan en riesgo la información.

Objetivos específicos

- Capacitar al personal de INFRAROM SAS en seguridad de la información, para crear una cultura de compromiso y adopción de buenas prácticas en el reporte de incidentes de seguridad e identificación de riesgos.
- Disminuir los riesgos asociados a la seguridad de la información en INFRAROM SAS.
- Implementar sistemas que garanticen y fortalezcan la seguridad de la información.
- Desarrollar e implementar un modelo de seguridad de la información que se ajuste a la empresa.
- Identificar la conducta a seguir en relación con el uso, manejo, acceso y administración de los recursos de información.
- Determinar los responsables de los activos de la información que aseguren el cumplimiento de las políticas establecidas.

Base legal y ámbito de aplicación.

INFRAROM SAS, con el objetivo de dar garantía a un adecuado cumplimiento de la Ley Estatutaria 1581 de 2012 de Protección de Datos (LEPD) y del Decreto 1377 de 2013, crea un Manual Interno de Seguridad que recoge todas las medidas administrativas, humanas y técnicas necesarias para la seguridad de los registros con el fin de impedir el uso inadecuado, consulta, modificación, pérdida o acceso no autorizado, de acuerdo con el principio de seguridad recogido en el artículo 4 de la LEPD.

Este manual se aplica a las bases de datos encontradas y de responsabilidad de INFRAROM SAS, incluyendo los equipos y sistemas de información que se emplean en el tratamiento de los datos, siguiendo las normas vigentes que aplican para todas las personas que participan para el tratamiento de los datos, ya sea usuarios, socios, proveedores o entes de control que tengan acceso a cualquier activo de información sin importar si son internos o externos.

La seguridad de la información es un deber de todas las personas que tienen acceso a ella, dando cumplimiento a las políticas, entendiendo y asumiendo el rol establecido para la protección de la información.

En cualquier situación en la que se comprometa la integridad, confidencialidad y disponibilidad de la información provocará una acción disciplinaria, o la cancelación del contrato laboral por justa causa, también puede ocasionar un proceso judicial bajo sin perjuicio de acciones civiles y/o penales a que haya lugar.

Clasificación de la información.

Publica: Información contenida en registros públicos a la cual pueden tener acceso todas las personas sin necesidad de ninguna autorización. Datos como oficio, profesión, estado civil, NIT; estos datos son encontrados en documentos públicos.

Interna: El acceso a la información interna depende de la organización que requiera el cumplimiento de las actividades diarias implícitas en las responsabilidades del cargo o la prestación del servicio, deben ser de carácter general; la disponibilidad a terceros es de carácter contractual que exprese la necesidad de su uso, con el compromiso a no divulgarla.

Confidencial: La información confidencial solo está disponible para los empleados autorizados por INFRAROM SAS y no pueden otros empleados o terceros tener acceso a ella sin una autorización previa del responsable de administra la base de datos.

Reservada: A la información reservada solo tiene acceso un personal específico, ya que, su uso indebido pude causar daño a la reputación, afectar la intimidad o causar discriminación, ya sea, por pertenecer a determinado grupo étnico, religioso, orientación política, filosófica, partido de oposición, condición de salud, inclinación sexual o datos biométricos entre otros.

Cumplimiento y actualización.

Todos los empleados y terceros que tengan relación con INFRAROM SAS, deben cumplir de forma obligatoria con las políticas de seguridad aplicadas al sistema de información donde se encuentren bases de datos que contengan información personal.

Las políticas de seguridad deben revisarse y actualizarse cada vez que se presente un cambio en las bases de información, en el tratamiento de datos, en el responsable de la información, que pueda afectar la seguridad de la misma; como también debe adaptarse a los cambios que presente la ley.

Medidas de seguridad, bases de datos automatizadas y físicas.

En gestión de documentos y soportes se deben tomar medidas que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos., acceso restringido al lugar donde se almacenan los datos, automatización del responsable para la salida de documentos o soportes por medio físico o electrónico, se debe crear un sistema de etiquetado o identificación del tipo de información, tener un inventario de soportes
Con relación al control de acceso debe ser limitado a los datos necesarios para el desarrollo de sus funciones con una lista actualizada de usuarios y accesos autorizados, se implementan mecanismos para evitar el acceso a datos con derechos distintos de los autorizados, se implementa control de acceso al lugar o lugares donde se ubican los sistemas de información, archivadores ubicados en áreas de acceso protegidas con llaves u otras medidas, definición de perfiles de usuarios, cifrado de datos, registro de accesos y controles del responsable de

administrar la base de datos

Cuando ocurre una incidencia se debe registrar identificando tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras, procedimiento de notificación y gestión de incidencias, registrar los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados, datos grabados manualmente, tener la autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.

Se elabora e implementa el manual interno de seguridad de cumplimiento obligatorio para el personal, teniendo en cuenta el ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, identificación de los encargados del tratamiento y controles periódicos de cumplimiento

Se establecen políticas de archivo, almacenamiento y custodia de documentos, siguiendo procedimientos que garanticen una correcta conservación, localización y consulta y permitan el ejercicio de los derechos de los titulares, dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas, contra con registro de entrada y salida de documentos y soportes; fecha, emisor y receptor, número, tipo de información, forma de envío, responsable de la recepción o entrega.

Identificación y autenticación usuarios para acceder a los sistemas de información y verificación de su autorización, se debe tener mecanismos de identificación y autenticación; contraseñas: asignación, caducidad y almacenamiento cifrado, todos los acceso a datos deben realizarse mediante redes seguras, mecanismos que limiten el número de intentos reiterados de acceso no autorizado.

Se deben realizar auditorías ordinarias (interna o externa) cada dos meses,

auditoria extraordinaria por modificaciones sustanciales en los sistemas de información, realizar un informe de detección de deficiencia y propuestas de corrección y realizar un análisis y conclusiones del responsable de seguridad y del responsable del tratamiento

Responsable de seguridad de la información designación de uno o varios responsables de administra las bases de datos, designación de uno o varios encargados del control y la coordinación de las medidas del manual interno de seguridad, prohibición de delegación de la responsabilidad del responsable del tratamiento en los responsables de administrar las bases de datos.

Funciones y obligaciones del personal.

Las personas que participen en las funciones de almacenar, consultar o realizar tratamiento de los datos personales y del sistemas de información de INFRAROM SAS, deben cumplir las funciones y obligaciones que se describirán a continuación

INFRAROM SAS, tiene la obligación de dar a conocer a su personal las medidas y normas de seguridad que deben tener en el desarrollo de sus funciones, y debe informar las sanciones a las cuales se expone por el incumplimiento de la norma, debe transmitir esta información por algún medio masivo como correo electrónico o cartelera de anuncios que garantice el suministro de la información. El documento y manual de seguridad debe estar publicado para que los empleados tengan acceso y se pueda dar a conocer las normas de seguridad y las obligaciones que deben tener según el cargo que ocupan.

INFRAROM SAS generará los acuerdos de confidencialidad que serán anexados al contrato de sus empleados informando el deber de secreto que suscriben, sobre bases de datos y sistemas de información de la empresa.

Si los empleados previamente informados sobre el manual de seguridad de la información y sus acuerdos de confidencialidad incumplen con las obligaciones

establecidas será sancionable de acuerdo a la normativa aplicable a la relación jurídica existente entre el usuario y INFRAROM SAS.

Se establecen las siguientes funciones y obligaciones que deben tener los empleados con las bases de datos personales que estén bajo su responsabilidad:

Deber de secreto: Este deber es aplicado a todos los empleados y proveedores que tengan acceso a las bases de datos personales, en cumplimiento de este deber, los usuarios de INFRAROM SAS deben evitar que la información personal de bases que manejen o de los que tengan conocimiento en el desempeño de su labor, sean conocidas por terceros, y debe velar por que la información sea confidencial e integra.

Funciones de autorizaciones delegadas: INFRAROM SAS puede contratar a terceros que manejen el tratamiento de datos, para que actúen como encargados del tratamiento, esto se debe realizar mediante la firma de un contrato de transmisión de datos.

Se debe contar con la autorización del responsable del tratamiento de los datos personales para acceder o extraer información de la empresa, asegurando no revelar información a terceros, ni a personal no autorizado garantizando que las acciones realizas no ponen en peligro la seguridad de la información.

Uso de recursos y materiales de trabajo: El material de trabajo debe ser utilizado para fines estrictamente laborales y no para uso personal, si para su labor es necesario sacar información en dispositivos extraíbles se debe contar con la autorización de los responsables de la información.

Al imprimir o escanear documentos que contengan datos personales deben ser tratados con confidencialidad, recogidos y borrados de las carpetas donde queden guardados donde puedan tener acceso terceros que no estén autorizados de su manejo.

Obligación de notificar incidencias: Los empleados deben informar las incidencias que se presenten con los datos personales que se encuentran en su custodia a los responsables de administrar las bases de datos u Oficial de

protección de datos, los cuales se deben encargar de resolver, gestiona o notificar. Entre las incidencias están caídas de los sistemas de información, el intento no autorizado de la salida de un documento o soporte, la pérdida de datos la destrucción intencional o sin ella de datos o soportes, el cambio de ubicación de bases de datos, adquisición por parte de terceros de contraseñas, la modificación no autorizada de datos, entre otros. Todas estas incidencias deben quedar registradas con fecha, tipo de incidencia, responsable y gestión.

Responsabilidad de los portátiles y equipos de trabajo: Los empleados deben hacerse responsables de su equipo de trabajo; debe bloquear el equipo cuando no esté frente a él o se desplace a algún lugar, deben tener contraseñas que cumplan con las medidas de seguridad establecidas por la empresa, de esta manera se impide el acceso a la información que contiene; los equipos deben apagarse al terminar la jornada laboral.

Normas del uso de Internet y correo electrónico: El empleado tendrá permiso de navegación dependiendo de sus funciones, los correos externos o almacenamientos en la nube que puedan causar salida de información estarán bloqueados por seguridad de INFRAROM SAS.

Protección de contraseñas: Las contraseñas que se entregan a los empleados son temporales y deben ser cambiadas en el primer ingreso, las contraseñas colocadas deben cumplir con estándares de seguridad, mínimo 8 caracteres entre mayúsculas, minúsculas, números y caracteres especiales, no deben tener relación con los nombres del empleado, estas son personales e intransferibles, por lo que se prohíbe su divulgación o comunicación a compañeros de trabajo o personas no autorizadas, el sistema pide cambio de contraseña cada mes, no se puede usar contraseñas ya utilizadas. Cuando sea necesario restaurar o recuperar la contraseña, el usuario debe comunicarlo al administrador del sistema.

Recuperación de datos y respaldos: Cumplir con las normas de seguridad para la generación de backups y datos de respaldo.

Procedimiento de notificación, gestión y respuesta ante incidencias.

Con el objeto de garantizar la confidencialidad, disponibilidad e integridad de la información contenida en las bases de datos bajo la responsabilidad de INFRAROM SAS, se establece un proceso de notificación, gestión y respuesta de incidencias.

Se debe dar a conocer a todos los empleados y personas que estén a cargo del tratamiento de datos personales de la forma a proceder ante cualquier incidencia.

El procedimiento de notificación, gestión y respuesta ante incidencias es el siguiente: A penas se identifique la incidencia ya sea perdida, hurto y/o acceso no autorizado que involucre la confidencialidad, integridad y disponibilidad de los datos y sistema de información se debe comunicar de manera inmediata al Oficial de Protección de Datos, debe diligenciarse un formato reportando el tipo de incidencia, el posible responsable de la incidencia, la fecha y hora, la persona que notifica la incidencia, la persona a quién se le comunica y los efectos que ha producido. Después de la comunicación se debe solicitar un recibido por parte del Oficial de Protección de Datos en el que conste la notificación de la incidencia con todos los requisitos enumerados anteriormente. INFRAROM SAS, tiene un registro de incidencias que debe contener: el tipo de incidencia (Fraude Interno o externo, Daños a activos físicos, Fallas tecnológicas, Ejecución y administración de procesos), fecha y hora de la misma, persona que la notifica, persona a la que se le comunica, efectos de la incidencia y medidas correctoras cuando corresponda. Este registro es gestionado por el Oficial de Protección de

Datos, formato de registro de incidencias y plan de acción.

Cuando se requiere medidas correctivas se debe realizar los procedimientos para la recuperación de los datos, se debe registrar quien ejecuta el procedimiento, que datos son restaurados y recuperados: el Oficial de Protección de Datos debe informar a la Superintendencia de Industria y Comercio, mediante el RNBD dentro de los 15 días hábiles siguientes de haber sido detectado, si el incidente afecta a los titulares INFRAROM SAS les notificará.

Medidas para el transporte, destrucción y reutilización de documentos y soportes.

INFRAROM SAS debe asegurar que la destrucción de cualquier documento que contenga datos personales, se realice implementando medidas que eviten la recuperación a acceso a la información.

Para el traslado de documentos que contengan datos personales se debe realizar cifrado utilizando mecanismos que eviten la manipulación, acceso o pérdida de la información, se debe evitar trasladar datos personales en portátiles fuera de las instalaciones de la empresa, si es necesario, estos datos deben ser cifrados y contar con medidas que garanticen la seguridad de la información.

En el matriz de riesgo se definen los controles a seguir de acuerdo a los riesgos detectados en la organización dentro de la protección de datos personales.

Disposición final.

INFRAROM SAS, aprueba el contenido de este manual, y se hace responsable del tratamiento de datos, el personal de la empresa debe ejecutar y cumplir con las políticas expuestas en él.

4.2.2. Protocolo de atención a titulares (consultas o reclamos)

Objetivo

INFRAROM SAS establece el presente protocolo para dar respuesta a las solicitudes de acceso y reclamos, en virtual de los derechos del titular de la información al acceso, corrección, supresión, revocación o reclamo; objeto de tratamiento por la empresa.

