# GUÍA PRÁCTICA PARA LA PROTECCIÓN DE DATOS PERSONALES

## INTRODUCCIÓN

El presente documento contiene los lineamientos necesarios para la Protección de Datos Personales a cargo de INALAMBRIA INTERNACIONAL S.A.

Debido a la complejidad de las normas sobre protección de datos, a través de la presente guía se pone a disposición de la compañía y se explican los documentos y actividades requeridas para garantizar la protección de los datos personales recolectados por INALAMBRIA. En la guía se explican las actividades a adelantar así como los documentos específicos que es necesario diligenciar con la finalidad lograr el cumplimiento y adecuación de INALAMBRIA INTERNACIONAL S.A a la normativa vigente en materia de Protección de Datos Personales.

## ADECUACIÓN A LA NORMATIVA SOBRE PROTECCIÓN DE DATOS

### ¿Qué normativa debe ser implementada?

En el tratamiento de datos de carácter personal, todas las bases de datos tienen que cumplir con las obligaciones que les son exigibles en virtud de la Ley 1581 de 2012, de Protección de Datos de Carácter Personal.

### ¿Qué bases de datos de carácter personal se tratan regularmente?

En el desarrollo de la actividad diaria de la empresa se tratan datos de carácter personal relativos, entre otros, a trabajadores, clientes y contratistas. Estos datos de carácter personal reciben protección en virtud de la Ley Estatutaria de Protección de Datos (LEPD), siendo una de las obligaciones de INALAMBRIA INTERNACIONAL S.A establecer las medidas de seguridad pertinentes.

### ¿De qué ficheros de datos personales puede ser responsable?

Hay que identificar los ficheros de datos de carácter personal de los que es responsable INALAMBRIA INTERNACIONAL S.A, la determinación de un fichero de datos de carácter personal se hace en atención a la finalidad con la que se tratan los datos de carácter personal en él. Al interior de INALAMBRIA INTERNACIONAL S.A se han identificado los siguientes ficheros sin que eso implique que no puedan existir o ser creados otros:

- **Contratistas:** Contiene los datos personales de los contratistas, necesarios para la realización de diferentes funciones dentro de la sociedad.

- **Trabajadores:** Contiene los datos personales del personal vinculado laboralmente a la empresa.

- **Clientes:** Contiene los datos personales de las personas que trabajan en los clientes de los servicios de Inalambria.

La organización de los ficheros tiene por objeto facilitar a INALAMBRIA INTERNACIONAL S.A la implementación de las medidas de seguridad exigidas en virtud del Reglamento de Desarrollo de la LEPD. En los ficheros Trabajadores y Clientes se consideran incluidos datos de carácter personal que por su especial naturaleza suponen la necesidad de adoptar medidas de seguridad de nivel alto con el fin de garantizar su integridad y confidencialidad. De acuerdo a los datos que contiene el fichero de contratistas a este se aplicará el nivel básico de medidas de seguridad.

Los datos que son objeto de tratamiento en estos ficheros se encuentran relacionados en el documento "Contenido Lógico De Cada Fichero"

**¿Cómo se determinan los ficheros de datos de carácter personal?**

Sin perjuicio de la ayuda que se proporciona a través de este documento que tiene por objeto explicar qué es un fichero de datos de carácter personal, es necesario que cada responsable encargado del tratamiento del fichero de los datos pueda identificar con qué ficheros de datos cuenta, atendiendo a la finalidad con la que se tratan los datos de carácter personal.

**¿Qué información se tiene que proporcionar la empresa en el momento de recoger datos personales?**

Cuando se procede a recoger datos personales, por ejemplo, de candidatos a ser trabajadores o de clientes corporativos, es necesario incluir en el documento o medio que se utilice para ello una cláusula informativa que haga referencia a los siguientes aspectos:

- Existencia del fichero o tratamiento, finalidad de la recogida de los datos y destinatarios de la información.
- Carácter obligatorio o facultativo de la respuesta a las preguntas planteadas.
- Consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- Posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- Identidad y dirección del responsable encargado del tratamiento del fichero del tratamiento o, en su caso, de su representante.

**¿Servicios prestados por terceros que tengan acceso a datos de carácter personal?**

Para el desarrollo de las actividades propias de INALAMBRIA INTERNACIONAL S.A se contrata la prestación de servicios con terceros, en este caso nos encontramos ante un tercero que puede tener acceso a datos de carácter personal a cargo de la empresa. Desde la óptica de la normativa sobre protección de datos, esa tercera entidad se denomina encargado del tratamiento.

En los acuerdos o contratos que INALAMBRIA INTERNACIONAL S.A suscriba con estas entidades deberá incluirse una cláusula relativa al tratamiento de datos de carácter personal.

**¿Otras relaciones con terceros?**

Además de los contratos, acuerdos, convenios u otros que pueda haber con terceras entidades que prestan un servicio a INALAMBRIA INTERNACIONAL S.A y que implica el acceso a datos de carácter personal, es necesario determinar si se proporcionan los datos con determinadas finalidades a terceras entidades, como por ejemplo bancos, entidades comerciales, cooperativas, entidades públicas, etc. con el fin de implementar las medidas de seguridad pertinentes.

**¿Qué es el manual interno de políticas y procedimientos?**

El manual interno de políticas y procedimientos, previsto en el artículo 17 literal K, de la Ley Estatutaria 1581 de 2012, es un documento de obligado cumplimiento para el personal de INALAMBRIA INTERNACIONAL S.A que trata o accede a datos de carácter personal que se encuentren en soporte físico o electrónico y cuya aplicación tiene que realizarse por el responsable encargado del tratamiento del fichero del fichero.

**¿Cuáles son los niveles de medidas de seguridad?**

Existen tres niveles de seguridad que se aplican en virtud de los datos de carácter personal objeto de tratamiento:

- **Nivel básico:** Se aplica a todos los