INFRAROM SAS se compromete a difundir el protocolo de atención a titulares, a todas las personas que pertenecen a la empresa y tiene acceso a bases de

datos que contenga información personal y a los titulares de la información sobre los procedimientos establecidos en cada caso.

Derechos del titular:

Los derechos del tratamiento de datos pueden ser realizador por los titulares, acreditando su identidad; representantes o apoderados del titular o por estipulación a favor de otro.

Consulta o acceso: Este derecho obliga al responsable del tratamiento solicitar autorización previa e informar el uso y finalidad que se le ha de dar a sus datos personales.

Reclamos y quejas: el titular podrá realizar reclamos por corrección, cuando necesite actualizar, modificar o rectificar datos que crea inexactos o incompletos o aquellos que no hayan sido autorizados; por supresión, el titular puede suprimir datos que crea inadecuados o que vayan en contra de sus principios y derechos constitucionales; por revocación: el titular puede revocar la autorización dada para el tratamiento de sus datos personales; por infracción: el titular puede exigir remediar el incumplimiento de la norma.

Solicitud de pruebas: el titular tiene el derecho a solicitar la autorización del tratamiento de sus datos, siempre y cuando no sea una excepción prevista en el artículo 10 de la ley de protección de datos.

Quejas por infracción: el titular puede presentar ante la Superintendencia de Industria y Comercio quejas por infracciones una vez haya agotado el trámite de consulta o reclamo ante el responsable del tratamiento.

Atención a los titulares de datos.

Las consultas, peticiones o reclamos serán atendidas por el oficial de protección de Datos de INFRAROM SAS, teniendo como medio de atención el teléfono: 3819905 y el correo electrónico: protecciondedatos@infrarom.com.

Procedimientos para ejercer los derechos del titular.

Consulta o acceso

Según el artículo 2.2.2.25.4.2 del decreto 1074 de 2015 (artículo 21 del decreto 1377 de 2013), el Titular podrá consultar sus datos una vez al mes y cuando requiera realizar modificaciones de las políticas de tratamiento de la información que motiven nuevas consultas. Si requiere consultar más de una vez al mes se cobrará los gastos de envío.

Para ejercer el derecho de consulta INFRAROM SAS a habilitado el correo electrónico protecciondedatos@infrarom.com, donde puede enviar su solicitud indicando en el Asunto "Ejercicio del derecho de acceso o consulta", también a través del correo dirigido a la dirección Diagonal 128B Bis No. 56D -20 Apto 201, BOGOTÁ. En la solicitud deben enviar su nombre y apellido completo, adjuntar fotocopia de la Cédula de Ciudadanía, en caso de solicitarlo el representante debe adjuntar su cédula y un documento que lo acredite como tal, redactar una petición concreta solicitando el acceso o consulta de sus datos personales, incluir una dirección para dar respuesta y la fecha y firma del solicitante.

INFRAROM SAS tiene como plazo diez (10) días hábiles a partir de la fecha de radicada la solicitud, si en este tiempo no puede tender la solicitud, informará al titular los motivos de la demora señalando la fecha en la que se dará respuesta no puede ser mayor a cinco (5) días conforme lo estipula el artículo 14 de la LEPD. Si el trámite de consulta supera dichos plazos el titular podrá poner una queja ante la Superintendencia de Industria y Comercio.

Quejas y reclamos

Para ejercer el derecho de quejas y reclaos INFRAROM SAS ha habilitado el correo electrónico protecciondedatos@infrarom.com, donde puede enviar su solicitud indicando en el Asunto "Ejercicio del derecho de quejas y reclamos", también a través del correo dirigido a la dirección Diagonal 128B Bis No. 56D -20 Apto 201, BOGOTÁ. En la solicitud deben enviar su nombre y apellido completo, adjuntar fotocopia de la Cédula de Ciudadanía, en caso de solicitarlo

el representante debe adjuntar su cédula y un documento que lo acredite como tal, redactar una descripción de la queja o reclamo donde se solicite corrección, supresión revocación o infracción, incluir una dirección para dar respuesta y la fecha y firma del solicitante. Si los documentos requeridos para realizar el reclamo o queja están incompletos, INFRAROMM SAS tiene cinco (5) dias hábiles para requerirle al titular los documentos faltantes, si pasados dos (2) meses de la fecha del requerimiento no se han presentado la información faltante, se entenderá que desistió de la queja o reclamo.

INFRAROM SAS tiene como plazo quince (15) días hábiles a partir de la fecha de radicada la queja o reclamo, si en este tiempo no puede tener respuesta, informará al titular los motivos de la demora señalando la fecha en la que se dará respuesta, no puede ser mayor a ocho (8) días conforme lo estipula el la ley de protección de datos. Si el trámite de consulta supera dichos plazos el titular podrá poner una queja ante la Superintendencia de Industria y Comercio.

Infracciones y sanciones.

En el Capítulo 2 de la Ley Estatutaria 1581 de 2012 de Protección de Datos, la Superintendencia de Industria y Comercio expone las sanciones que pueden ser aplicadas por el incumplimiento de la norma, entre las sanciones están multas aplicadas a la persona o a empresas que pueden llegar a dos mil (2.000) SMLV al momento de la imposición de la sanción. Estas multas podrán ser sucesivas mientras el responsable del tratamiento de los datos siga incumplimiento con la norma que la originó.

Otra sanción impuesta por la norma es la suspensión para realizar las actividades que impliquen el tratamiento por un tiempo de seis (6) meses. Dentro de suspensión se debe indicar los correctivos a seguir. Si se hacen caso omiso a los correctivos correspondientes se realizará el cierre temporal de la operación que tenga relación con el tratamiento de datos personales y en última instancia se dará el cierre inmediato y definitivo.

4.2.3. Manual recomendaciones de seguridad al empleado

Base legal y ámbito de aplicación.

El derecho a la Protección de los Datos tiene como finalidad permitir que las personas conozcan, actualicen y rectifiquen la información recogida sobre ellas en archivos o bases de datos de la empresa. Este derecho constitucional se recoge en los artículos 15 y 20 de la Constitución Política; en la Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la Protección de Datos Personales (LEPD); y en el Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley anterior y compilado en el Capítulo 25 del Decreto 1074 de 2015.

La empresa INFRAROM SAS se hace responsable del tratamiento de datos del titular que ha dado su consentimiento para que estos formen parte de la base de datos y responde por su seguridad, cautela, vela por su integridad y aparece como entidad a la que puede dirigirse en el seguimiento de la información y el control de la misma, garantizando sus derechos a la consulta actualización y reclamo.

El cumplimiento del manual interno de seguridad es responsabilidad de las personas que están a cargo de las bases de datos que contienen información personal deben velar por la implementación de las políticas de seguridad cumpliendo con sus funciones.

INFRAROM SAS cuenta con un equipo de responsables de la seguridad de las bases de datos, que se encarga de desarrollar, coordinar, controlar y verificar el cumplimiento de estas medidas. Este equipo está obligado a cumplir con el acuerdo de confidencialidad, toda vez, que lo ha firmado, suscrito entre el usuario y el responsable del tratamiento; incluso después de finalizar su relación laboral o profesional con la empresa.

Principios de la protección de datos.

Legalidad: La protección y tratamiento de datos personales está reglamentada en la LEPD, el Decreto 1377 de 2013, establecida en el capítulo 25 del Decreto 1074 de 2015.

Finalidad: La finalidad del tratamiento de datos personales debe ser informada al titular para su conocimiento y autorización.

Libertad: El titular tiene el derecho de dar o no el consentimiento del uso de sus datos personales, sin previa autorización no podrán ser divulgados ni tratados excepto cuando la información sea requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial, cuando los datos se consideran públicos, en caso de una emergencia médica o sanitaria, cuando la recolección de datos se realiza con un fin histórico, estadístico o científico, datos que se encuentran en el registro civil de nacimiento.

Veracidad o calidad: La información almacenada en las bases de datos debe contener datos verídicos, completos, exactos, actualizados y comprobables.

Transparencia: El responsable del tratamiento de datos personales debe ser transparente ante la utilización de ellos informando a su titular a que serán sometidos sus datos y su finalidad.

Acceso y circulación restringida: los datos personales solo pueden ser manejados por personas o empresas autorizadas por el titular o por personas que estipule la ley. No deben estar disponibles en las redes de comunicación masiva ni ser divulgación por cualquier medio.

Seguridad: el tratamiento de los datos personales debe realizarse con las medidas de seguridad necesarias para evitar la pérdida, cambio, uso o consulta de personal no autorizado. Los usuarios deben conocer y cumplir con las normas y medidas de seguridad que correspondan a sus funciones que se encuentran expresas en el Manual Interno de Seguridad, las modificaciones deben informarse a todos los usuarios que manejan datos personales.

Confidencialidad: las personas que tengan acceso a los datos personales y que en sus funciones impliquen el tratamiento de ellos, están obligadas a mantener

la confidencialidad de dicha información, incluso si ya no se encuentran en el cargo.

Categorías especiales de datos.

Datos sensibles

Estos datos son de suma importancia ya que su mal manejo puede afectar la intimidad del titular generando discriminación, dentro de estos datos encontramos raza o etnia, la orientación política, religión, filosofía, pertenencia a un sindicatos, pertenencia a una organización sociales o de derechos humanos, así como los datos de salud, orientación sexual y los datos biométricos. Según el artículo 6 de la LEPD, se prohíbe el tratamiento de datos sensibles, excepto cuando: Se tenga autorización escrita del titular del tratamiento de estos datos; se realice el tratamiento de los datos para salvaguardar la vida del titular y él se encuentre impedido física o jurídicamente incapacitado, debe el representante legal dar su autorización; el tratamiento de datos por fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular, para defensa o reconocimiento en un proceso jurídico y en caso de que los datos sean necesarios para una finalidad histórica, estadística o científica.

Funciones y obligaciones.

INFRAROM SAS se hace responsable del tratamiento de los datos, como también, de coordinar e implementar las medidas de seguridad del manual interno de la empresa actualizando y haciendo los cambios pertinentes cuando estos se realicen o si se presenta alguna dificultad y si se corre algún riesgo.

La empresa debe asignar uno o varios responsables de administrar las bases de datos, un oficial de protección de datos que vele por las políticas de seguridad como son: acceso identificado, uso de políticas de contraseñas, obtención de autorización de los titulares de la información, diligenciamiento de formatos para la salida o transferencia de la información, aplicación de políticas para los backup, recuperación de datos y establecimiento de perfiles entre otros.

Cada tres meses se deben analizar las incidencias presentadas para establecer las medidas correspondientes en forma oportuna. Por medio de auditorías internas o externas por lo menos una vez cada dos años, se debe modificar y revisar si se están llevando a cabo todas las medidas de seguridad.

Responsables de administrar las bases de datos

INFRAROM SAS establece como responsables de administrar las bases de datos, Sensibles, no automatizadas y automatizadas a las personas que señala en la Organización Bases de Datos a Paula Yamile Sarmiento Gamboa, directora administrativa de la empresa, como responsable de administrar las bases de datos debe cumplir las siguientes funciones: realizar la implementación de las normas de seguridad, y divulgar el manual interno de seguridad, establecer mecanismos para acceder a la información de forma segura, tramitar los permisos para el ingreso a los datos por parte de los usuarios autorizados identificados en el Manual Interno de Seguridad, realizar un registro de incidencias para que los usuarios comuniquen y registren las incidencias relacionadas con la seguridad de los datos; así como establecer medidas correctivas.

Dentro de sus responsabilidades debe comprobar la validez y vigencia de los usuarios autorizados, la existencia de copias de seguridad para la recuperación de los datos, la actualización del manual interno de seguridad y el cumplimiento de las medidas relacionadas con las entradas y salidas de datos, definir el proyecto de auditorías, internas o externas, recibir y analizar el informe de auditoría para elevar sus conclusiones y proponer medidas correctoras al responsable del tratamiento, gestionar y controlar los registros de entradas y salidas de documentos o soportes que contengan datos personales.

Usuarios

Se denominan usuarios a las personas que participan en el proceso de consultar, almacenar, tratar o cualquier otra actividad relacionada con el sistema de información y los datos personales de INFRAROM SAS, los usuarios deben proceder de acuerdo a las obligaciones y funciones establecidas en el manual y políticas de seguridad de la empresa.

INFRAROM SAS cuenta con acuerdos de confidencialidad donde los usuarios deben cumplir con los deberes de custodia y cuidado de la información y deber de secreto que respaldan, se debe informar a los usuarios mediante una circular informativa sobre su obligación en el manejo del sistema de información y registros en las bases de datos de la empresa.

El personal de INFRAROM SAS cuenta con un manual de obligaciones y funciones definidas según las actividades que desarrollen dentro de la empresa. Se cuenta con un listado de usuarios y perfiles que tienen acceso a los sistemas de información y están consignados en el Manual Interno de Seguridad. Cuando un usuario tiene en su poder soportes o documentos que contengan datos personales debe custodiarlos, vigilar, controlar y garantizar que las personas no autorizadas no puedan acceder a ellos.

Si se incumple las medidas y obligaciones que se encuentran establecidas en el Manual por el personal de INFRAROM SAS, se establecen las sanciones de acuerdo a la norma y a los acuerdos de confidencialidad firmados entre el usuario y la empresa.

INFRAROM SAS determina las siguientes obligaciones y funciones que deben ser cumplidas por los usuarios que manejan bases de datos personales:

Deber de secreto, es aplicada tanto a usuarios como los contratistas que tengan acceso a las bases de datos personales de la empresa, se comprometen a no divulgar o relevar a terceros, los datos de los cuales tienen conocimiento por el desempeño de su oficio, velando siempre por la integridad y confidencialidad de los mismos.

Autorizaciones y control: A través de un contrato de transmisión de datos el responsable de la información puede encargar el tratamiento de datos a un tercero, que sea el encargado del tratamiento. Las obligaciones que debe cumplir este tercero relacionadas con la seguridad de la información son, ingresar a las bases de datos con la autorización y cuando sea necesario para el ejercicio de sus funciones, no puede suministrar información a terceros, ni a usuarios no autorizados, cumplir con las normas de seguridad establecidas y aportar mejoras, poner en peligro la seguridad de la información, no debe extraer información de la empresa sin debida autorización.

Uso de materiales y recursos: los recursos deben utilizarse según las funciones establecidas, no pueden utilizarse para fines personales o diferentes a las tareas que le corresponden a su función. Si por motivos de trabajo se debe extraer de la empresa dispositivos periféricos o extraíbles, se debe comunicar al responsable de seguridad para solicitar una autorización dejándola registrada.

Uso de escáner, impresión o copias: Al utilizar la impresora, copiadora o escáner se debe recoger de inmediato los documentos para evitar el acceso de datos personales a personas no autorizadas.

Notificación de incidencias: toda incidencia que ocurra con el tratamiento de los datos personales debe ser notificada al responsable de seguridad que corresponda, él se encargará de gestionar y resolver la incidencia según el caso. Entre las incidencias encontradas está caída del sistema de seguridad informática donde puede presentarse acceso a los datos personales a personas no autorizadas, sacar documentos sin la debida autorización, perdida o destrucción de los datos, cambios de ubicación en las bases de datos, acceso a contraseñas personales por terceros, la modificación de datos por personal no autorizado, etc.

Responsabilizarse de los equipos y portátiles: los usuarios deben hacerse responsables de su equipo; bloqueando su escritorio cada vez que se ausente, de esta manera impedir el acceso a la información confidencial que contiene; y los equipos deben ser apagados al finalizar la jornada laboral. Los portátiles

deben tener un control de acceso que evite la pérdida o sustracción de la información.

Internet y correo electrónico: solo está autorizado el correo corporativo donde se puede monitorear la información que se envía, los correos personales y externos están bloqueados, y el uso de páginas web están restringidos a la navegación que necesite según su función.

Contraseñas: Al realizar entrega del usuario, se le asignará una contraseña temporal, que deberá cambiar en el primer ingreso, la contraseña es personal e intransferible y se prohíbe su divulgación a personas no autorizadas. Cada contraseña debe cumplir con estándares de seguridad establecidos por la empresa, mínimo ocho caracteres con mayúsculas, minúsculas, números y caracteres especiales, la contraseña debe ser cambiada cada mes, cuando sea necesario restaurar la contraseña, se debe comunicar al administrador del sistema quien le generará otra contraseña temporal, no debe guardar las contraseñas en el equipo.

Copias de seguridad: deben ser programadas y existir una copia de seguridad de las bases de datos personales, aplicando las mismas medidas de seguridad enmarcadas en las políticas de la empresa.

Gestor de documentos y archivo: todos los documentos deben ser debidamente archivados y clasificados teniendo en cuenta las políticas de seguridad que se establecieron en el Manual de Políticas y Procedimiento y en el Manual Interno de Seguridad.

4.2.4. Documentos para la implementación de la ley estatutaria de protección de datos personales 1581 de 2012 y normas reglamentarias.

Dentro de este proyecto se realizó toda la documentación relacionada con los formatos para la implementación de la ley estatutaria de protección de datos Ley 1581 de 2012; estos comprenden:

Políticas:

1. Organización Bases de Datos. Documento de carácter interno que contiene la estructura e información de las bases de datos sujetas a inscripción en el RNBD.

Contratos y acuerdos tipo:

1. Contratos para empleados de confidencialidad y deber de secreto: Acuerdo contractual entre la organización y el empleado que tiene como objeto garantizar la confidencialidad y el deber de secreto de este último respecto de los datos personales a los que accede en el desempeño de sus funciones. DEBE SER SUSCRITO POR TODOS LOS EMPLEADOS.

2. Contrato de Transmisión de Datos (proveedores): Contrato que debe firmar la organización con todas aquellas personas u organizaciones a las que se le suministre o permita acceso a las bases de datos personales que estén bajo su custodia. Para la transmisión de datos se necesita la autorización expresa de los titulares. DEBE SER SUSCRITO CON LOS PROVEEDORES A LOS CUALES ES NECESARIO SUMINISTRAR DATOS PERSONALES DE LAS BASES DE DATOS REGISTRADAS PARA LA PRESTACION DE UN SERVICIO.

3. Contrato de Cesión de Bases de Datos: Modelo de acuerdo para terceros a quienes se le cedan las bases de datos personales. Mediante este acuerdo se indican las características de las bases de datos cedidas, las finalidades y el alcance para el tratamiento de los datos, la organización le informa al cesionario la calidad de Responsable que adoptará y por lo tanto las obligaciones que en delante debe cumplir, eximiéndole de cualquier responsabilidad por el tratamiento que le dé a la información que le será cedida.

Consentimientos y clausulas:

1. Aviso de privacidad: Texto que informa al titular sobre las políticas de tratamiento de datos personales de la organización con el fin de obtener su autorización expresa e informada. Debe incluir los datos de contacto de la organización, la finalidad del tratamiento, los derechos de los titulares de datos

y los mecanismos dispuestos por la organización para el titular conozca las políticas de tratamiento. Debe publicarse en el sitio web.

2. Clausula informativa: Clausula que informa al titular que sus datos serán almacenados en una base de datos y sometidos a tratamiento por parte de la organización. Autorización tácita. Podrá utilizarse en eventos para obtener el consentimiento del titular de los datos a través de planilla de asistencia.

3. Cláusula de consentimiento Web: Clausula que informa al titular de sus datos, que ingresa a la página y deja sus datos para comunicación posterior, la finalidad con la que son recaudados los datos. Debe fijarse en el formulario de contáctenos de la página web.

4. Cláusula de aviso de regularización de las bases de datos anteriores a la aprobación de la ley 1581 del 2012 (Consentimiento Tácito): Clausula que informa a los titulares de los datos contenidos en bases de datos anteriores a la entrega en vigor de la normativa sobre protección de datos sobre los derechos legales de los titulares, la finalidad del tratamiento y las políticas de protección de datos de la organización. Autorización tácita.

5. Cláusula de video vigilancia: Texto que informa al titular sobre las políticas de tratamiento de video vigilancia y monitoreo. Debe fijarse en un lugar visible o acceso donde se han instalado cámaras de seguridad.

6. Consentimiento expreso con transferencia de datos: Cláusula contractual para que los titules autoricen expresamente el tratamiento y la transferencia o transmisión de los datos. Debe ser suscrito por todo los empleados.

7. Consentimiento informado para datos de menores de edad: Cláusula contractual para que los padres o tutores legales autoricen el tratamiento de datos de los hijos o tutorados menores de edad. Debe ser suscrito por todos los empleados cuyos hijos menores de edad que se encuentren afiliados al sistema de seguridad social como beneficiarios o en caso de que por cualquier otro motivo se almacenen los datos del menor.

8. Consentimiento para correos electrónicos: Clausula que la organización introduce en todas sus comunicaciones electrónicas (correos electrónicos) para

garantizar el secreto de la información. Debe fijarse en la firma de todos los correos electrónicos de los empleados.

9. Consentimiento para tratamiento de datos personales: Clausula para que los titulares autoricen el tratamiento de los datos. Debe suscribirse con clientes y proveedores con la finalidades correspondiente a cada caso.

10. Consentimiento para datos sensibles: Cláusula contractual para que los titulares autoricen expresamente el tratamiento de sus datos sensibles. Debe ser suscrito por todos los empleados.

11. Cláusula de datos biométricos: Clausula para que los titulares autoricen que las huellas registradas serán incorporadas en una base de datos. Debe ser suscrito en caso de utilizar datos biométricos, tales como: huella dactilar, imágenes, reconocimiento facial, videos, reconocimiento de retina, voz, etc.

12. Consentimiento expreso para utilización de imágenes personales: Cláusula contractual para que los titulares autoricen el uso exclusivo de imágenes. Debe ser suscrito por los empleados que utilizan carnet con foto que lo identifican como empleado o funcionario de la empresa.

4.3. IMPLEMENTACION DE POLÍTICAS, MANUALES Y FORMATOS

Después de crear todos las políticas, manuales y formatos con todo el equipo de Infrarom SAS y la asesoría de Protecdata, se inició el proceso de capacitación al personal sobre las políticas de tratamiento de datos, recolección de autorizaciones de empleados, clientes, proveedores y demás personas registradas en las bases de datos encontrados, establecimiento de cláusulas en e- mail cooperativos, en contáctenos de la página web, grabación de la ley de tratamiento de datos en el PBX, implementación de medidas de seguridad y medidas de control expuestas en los manuales del punto anterior en toda la organización de las cuales mostramos la evidencia en las siguientes imágenes.

Capacitación a los empleados de INFRAROM SAS sobre los manuales y políticas de seguridad establecidos en la empresa.

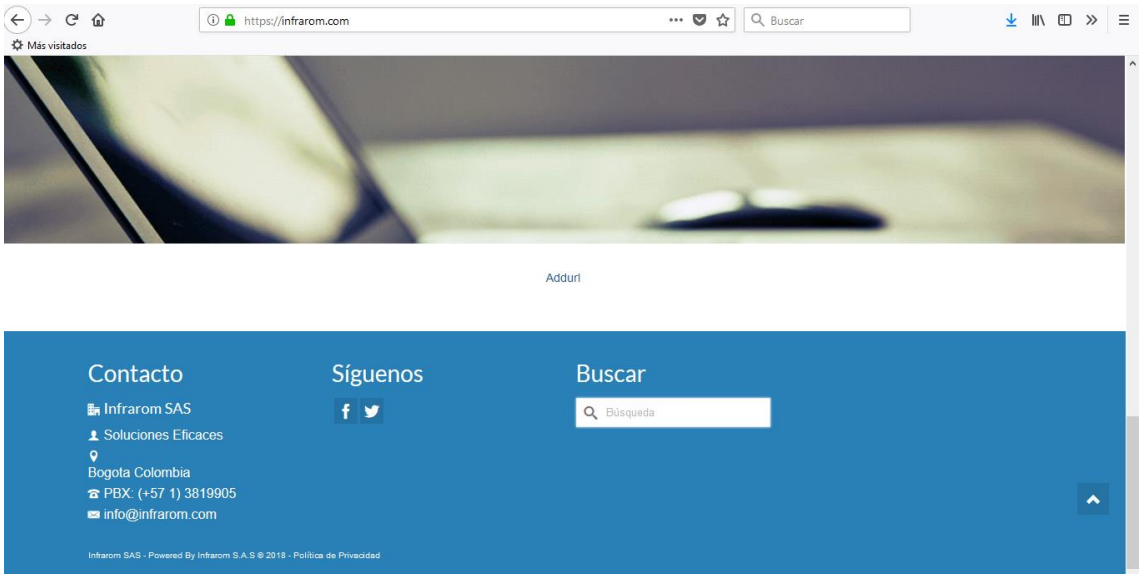
Capacitación de empleados

Fuente: El autor

Autorización y consentimiento de tratamiento de datos en los formularios que se encuentran en la página web de INFRAROM SAS

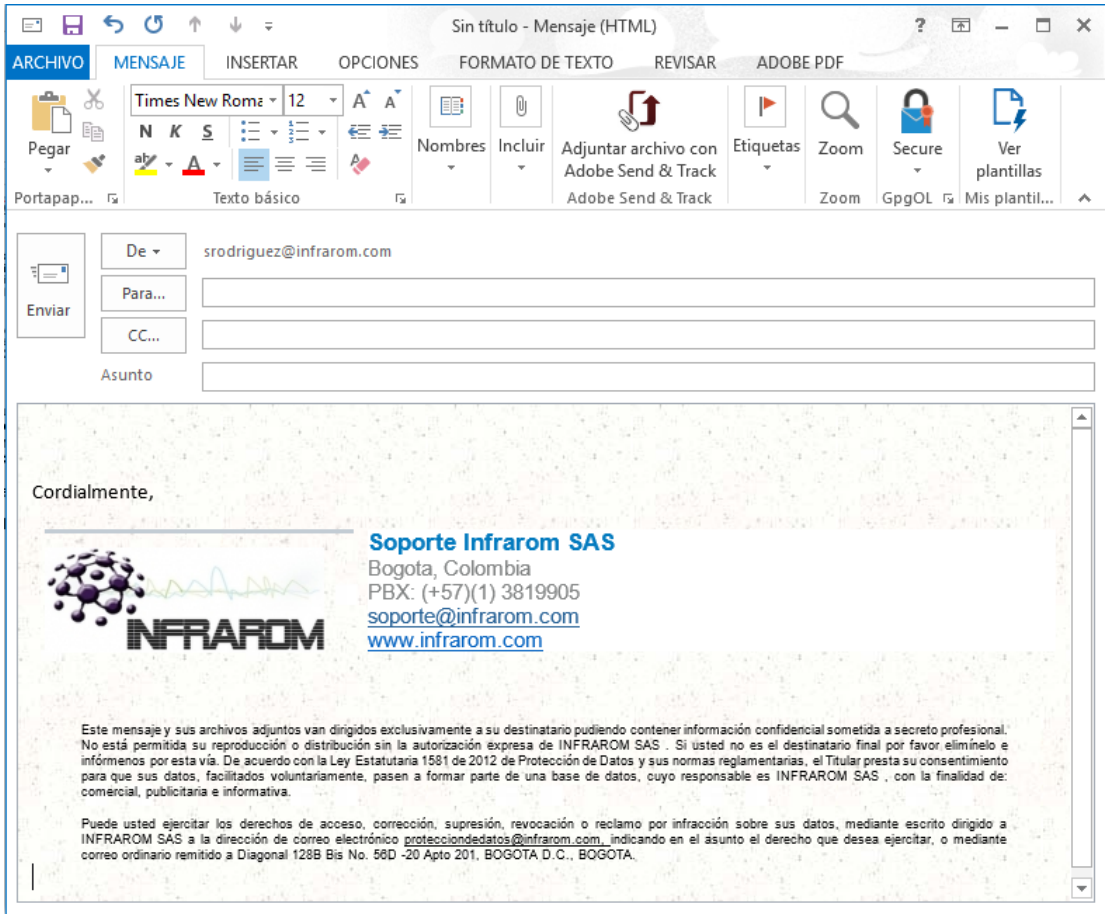
Fuente: El autor

Políticas de seguridad y publicadas en la página para que sean consultadas tanto por los empleados como por usuarios o personas externas que tengan alguna solicitud sobre los datos personales



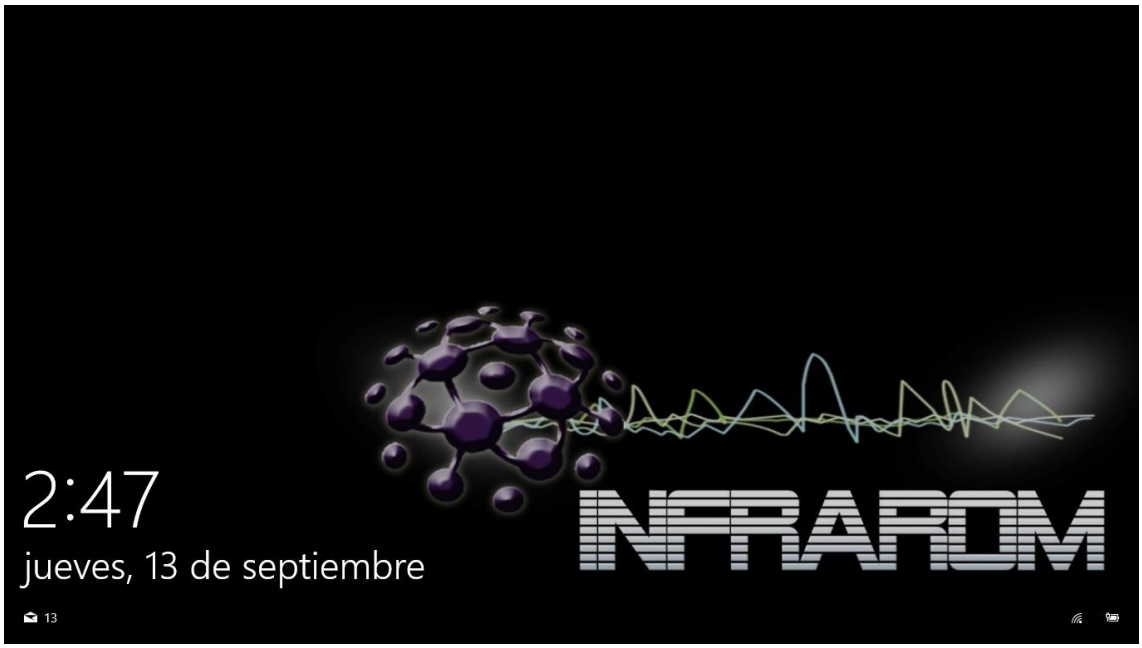
Fuente: El autor

Consentimiento de tratamientos de datos en los correos electrónicos corporativos de INFRAROM SAS.



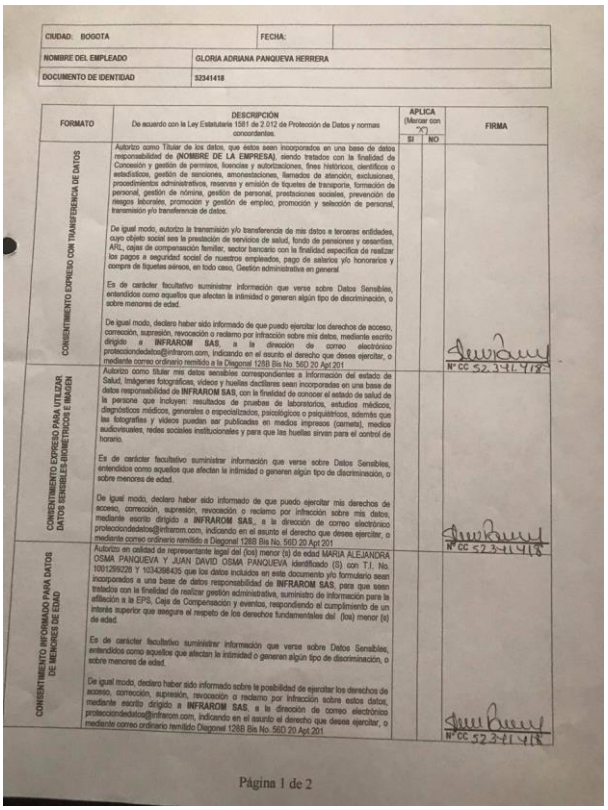
Fuente: El autor

Política de seguridad de bloqueo de pantalla para cuando el empleado no esté en su puesto de trabajo que impida el acceso a los documentos confidenciales del equipo.



Políticas de seguridad en contraseñas de los usuarios de INFRAROM SAS, determinando el perfil de cada empleado y los accesos a los cuales tiene permiso.

Firma de contratos de confidencialidad con todos los empleados y contratistas de la empresa, donde se establezcan los deberes y sanciones a las que están sometidos si no incumple con estas normas.



CIUDAD: BOGOTA		FECHA:	
NOMBRE DEL EMPLEADO	GLORIA ADRIANA PANQUEVA HERRERA		
DOCUMENTO DE IDENTIDAD	52341418		

FORMATO	DESCRIPCION De acuerdo con la Ley Estatutaria 1581 de 2.012 de Protección de Datos y normas concordantes.	APLICA (Marcar con "X") SI	APLICA (Marcar con "X") NO	FIRMA
CONSENTIMIENTO EXPRESO CON TRANSFERENCIA DE DATOS	Autorizo como Titular de los datos, que estos sean incorporados en una base de datos responsabilidad de (NOMBRE DE LA EMPRESA), siendo tratados con la finalidad de Concesión y gestión de permisos, licencias y autorizaciones, fines históricos, científicos o estadísticos, gestión de sanciones, amonestaciones, llamados de atención, exclusiones, procedimientos administrativos, reservas y emisión de tiquetes de transporte, formación de personal, gestión de nómina, gestión de personal, prestaciones sociales, prevención de riesgos laborales, promoción y gestión de empleo, promoción y selección de personal, transmisión y/o transferencia de datos. De igual modo, autorizo la transmisión y/o transferencia de mis datos a terceras entidades, cuyo objeto social sea la prestación de servicios de salud, fondo de pensiones y cesantías, ARL, cajas de compensación familiar, sector bancario con la finalidad específica de realizar los pagos a seguridad social de nuestros empleados, pago de salarios y/o honorarios y compra de tiquetes aéreos, en todo caso, Gestión administrativa en general. Es de carácter facultativo suministrar información que verse sobre Datos Sensibles, entendidos como aquellos que afectan la intimidad o generen algún tipo de discriminación, o sobre menores de edad. De igual modo, declaro haber sido informado de que puedo ejercitar los derechos de acceso, corrección, supresión, revocación o reclamo por infracción sobre mis datos, mediante escrito dirigido a **INFRAROM SAS**, a la dirección de correo electrónico protecciondedatos@infrarom.com, indicando en el asunto el derecho que desea ejercitar, o mediante correo ordinario remitido a la Diagonal 128B Bis No. 56D 20 Apt 201			N° CC 52.341.418
CONSENTIMIENTO EXPRESO PARA UTILIZAR DATOS SENSIBLES BIOMETRICOS E IMAGEN	Autorizo como titular mis datos sensibles correspondientes a información del estado de Salud, Imágenes fotográficas, videos y huellas dactilares sean incorporadas en una base de datos responsabilidad de **INFRAROM SAS**, con la finalidad de conocer el estado de salud de la persona que incluyen: resultados de pruebas de laboratorios, estudios médicos, diagnósticos médicos, generales o especializados, psicológicos o psiquiátricos, además que las fotografías y videos puedan ser publicadas en medios impresos (carnets), medios audiovisuales; redes sociales institucionales y para que las huellas sirvan para el control de horario. Es de carácter facultativo suministrar información que verse sobre Datos Sensibles, entendidos como aquellos que afectan la intimidad o generen algún tipo de discriminación, o sobre menores de edad. De igual modo, declaro haber sido informado de que puedo ejercitar mis derechos de acceso, corrección, supresión, revocación o reclamo por infracción sobre mis datos; mediante escrito dirigido a **INFRAROM SAS**, a la dirección de correo electrónico protecciondedatos@infrarom.com, indicando en el asunto el derecho que desea ejercitar, o mediante correo ordinario remitido a Diagonal 128B Bis No. 56D 20 Apt 201			N° CC 52.341.418
CONSENTIMIENTO INFORMADO PARA DATOS DE MENORES DE EDAD	Autorizo en calidad de representante legal del (los) menor (s) de edad MARIA ALEJANDRA OSMA PANQUEVA Y JUAN DAVID OSMA PANQUEVA identificado (S) con T.I. No. 1001266228 Y 1034288435 que los datos incluidos en este documento y/o formulario sean incorporados a una base de datos responsabilidad de **INFRAROM SAS**, para que sean tratados con la finalidad de realizar gestión administrativa, suministro de información para la afiliación a la EPS, Caja de Compensación y eventos, respondiendo al cumplimiento de un interés superior que asegure el respeto de los derechos fundamentales del (los) menor (s) de edad. Es de carácter facultativo suministrar información que verse sobre Datos Sensibles, entendidos como aquellos que afectan la intimidad o generen algún tipo de discriminación, o sobre menores de edad. De igual modo, declaro haber sido informado sobre la posibilidad de ejercitar los derechos de acceso, corrección, supresión, revocación o reclamo por infracción sobre estos datos, mediante escrito dirigido a **INFRAROM SAS**, a la dirección de correo electrónico protecciondedatos@infrarom.com, indicando en el asunto el derecho que desea ejercitar, o mediante correo ordinario remitido Diagonal 128B Bis No. 56D 20 Apt 201			N° CC 52.341.418

Página 1 de 2

Planillas de capacitación o ingreso con la cláusula de consentimiento de manejo de los datos personales consignados.

INFRAROM	**Asistencia Capacitación**		
Fecha		Nombre:	

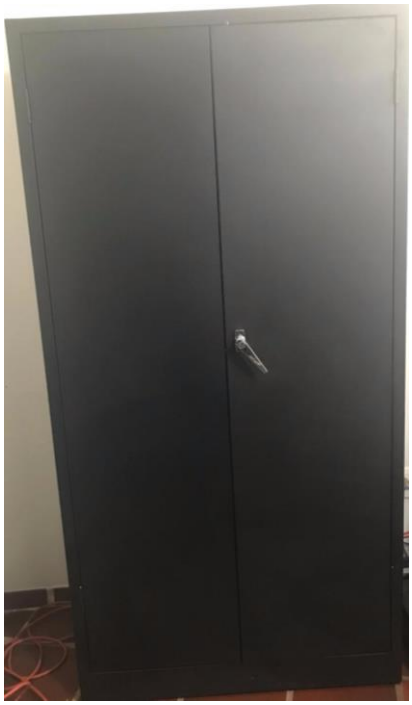
En cumplimiento de la Ley Estatutaria 1581 de 2012 de Protección de Datos (LEPD) y normas concordantes, el presente Aviso de Privacidad tiene como objeto informar al Titular sobre el tratamiento al cual serán sometidos los datos almacenados en nuestras bases de datos e informar si estos estarán sujetos a transmisión y/o transferencia a terceras entidades. Las condiciones del tratamiento son las siguientes:

1. INFRAROM SAS identificada con el NIT No. 900598259, será el responsable del tratamiento de sus datos personales.
2. Con objeto de recibir una atención integral como cliente, los datos personales recabados serán tratados con las siguientes finalidades:
3. Es de carácter facultativo suministrar información que verse sobre Datos Sensibles, entendidos como aquellos que afectan la intimidad o generen algún tipo de discriminación, o sobre menores de edad.
4. La política de tratamiento de los datos del Titular, así como los cambios sustanciales que se produzcan en ésta, se podrán consultar en el siguiente correo electrónico: protecciondedatos@infrarom.com.
5. El Titular puede ejercitar los derechos de acceso, corrección, supresión, revocación o reclamo por infracción sobre sus datos con un escrito dirigido a INFRAROM SAS a la dirección de correo electrónico protecciondedatos@infrarom.com indicando en el asunto el derecho que desea ejercitar; o mediante correo postal remitido a Diagonal 128B Bis No. 56D -20 Apto 201, BOGOTÁ D.C., BOGOTÁ.

Cédula	Nombres y Apellidos	Correo electrónico	Teléfono de contacto

Cláusula de consentimiento Web: Clausula que informa al titular de sus datos, que ingresa a la página y deja sus datos para comunicación posterior, la finalidad con la que son recaudados los datos.

Los datos personales que se encuentran en archivos físicos, se encuentran archivados en mueble con llave que solo maneja la encargada de el tratamiento de datos Paula Yamile Sarmiento Gamboa, lo cual garantiza que no están al alcance de personas sin autorización para su extracción.



4.4. REGISTRO NACIONAL DE BASES DE DATOS

En el ANEXO F se describe el paso a paso que se realiza para el registro de cada base ante la Superintendencia de Industria y Comercio.

La empresa Infrarom SAS realizó el registro de cada una de las bases de datos personales que maneja y se recibió la constancia de este registro, las bases de datos registradas fueron en total 8, son: empleados activos, clientes activos, proveedores automatizada, correos corporativos, clientes inactivos automatizada, empleados retirados automatizada, clientes prospecto intranet y clientes prospectos otros.

Cada uno de los radicados se muestra en las siguientes imágenes.

Fig. 1 Correos Corporativos

Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RAD: 17-295051--0-0	FECHA: 2017-08-04 15:47:18
DEP: DIRINVDATOSPERS	EVE:DEPOSITO R
TRA: REGISTRO D	FOLIOS: 1
ACT: PRESENTACION	

Señor (a) (es)
Empresa INFRAROM S.A.S.
Ciudad BOGOTÁ, D.C.

ASUNTO: Radicación: 17-295051--000000-000
Trámite: 413
Evento: 336
Actuación: 411

El presente documento constituye constancia de radicación ante la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO del trámite de registro de una base de datos con información personal, por consiguiente NO es necesario que realice este trámite vía fax, correo electrónico o radicarlo en las instalaciones de la SIC.

DATOS DEL REGISTRO DE LA BASE DE DATOS

RESPONSABLE DE LA BASE DE DATOS CON INFORMACIÓN PERSONAL
Nombre: INFRAROM S.A.S.
Identificación No.: 900596259
Dirección: DG 126B BIS 56D 20 AP 201
Ciudad: BOGOTÁ, D.C.
Teléfono: 3819905
Celular:
Email: info@infrarom.com

INFORMACIÓN DE LA BASE DE DATOS
RADICACIÓN: 295051
FECHA DE FINALIZACIÓN: 2017-08-04 15:47:18
NOMBRE: CORREOS CORPORATIVOS
FINALIDAD: Finalidades varias - Procedimientos administrativos, Marketing, Publicidad y prospección comercial - Prospección comercial

Toda la información asociada a esta radicación, en el Registro Nacional de Bases de Datos, está sujeta a verificación y cualquier inconsistencia le será comunicada.

Nota: Recuerde que se debe realizar un registro por cada una de las bases de datos con información personal que tenga el Responsable del Tratamiento.
Cordialmente,

Dirección de Investigación de Protección de Datos Personales
Superintendencia de Industria y Comercio

Fuente: El autor

Fig. 2 Clientes Inactivos Automatizados

Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
RAD: 17-294743--0-0 FECHA: 2017-08-04 12:48:47
DEP: DIRINVDATOSPERS EVE:DEPOSITO R
TRA: REGISTRO D FOLIOS: 1
ACT: PRESENTACION

Señor (a) (es)
Empresa INFRAROM S.A.S.
Ciudad BOGOTÁ, D.C.

ASUNTO: Radicación: 17-294743--000000-000
Trámite: 413
Evento: 336
Actuación: 411

El presente documento constituye constancia de radicación ante la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO del trámite de registro de una base de datos con información personal, por consiguiente NO es necesario que realice este trámite vía fax, correo electrónico o radicarlo en las instalaciones de la SIC.

DATOS DEL REGISTRO DE LA BASE DE DATOS

RESPONSABLE DE LA BASE DE DATOS CON INFORMACIÓN PERSONAL
Nombre: INFRAROM S.A.S.
Identificación No.: 900598259
Dirección: DG 126B BIS 56D 20 AP 201
Ciudad: BOGOTÁ, D.C.
Teléfono: 3819905
Celular:
Email: info@infrarom.com

INFORMACIÓN DE LA BASE DE DATOS
RADICACIÓN: 294743
FECHA DE FINALIZACIÓN: 2017-08-04 12:48:47
NOMBRE: CLIENTES INACTIVOS AUTOMATIZADO
FINALIDAD: Finalidades varias - Fidelización de clientes, Finalidades varias - Gestión de estadísticas internas, Finalidades varias - Procedimientos administrativos, Gestión contable, fiscal y administrativa - Gestión de clientes, Gestión contable, fiscal y administrativa - Gestión de cobros y pagos, Gestión contable, fiscal y administrativa - Gestión de facturación, Gestión contable, fiscal y administrativa - Gestión económica y contable, Gestión contable, fiscal y administrativa - Gestión fiscal, Gestión contable, fiscal y administrativa - Históricos de relaciones comerciales, Marketing, Publicidad y prospección comercial - Encuestas de opinión, Publicidad y prospección comercial - Prospección comercial, Publicidad y prospección comercial - Publicidad propia, Publicidad y prospección comercial - Venta a distancia

Toda la información asociada a esta radicación, en el Registro Nacional de Bases de Datos, está sujeta a verificación y cualquier inconsistencia le será comunicada.

Nota: Recuerde que se debe realizar un registro por cada una de las bases de datos con información personal que tenga el Responsable del Tratamiento.

Cra. 13 # 27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (571) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfono en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO

Fuente: El autor

Fig. 3 Empleados Automatizados

Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RAD: 17-294693--0-0	FECHA: 2017-08-04 12:03:14
DEP: DIRINVDATOSPERS	EVE:DEPOSITO R
TRA: REGISTRO D	FOLIOS: 1
ACT: PRESENTACION	

Señor (a) (es)
Empresa INFRAROM S.A.S.
Ciudad BOGOTÁ, D.C.

ASUNTO: Radicación: 17-294693--000000-000
Trámite: 413
Evento: 336
Actuación: 411

El presente documento constituye constancia de radicación ante la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO del trámite de registro de una base de datos con información personal, por consiguiente NO es necesario que realice este trámite vía fax, correo electrónico o radicarlo en las instalaciones de la SIC.

DATOS DEL REGISTRO DE LA BASE DE DATOS

RESPONSABLE DE LA BASE DE DATOS CON INFORMACIÓN PERSONAL
Nombre: INFRAROM S.A.S.
Identificación No.: 900596259
Dirección: DG 126B BIS 56D 20 AP 201
Ciudad: BOGOTÁ, D.C.
Teléfono: 3819905
Celular:
Email: info@infrarom.com

INFORMACIÓN DE LA BASE DE DATOS
RADICACIÓN: 294693
FECHA DE FINALIZACIÓN: 2017-08-04 12:03:14
NOMBRE: EMPLEADOS RETIRADOS AUTOMATIZADO
FINALIDAD: Finalidades varias - Procedimientos administrativos, Gestión contable, fiscal y administrativa - Gestión administrativa, Gestión contable, fiscal y administrativa - Gestión económica y contable, Información de Empleados, Recursos humanos - Gestión de nómina, Recursos humanos - Gestión de personal, Recursos humanos - Gestión de trabajo temporal, Recursos humanos - Prestaciones sociales, Recursos humanos - Prevención de riesgos laborales

Toda la información asociada a esta radicación, en el Registro Nacional de Bases de Datos, está sujeta a verificación y cualquier inconsistencia le será comunicada.

Nota: Recuerde que se debe realizar un registro por cada una de las bases de datos con información personal que tenga el Responsable del Tratamiento.
Cordialmente,

Cra. 13 # 27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (571) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfono en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO

Fuente: El autor

Fig. 4 Proveedores Automatizados

Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
RAD: 17-294612--0-0 FECHA: 2017-08-04 11:30:43
DEP: DIRINVDATOSPERS EVE:DEPOSITO R
TRA: REGISTRO D FOLIOS: 1
ACT: PRESENTACION

Señor (a) (es)
Empresa INFRAROM S.A.S.
Ciudad BOGOTÁ, D.C.

ASUNTO: Radicación: 17-294612--000000-000
Trámite: 413
Evento: 336
Actuación: 411

El presente documento constituye constancia de radicación ante la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO del trámite de registro de una base de datos con información personal, por consiguiente NO es necesario que realice este trámite vía fax, correo electrónico o radicarlo en las instalaciones de la SIC.

DATOS DEL REGISTRO DE LA BASE DE DATOS

RESPONSABLE DE LA BASE DE DATOS CON INFORMACIÓN PERSONAL
Nombre: INFRAROM S.A.S.
Identificación No.: 900596259
Dirección: DG 126B BIS 56D 20 AP 201
Ciudad: BOGOTÁ, D.C.
Teléfono: 3819905
Celular:
Email: info@infrarom.com

INFORMACIÓN DE LA BASE DE DATOS
RADICACIÓN: 294612
FECHA DE FINALIZACIÓN: 2017-08-04 11:30:43
NOMBRE: PROVEEDORES AUTOMATIZADO
FINALIDAD: Finalidades varias - Procedimientos administrativos, Gestión contable, fiscal y administrativa - Gestión administrativa, Gestión contable, fiscal y administrativa - Gestión de cobros y pagos, Gestión contable, fiscal y administrativa - Gestión de facturación, Gestión contable, fiscal y administrativa - Gestión de proveedores y contratistas, Gestión contable, fiscal y administrativa - Gestión económica y contable, Gestión contable, fiscal y administrativa - Gestión fiscal, Gestión contable, fiscal y administrativa - Históricos de relaciones comerciales

Toda la información asociada a esta radicación, en el Registro Nacional de Bases de Datos, está sujeta a verificación y cualquier inconsistencia le será comunicada.

Nota: Recuerde que se debe realizar un registro por cada una de las bases de datos con información personal que tenga el Responsable del Tratamiento.
Cordialmente,

Cra. 13 # 27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (571) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfono en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO

Fuente: El autor

Fig. 5 Empleados Retirados

Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
RAD: 17-294656--0-0 FECHA: 2017-08-04 11:47:49
DEP: DIRINVDATOSPERS EVE:DEPOSITO R
TRA: REGISTRO D FOLIOS: 1
ACT: PRESENTACION

Señor (a) (es)
Empresa INFRAROM S.A.S.
Ciudad BOGOTÁ, D.C.

ASUNTO: Radicación: 17-294656--000000-000
Trámite: 413
Evento: 336
Actuación: 411

El presente documento constituye constancia de radicación ante la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO del trámite de registro de una base de datos con información personal, por consiguiente NO es necesario que realice este trámite vía fax, correo electrónico o radicarlo en las instalaciones de la SIC.

DATOS DEL REGISTRO DE LA BASE DE DATOS

RESPONSABLE DE LA BASE DE DATOS CON INFORMACIÓN PERSONAL
Nombre: INFRAROM S.A.S.
Identificación No.: 900596259
Dirección: DG 126B BIS 56D 20 AP 201
Ciudad: BOGOTÁ, D.C.
Teléfono: 3819905
Celular:
Email: info@infrarom.com

INFORMACIÓN DE LA BASE DE DATOS
RADICACIÓN: 294656
FECHA DE FINALIZACIÓN: 2017-08-04 11:47:49
NOMBRE: EMPLEADOS RETIRADOS
FINALIDAD: Finalidades varias - Procedimientos administrativos, Gestión contable, fiscal y administrativa - Gestión administrativa, Gestión contable, fiscal y administrativa - Gestión económica y contable, Información de Empleados, Recursos humanos - Gestión de nómina, Recursos humanos - Gestión de personal, Recursos humanos - Gestión de trabajo temporal, Recursos humanos - Prestaciones sociales, Recursos humanos - Prevención de riesgos laborales

Toda la información asociada a esta radicación, en el Registro Nacional de Bases de Datos, está sujeta a verificación y cualquier inconsistencia le será comunicada.

Nota: Recuerde que se debe realizar un registro por cada una de las bases de datos con información personal que tenga el Responsable del Tratamiento.
Cordialmente,

Cra. 13 # 27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (571) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfono en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO

Fuente: El autor

Fig. 6 Clientes Inactivos

Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
RAD: 17-294731--0-0 FECHA: 2017-08-04 12:36:14
DEP: DIRINVDATOSPERS EVE:DEPOSITO R
TRA: REGISTRO D FOLIOS: 1
ACT: PRESENTACION

Señor (a) (es)
Empresa INFRAROM S.A.S.
Ciudad BOGOTÁ, D.C.

ASUNTO: Radicación: 17-294731--000000-000
Trámite: 413
Evento: 336
Actuación: 411

El presente documento constituye constancia de radicación ante la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO del trámite de registro de una base de datos con información personal, por consiguiente NO es necesario que realice este trámite vía fax, correo electrónico o radicarlo en las instalaciones de la SIC.

DATOS DEL REGISTRO DE LA BASE DE DATOS

RESPONSABLE DE LA BASE DE DATOS CON INFORMACIÓN PERSONAL
Nombre: INFRAROM S.A.S.
Identificación No.: 900596259
Dirección: DG 126B BIS 56D 20 AP 201
Ciudad: BOGOTÁ, D.C.
Teléfono: 3819905
Celular:
Email: info@infrarom.com

INFORMACIÓN DE LA BASE DE DATOS
RADICACIÓN: 294731
FECHA DE FINALIZACIÓN: 2017-08-04 12:36:14
NOMBRE: CLIENTES INACTIVOS
FINALIDAD: Finalidades varias - Gestión de estadísticas internas, Finalidades varias - Procedimientos administrativos, Gestión contable, fiscal y administrativa - Gestión de clientes, Gestión contable, fiscal y administrativa - Gestión de cobros y pagos, Gestión contable, fiscal y administrativa - Gestión de facturación, Finalidades varias - Fidelización de clientes, Gestión contable, fiscal y administrativa - Gestión económica y contable, Gestión contable, fiscal y administrativa - Gestión fiscal, Gestión contable, fiscal y administrativa - Históricos de relaciones comerciales, Marketing, Publicidad y prospección comercial - Encuestas de opinión, Publicidad y prospección comercial - Prospección comercial, Publicidad y prospección comercial - Publicidad propia, Publicidad y prospección comercial - Venta a distancia

Toda la información asociada a esta radicación, en el Registro Nacional de Bases de Datos, está sujeta a verificación y cualquier inconsistencia le será comunicada.

Nota: Recuerde que se debe realizar un registro por cada una de las bases de datos con información personal que tenga el Responsable del Tratamiento.

Cra. 13 # 27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (571) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfono en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO

Fuente: El autor

Fig. 7 Clientes Prospecto Otros

Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RAD: 17-295023--0-0	FECHA: 2017-08-04 15:39:42
DEP: DIRINVDATOSPERS	EVE:DEPOSITO R
TRA: REGISTRO D	FOLIOS: 1
ACT: PRESENTACION	

Señor (a) (es)
Empresa INFRAROM S.A.S.
Ciudad BOGOTÁ, D.C.

ASUNTO: Radicación: 17-295023--000000-000
Trámite: 413
Evento: 336
Actuación: 411

El presente documento constituye constancia de radicación ante la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO del trámite de registro de una base de datos con información personal, por consiguiente NO es necesario que realice este trámite vía fax, correo electrónico o radicarlo en las instalaciones de la SIC.

DATOS DEL REGISTRO DE LA BASE DE DATOS

RESPONSABLE DE LA BASE DE DATOS CON INFORMACIÓN PERSONAL
Nombre: INFRAROM S.A.S.
Identificación No.: 900596259
Dirección: DG 126B BIS 56D 20 AP 201
Ciudad: BOGOTÁ, D.C.
Teléfono: 3819905
Celular:
Email: info@infrarom.com

INFORMACIÓN DE LA BASE DE DATOS
RADICACIÓN: 295023
FECHA DE FINALIZACIÓN: 2017-08-04 15:39:42
NOMBRE: CLIENTES PROSPECTO OTROS
FINALIDAD: Finalidades varias - Procedimientos administrativos, Marketing, Publicidad y prospección comercial - Encuestas de opinión, Publicidad y prospección comercial - Prospección comercial, Publicidad y prospección comercial - Publicidad propia, Publicidad y prospección comercial - Segmentación de mercados, Publicidad y prospección comercial - Venta a distancia

Toda la información asociada a esta radicación, en el Registro Nacional de Bases de Datos, está sujeta a verificación y cualquier inconsistencia le será comunicada.

Nota: Recuerde que se debe realizar un registro por cada una de las bases de datos con información personal que tenga el Responsable del Tratamiento.
Cordialmente,

Dirección de Investigación de Protección de Datos Personales

Cra. 13 # 27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (571) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfono en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO INDUSTRIA Y TURISMO

Fuente: El autor

Fig. 8 Clientes Prospecto Intranet

Industria y Comercio
SUPERINTENDENCIA

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
RAD: 17-299918--0-0 FECHA: 2017-08-04 15:10:36
DEP: DIRINVDATOSPERS EVE:DEPOSITO R
TRA: REGISTRO D FOLIOS: 1
ACT: PRESENTACION

Señor (a) (es)
Empresa INFRAROM S.A.S.
Ciudad BOGOTÁ, D.C.

ASUNTO: Radicación: 17-299918--000000-000
Trámite: 413
Evento: 336
Actuación: 411

El presente documento constituye constancia de radicación ante la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO del trámite de registro de una base de datos con información personal, por consiguiente NO es necesario que realice este trámite vía fax, correo electrónico o radicarlo en las instalaciones de la SIC.

DATOS DEL REGISTRO DE LA BASE DE DATOS

RESPONSABLE DE LA BASE DE DATOS CON INFORMACIÓN PERSONAL
Nombre: INFRAROM S.A.S.
Identificación No.: 900596259
Dirección: DG 126B BIS 56D 20 AP 201
Ciudad: BOGOTÁ, D.C.
Teléfono: 3819905
Celular:
Email: info@infrarom.com

INFORMACIÓN DE LA BASE DE DATOS
RADICACIÓN: 299918
FECHA DE FINALIZACIÓN: 2017-08-04 15:10:36
NOMBRE: CLIENTES PROSPECTO INTRANET
FINALIDAD: Finalidades varias - Procedimientos administrativos, Marketing, Publicidad y prospección comercial - Análisis de perfiles, Publicidad y prospección comercial - Encuestas de opinión, Publicidad y prospección comercial - Prospección comercial, Publicidad y prospección comercial - Publicidad propia, Publicidad y prospección comercial - Segmentación de mercados, Publicidad y prospección comercial - Venta a distancia

Toda la información asociada a esta radicación, en el Registro Nacional de Bases de Datos, está sujeta a verificación y cualquier inconsistencia le será comunicada.

Nota: Recuerde que se debe realizar un registro por cada una de las bases de datos con información personal que tenga el Responsable del Tratamiento.
Cordialmente,

Dirección de Investigación de Protección de Datos Personales

Cra. 13 # 27 - 00 pisos 1, 3, 4, 5, 6, 7 y 10 - PBX: (571) 5870000 - contactenos@sic.gov.co - Bogotá D.C., Colombia
Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co - Teléfono en Bogotá: 5920400 - Línea gratuita a nivel nacional: 018000 910165

MINCOMERCIO
INDUSTRIA Y TURISMO

Fuente: El autor

5. CONCLUSIONES

- Con el desarrollo de este proyecto se clasifico la información que se tenía sobre datos personales de clientes, proveedores y empleados, determinando el tipo de datos, la finalidad de su recolección, logrando una adecuada organización que mejoró los proceso y buenas prácticas de seguridad de la empresa INFRAROM SAS
- En el transcurso de este proyecto Infrarom SAS realizó todo el proceso de recolección y análisis de la información contenida en las bases de datos; creación de políticas, manuales y formatos para el tratamiento de los datos personales; implementación de las políticas y capacitación del personal de la empresa sobre la importancia del tratamiento de los datos personales y el Registro Nacional de la Bases de Datos ante la Superintendencia de Industria y Comercio.
- INFRAROM SAS, crea el Manual Interno de Seguridad donde se describe todas las medidas humanas, administrativas y técnicas para lograr la seguridad de los registros de datos personales con el fin de impedir su perdida, o acceso fraudulento o no autorizado, de acuerdo a la ley de protección de datos.
- Con el registro nacional de bases de datos ante la superintendencia de industria y comercio la empresa INFRAROM SAS está cumpliendo con la ley estatutaria 1581 de 2012 sobre el tratamiento de datos personales, lo cual ha servido de instrumento para mejorar la protección integral del derecho a la privacidad, el derecho a la intimidad, buen nombre y a la honra, que es vulnerada cuando no hay una adecuado tratamiento de los datos.

6. RECOMENDACIONES

Las personas que deseen investigar sobre la seguridad en los datos personales deben tener en cuenta que existen varias leyes que hablan sobre el tema, pero la principal es la ley 1581 de 2012 sobre la protección de datos personales, estas leyes han tomado importancia en el ámbito empresarial ya que hay un ente que es la Superintendencia de Industria y Comercio que se encarga de evaluar el cumplimiento de la ley e implementación en las empresas.

Aun así las leyes son cambiantes y se creía que esta ley iba a ser aplicada a todas las empresas e incluso personas naturales que manejaran bases de datos personales, pero al principio de este año solo se reglamentó para grandes empresas sin ánimo de lucro y empresas públicas, lo cual hace que se siga atropellando los derechos de privacidad y buen nombre de las personas.

Para dar continuidad con este proyecto se pueden comparar las leyes de protección de datos de otros países que se toman más en serio los derechos de las personas, con el avance que se ha tenido en Colombia con respecto al tema, para llevarse una idea de los cambios a través de los años y de lo avanzadas que están estas leyes en otros países.

Otro aspecto importante para futuros proyectos de investigación de la empresa INFRAROM SAS, se enmarcaran en las auditorías internas y externas que se deben realizar para determinar el cumplimiento de los manuales y políticas creados, e ir optimizando la seguridad en cuanto al tratamiento de los datos personales.

REFERENCIAS BIBLIOGRAFÍCAS

ÁLZATE, W. A. C., ROMAÑA, C. A. S., & Barco, Y. A. Q. (2015). Factores y causas de la fuga de información sensibles en el sector empresarial. CUADERNO ACTIVA, 7(7), 67-73.

ARDILA, R., & YOHANNA, B. (2016). Regulación en materia de protección de datos personales o Habeas Data en Colombia a través de la Ley 1581 de 2012: Examen histórico y crítico sobre su ineficacia ante las administradoras de bases de datos, portales de Internet y motores de búsquedas.

AYALA, V., DANIEL, J., & PÁEZ Escobar, A. M. (2016). Sanciones por parte de la Superintendencia de Industria y Comercio por el cambio de la finalidad en el uso de los datos personales en Colombia período 2013-2014.

BERNAL, C. (2006). Metodología de la Investigación. México: Pearson Educación.

BERMÚDEZ DURANA, José Alejandro. El futuro de la protección de datos personales en Colombia. Consultado el 22 de abril en http://www.portafolio.co/opinion/el-futuro-la-proteccion-datos-personales-colombia

BUITRAGO BOTERO, D. M. (2016). El valor de los datos personales en Colombia. Revista CES Derecho, 7(1), 1-2.

CANO, L. G. (2012). Protección de datos en Colombia, avances y retos. *Revista Lebret*, *4*(4), 195-214.

CERDA, H. (2008). Los elementos de la Investigación. Bogotá: Ed Norma.

CUEVAS RODRÍGUEZ, M. P. (2016). De la protección de datos personales en Colombia (Ley 1581 de 2012): un estudio comparado con el sistema canadiense.

DECRETO 2952 DE 2010. Tomado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=40120

Decreto 1377 de 2013 Nivel Nacional. Tomado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma_temas.jsp?i=53646

DE DATOS PERSONALES, L. D. P. Politicas de privacidad y protección de datos.

DE INDUSTRIA, S. (2016). Ámbito de aplicación de la Ley 1581 de 2012.

DE INDUSTRIA, S. (2016). SuperIndustria-bases de datos-registro.

DE INDUSTRIA, S. (2015). Circular Externa 02. Tomado de: http://www.sic.gov.co/sites/default/files/normatividad/CE_Implementacion_RNBD_fase_2.pdf

FORERO LOAIZA, D. C., & Velez Trucco, S. (2016). Ley 1581 de 2012: contextualización de la norma a nivel nacional e internacional y análisis de algunas sanciones interpuestas.

INFRAROM (2014) Misión. Tomado de: http://infrarom.com

MENDOZA MORALES, J. A. (2016). Protección de datos personales en Colombia (Bachelor's thesis, Universidad Militar Nueva Granada).

PUCCINELLI O R (2004) Evolución histórica y análisis de las distintas especies, subespecies, tipos y subtipos de Habeas Data en América Latina: un intento clasificatorio con fines didácticos, Revista Universitas No. 107, Universidad Javeriana, Bogotá.

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.

REMOLINA – ANGARITA, Nelson (2003) Data protection: Panorama nacional e internacional. Chapter of the book "Internet, Comercio Electrónico &Telecomunicaciones" Legis. Bogotá, Colombia.

REMOLINA-ANGARITA N. (2002) Centrales de información, habeas data y protección de datos personales: Avances, retos y elementos para su regulación. En “Derecho de Internet & Telecomunicaciones”.Legis. Bogotá, Colombia

REINA, M. G. Privacidad y protección de los datos personales: un breve recorrido por el caso colombiano.

RONDEROS, M. F. C. (2014). Legislación informática y protección de datos en Colombia, comparada con otros países. Revista Inventum, (17).

SAMPIERI, R. COLLADO, C. & LUCIO, P. (2007) Fundamentos de la Metodología de la Investigación. México: Limusa.

SÁNCHEZ, M. Y. N. (2008). Protección de datos personales. In A 21 años de la Constitución Política: vigencia y desafíos (pp. 109-114).

SERVIMCOOP, (s.f) ABC de la protección de datos. Tomado de: http://www.servimcoop.com/Proteccion_datos.pdf

TAMAYO, M. (2007) El proceso de la Investigación Científica. México: Limusa.

ANEXO A

RECOLECCIÓN DE DATOS PARA LA ADAPTACION A LA LEPD

RECOLECCIÓN DE DATOS PARA LA ADAPTACIÓN A LA LEPD: **EMPRESA/CLIENTE:**	
DATOS CONTACTO PARA LA RECOLECCION DE DATOS:	
NOMBRE:	
CORREO ELECTRONICO:	
TELEFONO:	

INFORMACION REQUERIDA DE LA EMPRESA:

1) Adjuntar logo de la empresa para personalizar la documentación.

INFORMACION Y DATOS GENERALES PARA EL RNBD

- Responsable del tratamiento: (Nombre de la razón Social)
- NIT:
- Naturaleza jurídica o natural:
- Matricula Mercantil
- Dirección postal con ciudad incluida:
- Emails registrados en Cámara de Comercio:
    a) Notificaciones Judiciales:
    b) Comercial:
- Código CIIU (actividad económica): Información se encuentra en el Rut
- Nombre del representante legal:
- N° de cedula del representante legal y lugar de expedición:
- Teléfono del representante legal:
- Email del representante legal:
- Nombre del Oficial de Protección Datos del tratamiento: Persona que lidera el tema en la empresa.
- N° de cedula del encargado del tratamiento y lugar de expedición:
- Cargo del tratamiento:
- Dirección del encargado del tratamiento
- Teléfono del encargado del tratamiento:
- Email del encargado del tratamiento:
    - Canales de atención al titular de los datos:

    a) Página Web: www. Favor indicar página web de la empresa

    b) Correo Electrónico para la atención: Indicar el correo que se asignara para todo el tema de ley de protección de datos. Se sugiere el correo protecciondedatos@

ANEXO B

CLASES DE BASES DE DATOS

CLASES DE BASES DE DATOS
1 –Empleados históricos
2- Empleados Activos
3- Procesos de selección
3- Empleados carnetización
4- Empleados y control de acceso a visitantes.
5- Control de acceso biométrico
6- Video vigilancia propia (Días que guardan la información).
7- Control de acceso Residentes – Visitantes
8- Proveedores.
9- Clientes
10- Clientes prospectos.
11- Clientes arrendatarios y clientes propietarios en caso de las inmobiliarias.
12- Huéspedes
13- Asistentes de eventos
14- Capacitaciones (Capacitación creada para terceros)
15- Correo electrónico
16- Copias de respaldo
17- Patrocinadores
18- Encuestas
19- Deudor Solidario / Fiador
20- Asociados o Afiliados
21- Beneficiarios
22- Socios y Accionistas
23- Juntas Directivas y/o consejos de administración.
24. Docentes
25. Estudiantes

ANEXO C

Tabla 2 Finalidades

 **Finalidades para las bases de datos según la (SIC)**
Actividades asociativas, culturales, recreativas, deportivas y sociales – Asistencia social
Actividades asociativas, culturales, recreativas, deportivas y sociales – Gestión de actividades culturales
Actividades asociativas, culturales, recreativas, deportivas y sociales – Gestión de asociados o miembros de partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro
Actividades asociativas, culturales, recreativas, deportivas y sociales – Gestión de clubes o asociaciones deportivas, culturales, profesionales y similares
Actividades asociativas, culturales, recreativas, deportivas y sociales – Gestión de medios de comunicación social y/o contenido editorial.
Actividades asociativas, culturales, recreativas, deportivas y sociales – Gestión de organizaciones no gubernamentales
Arte
Capacitación
Comercialización de datos
Educación
Educación y cultura – Becas y ayudas a estudiantes
Educación y cultura – Deportes
Educación y cultura – Educación especial
Educación y cultura – Encuestas sociológicas y de opinión
Educación y cultura – Enseñanza Informal
Educación y cultura – Enseñanza Media
Educación y cultura – Enseñanza no formal
Educación y cultura – Enseñanza pre-escolar y primaria
Educación y cultura – Enseñanza secundaria
Educación y cultura – Enseñanza técnica o tecnológica formal
Educación y cultura – Enseñanza universitaria o superior
Educación y cultura – Otras enseñanzas
Educación y cultura – Protección del patrimonio artístico y cultural
Ejercicio de un derecho
Empleado
Finalidades varias – Atención al ciudadano
Finalidades varias – Concesión y gestión de permisos, licencias y autorizaciones
Finalidades varias – Fidelización de clientes
Finalidades varias – Fines históricos, científicos o estadísticos
Finalidades varias – Gestión de estadísticas internas
Finalidades varias – Gestión de sanciones, amonestaciones, llamados de atención, exclusiones.

Finalidades varias – Prestación de servicios de certificación
Finalidades varias – Procedimientos administrativos
Finalidades varias – Publicaciones
Finalidades varias – Registro de entrada y salida de documentos
Finalidades varias – Reservas y emisión de tiquetes de transporte
Financiera
Formación
Gestión contable, fiscal y administrativa – Administración de edificios
Gestión contable, fiscal y administrativa – Consultorías, auditorías, asesorías y servicios relacionados
Gestión contable, fiscal y administrativa – Gestión administrativa
Gestión contable, fiscal y administrativa – Gestión de clientes
Gestión contable, fiscal y administrativa – Gestión de cobros y pagos
Gestión contable, fiscal y administrativa – Gestión de facturación
Gestión contable, fiscal y administrativa – Gestión de proveedores
Gestión contable, fiscal y administrativa – Gestión económica y contable
Gestión contable, fiscal y administrativa – Gestión fiscal
Gestión contable, fiscal y administrativa – Históricos de relaciones comerciales
Hacienda pública y gestión económico-financiera – Gestión de catastros inmobiliarios
Hacienda pública y gestión económico-financiera – Gestión deuda pública y tesorería
Hacienda pública y gestión económico-financiera – Gestión tributaria y de recaudación
Hacienda pública y gestión económico-financiera – Regulación de mercados financieros
Hacienda pública y gestión económico-financiera – Relaciones comerciales con el exterior
Justicia – Prestación social
Justicia – Procedimientos judiciales
Justicia – Registros notariales
Marketing proveedores
Población vulnerable
Publicidad y prospección comercial – Análisis de perfiles
Publicidad y prospección comercial – Encuestas de opinión
Publicidad y prospección comercial – Prospección comercial
Publicidad y prospección comercial – Publicidad propia
Publicidad y prospección comercial – Segmentación de mercados
Publicidad y prospección comercial – Sistemas de ayuda a la toma de decisiones
Publicidad y prospección comercial – Venta a distancia
Recursos humanos – Acción social a favor de funcionarios públicos
Recursos humanos – Control de horario
Recursos humanos – Control de patrimonio de funcionarios públicos
Recursos humanos – Formación de personal
Recursos humanos – Gestión de nómina

Recursos humanos – Gestión de personal
Recursos humanos – Gestión de trabajo temporal
Recursos humanos – Prestaciones sociales
Recursos humanos – Prevención de riesgos laborales
Recursos humanos – Promoción y gestión de empleo
Recursos humanos – Promoción y selección de personal
Salud
Sanidad – Gestión de Sisbén
Sanidad – Gestión y control sanitario
Sanidad – Investigación epidemiológica y actividades análogas
Seguridad – Investigaciones privadas a personas
Seguridad – Seguridad
Seguridad – Seguridad y control de acceso a edificios
Seguridad pública y defensa – Actuaciones de fuerzas y cuerpos de seguridad con fines administrativos
Seguridad pública y defensa – Actuaciones de fuerzas y cuerpos de seguridad con fines policiales
Seguridad pública y defensa – Gestión y control de centros e instituciones penitenciarias
Seguridad pública y defensa – Protección civil
Seguridad pública y defensa – Seguridad vial
Seguridad pública y defensa – Solicitudes de visado/residencia
Seguridad pública y defensa – Trámites de servicio militar
Servicio de telecomunicaciones – Comercio electrónico
Servicio de telecomunicaciones – Guías/catálogos de servicios de telecomunicaciones
Servicio de telecomunicaciones – Prestación de servicios de telecomunicaciones
Servicios de salud – Historial Clínico
Servicios de salud – Programas de promoción y prevención
Servicios de salud – Registro de citas médicas u odontológicas
Servicios de salud – Registro de Donantes
Servicios de salud – Registro de imágenes y exámenes diagnósticos
Servicios de salud – Salud mental
Servicios de salud – Salud Sexual y reproductiva
Servicios económico-financieros y seguros – Cuenta de crédito
Servicios económico-financieros y seguros – Cuenta de depósito
Servicios económico-financieros y seguros – Cumplimiento/incumplimiento de obligaciones financieras
Servicios económico-financieros y seguros – Gestión de fondos de pensiones
Servicios económico-financieros y seguros – Gestión de patrimonios
Servicios económico-financieros y seguros – Gestión de tarjetas de crédito y similares
Servicios económico-financieros y seguros – Prestación de servicios de solvencia patrimonial y crédito
Servicios económico-financieros y seguros – Registro de acciones y obligaciones

Servicios económico-financieros y seguros – Seguros de vida y salud
Trabajo y bienestar social – Acción a favor de inmigrantes
Trabajo y bienestar social – Ayudas para el acceso a vivienda
Trabajo y bienestar social – Formación profesional ocupacional
Trabajo y bienestar social – Inspección y control de seguridad y protección social
Trabajo y bienestar social – Pensiones, subsidios y otras prestaciones económicas
Trabajo y bienestar social – Prestaciones a desempleados
Trabajo y bienestar social – Prestaciones de asistencia social
Trabajo y bienestar social – Prestaciones de garantía salarial
Trabajo y bienestar social – Promoción social a la juventud
Trabajo y bienestar social – Promoción social a la mujer
Trabajo y bienestar social – Protección del menor
Trabajo y bienestar social – Relaciones laborales y condiciones de trabajo
Trabajo y bienestar social – Servicios a favor de toxicómanos
Trabajo y bienestar social – Servicios sociales a la tercera edad
Trabajo y bienestar social – Servicios sociales a minusválidos

ANEXO D

1. Nombre de la base de datos:	xxx

Marcar X según corresponda	
	Automatizada (Solo una opción)
	Se guarda en Servidor Propio?
	Se guarda en Servidor externo propio?
	Se guarda en Servidor externo a cargo de un tercero?
	Computador Personal?
	Fisica (Marcar solo una opción)
	Se guarda en Archivo Propio Interno?
	Se guarda en Archivo Propio Externo?
	Se guarda en Archivo en custodia de un tercero?
	Mixta (Automatizada y Fisica. Marcar una opcion para cada uno)
	Se guarda en Servidor Propio?
	Se guarda en Servidor externo propio?
	Se guarda en Servidor externo a cargo de un tercero?
	Computador Personal? Se guarda en Archivo Propio Interno?
	Se guarda en Archivo Propio Externo?
	Se guarda en Archivo en custodia de un tercero?

3. Numero titulares en la base de datos (Cantidad de datos):	#

Marcar X según corresponda	**2. Información que contiene la Base de datos**
	Datos de menores de edad
	Datos de mayores de edad
	Nombre
	Número de identificación
	Edad
	Sexo
	Firma
	Nacionalidad
	Lugar y fecha de nacimiento o muerte
	Otros documentos de Identificación
	Fotografías

Tabla 7. (Continuación)

 **2. Información que contienen las base de datos:**	xxx
	Huella dactilar, Iris o registro de voz
	Videos
	ADN
	Estatura
	Peso
	Descripción morfológica de la persona
	Correo de actividad laboral
	Teléfono de actividad laboral
	Dirección de actividad laboral
	Correo personal
	Teléfono personal
	Dirección del lugar de residencia
	Información del estado de salud
	Resultados de pruebas y diagnósticos médicos
	Datos sobre pertenencia a organizaciones sociales, religiosas, políticas, etc.
	Datos de preferencia, orientación sexual de la persona,
	origen étnico-racial de la persona
	Datos sobre Población en condición vulnerable
	Datos sobre personas discapacitadas
	Información financiera, económica o crediticia de las personas
	Estrato
	Datos patrimoniales de la persona
	Información tributaria de la persona
	Datos sobre la actividad económica
	Información laboral de la persona
	Información académica de la persona
	Datos relacionados con afiliación y aportes al Sistema Integral de Seguridad Social.
	Perfiles, Usuarios y claves
	Dirección IP
	Información sobre gustos y preferencias
	Antecedentes judiciales o disciplinarios

ANEXO D (Continuación)

4. Responsable de la seguridad de la BD	
NOMBRE	xxx
CARGO	xxx
CEDULA Y LUGAR DE EXPEDICION	sin puntos
TELEFONO	
CORREO ELECTRONICO	@
4. Fuente: (Cómo llega la información para alimentar la base de datos, si es a través de un formato escrito o se descarga de algún programa principal, Etc.)	
5. Seguridad (¿Qué medidas de seguridad tiene la empresa para proteger los documentos y dispositivos que contienen bases de datos personales?) Si manejan usuarios y contraseñas para acceder a esta información	
6. Finalidades (Para qué finalidad será utilizada la BD - Revisar cuadro finalidades y adicionarlas a este cuadro)	

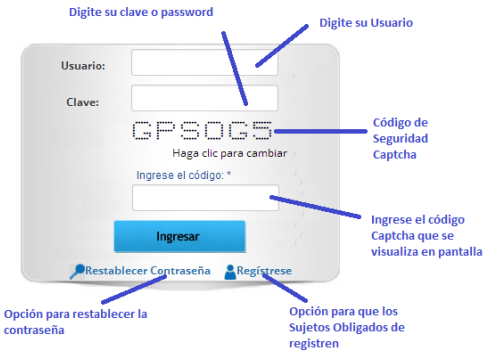
Fuente: El autor

ANEXO F

MANUAL PASO A PASO PARA EL REGISTRO NACIONAL DE BASE DE DATOS

Ingreso al sistema, para el ingreso al sistema se requiere de un usuario, contraseña (Creado en la página de la Superintendencia de Industria y Comercio), el ingreso de código captcha, el cual puede ser modificado por el usuario con la opción “Haga clic para cambiar.” Como se muestra en la fig. 1.

Fig 1 Ingreso al Sistema



Fuente: El autor

Al acceder al menú principal podemos observar dos pestañas en RNBD, accedemos al módulo de Registro de Base de Datos e Información del Responsable o al de administración de usuarios donde podemos cambiar la contraseña. Fig. 2.

Fig 2 Menú Principal

RN BD REGISTRO NACIONAL DE BASES DE DATOS

Fuente: El autor

Cuando se da clic en RNBD se accede a la página que muestra la Fig. 3, antes de realizar la inscripción de las bases de datos personales se debe ingresar por la opción de Responsable del Tratamiento y diligenciar la información solicitada.

Fig 3 Responsable del Tratamiento

Fuente: El autor

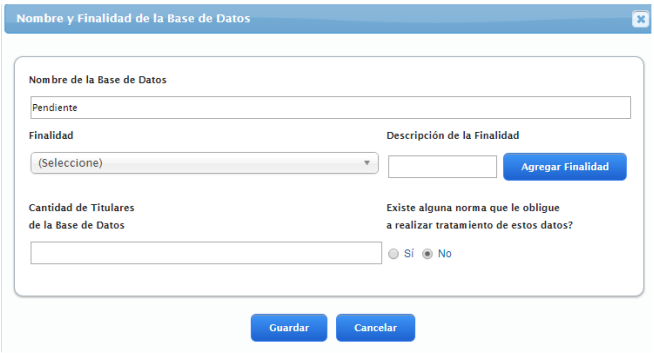
Al empezar a registrar las bases de datos nos pregunta cantidad de bases de datos a registrar, para registrar una base de datos se selecciona “Continuar Registro” como se muestra en la Fig. 4.

Fig 4 Inscripción de Base de Datos

Fuente: El autor

Se inicia con el registro de las bases de datos colocando el nombre de la base de datos, la finalidad, la cantidad de registros que tiene esta base, como se muestra en la fig. 5.

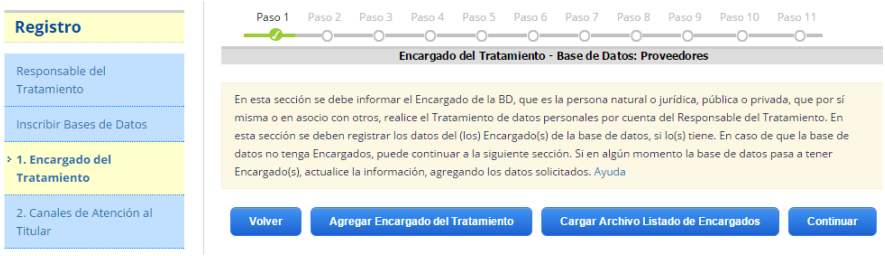
Fig 5 Inicio de Inscripción



Fuente: El autor

El Paso 1 (Fig. 6) se debe informar el encargado de la Base de Datos que es la persona natural o jurídica, pública o privada que se encarga del tratamiento de los datos de la base a registrar, si en algún momento se cambia de encargados se debe actualizar el registro.

Fig 6 Registro



Fuente: El autor

Paso 2 (Fig. 7 y 8) En esta sección se debe inscribir los canales de atención, los medios que el encargado o responsable a dispuesto como medio de comunicación para ejercer los derechos a que se refiere la Ley 1581 de 2012.

Fig 7 Canales de Atención

Fuente: El autor

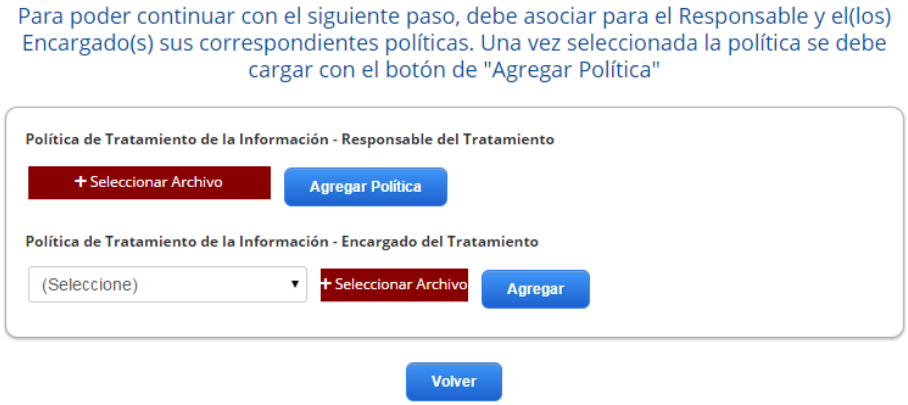
Fig. 8 Agregar Nuevo Canal

Fig 8 Agregar Nuevo Canal

Fuente: El autor

Para poder continuar con el siguiente paso se debe asociar las Políticas de Tratamiento de la Información, cargando el archivo con las políticas establecidas. Como lo muestra la Fig. 9.

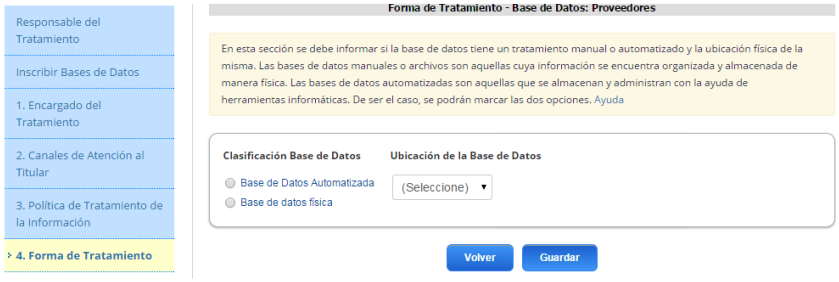
Fig 9 Políticas de Tratamiento de la Información



Fuente: El autor

En el paso 4 se debe informar si la base de datos es física o automatizada y donde se encuentra alojada, si se encuentra de ambas física y automatizada se deben marcar ambas opciones. Fig.10.

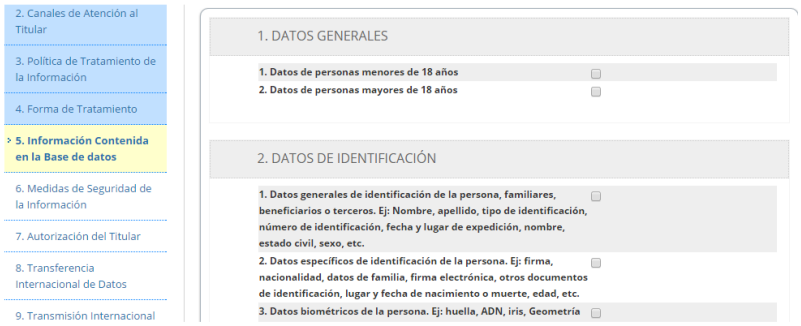
Fig 10 Forma de Tratamiento



Fuente: El autor

En el paso 5 se debe seleccionar la información que se tiene en cada base de datos, allí se dan varios opciones para escoger. Fig. 11.

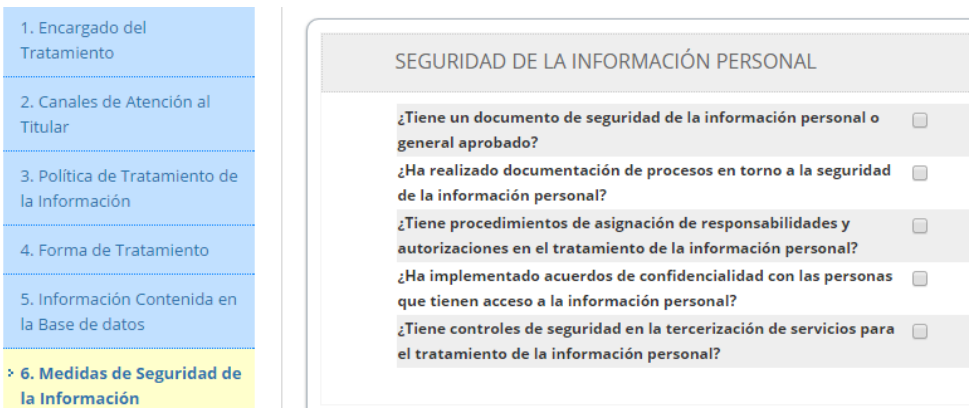
Fig 11 Información Base de Datos



En el paso 6 se escogen las medidas de seguridad de la información que se han implementado durante el desarrollo de este proyecto. Fig.12

Fig. 12 Medidas de Seguridad de la Información

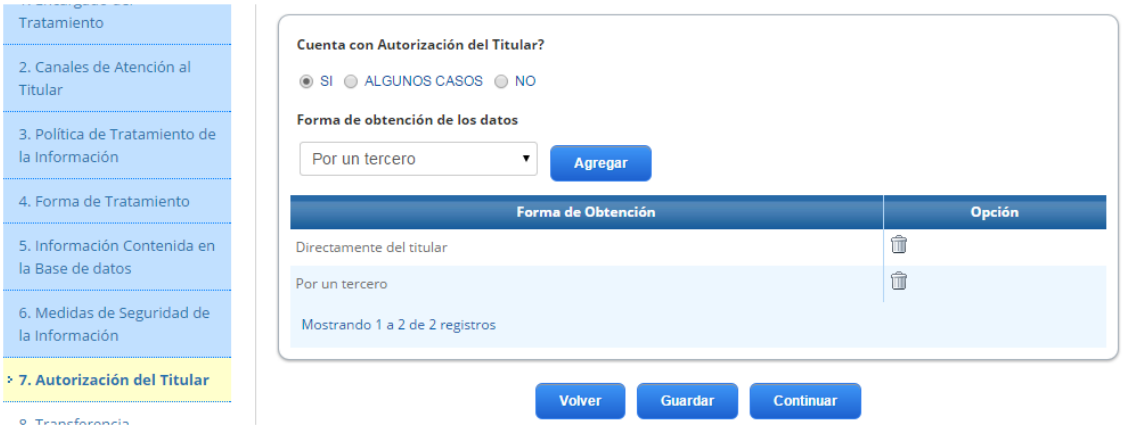
Fig 12 Medidas de Seguridad de la Información



Fuente: El autor

En el paso 7 se confirma si se tiene la autorización del titular de la información.

Fig 13 Autorización del titular



Fuente: El autor

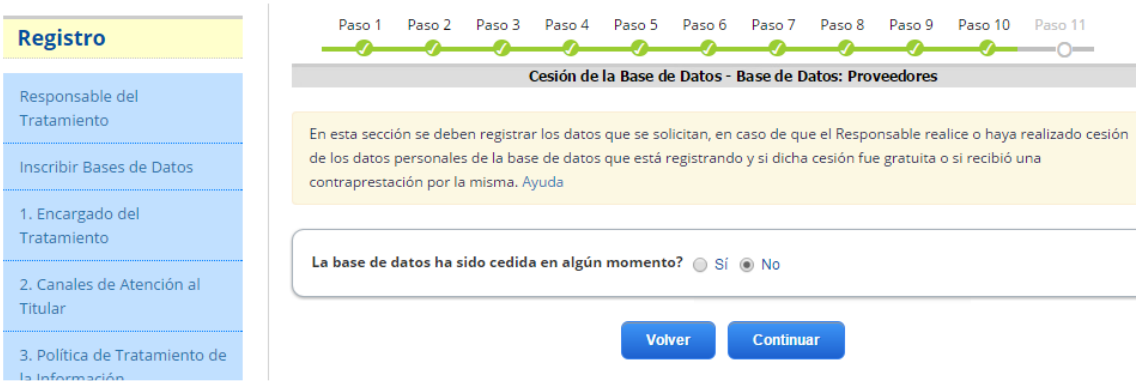
En el paso 8 se debe seleccionar si las bases de datos que se registran se van a realizar transferencias internacionales de los datos personales contenidas en ellas. (Fig. 14) Cuando se realiza la transferencia a un país que no proporciona un nivel adecuado de protección de datos se debe radicar una solicitud de conformidad del titular declarando la conformidad.

Fig 14 Transferencia Internacional de Datos

Fuente: El autor

Paso 10 en esta sección se debe registrar si en algún momento se ha cedido la base de datos registrada, si se ha hecho, si fue de forma gratuita o recibiendo una contraprestación económica. Fig. 15.

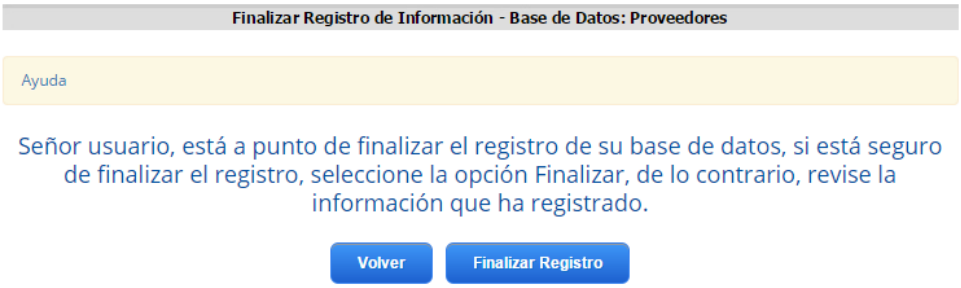
Fig 15 Cesión de la Base de Datos



Fuente: El autor

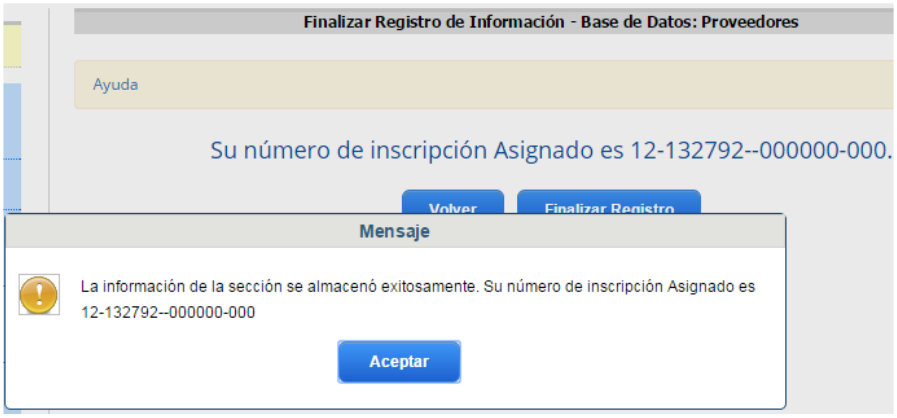
En el paso 11 (Fig. 16) se finaliza el registro o se revisa la información registrada.

Fig 16 Finalización del registro



El sistema arroga el número con el cual se radicó la base de datos ante la Superintendencia de Industria y Comercio, este es el fin del radicado de la base de datos.

Fig. 17 Fin del Radicado



Fuente: El autor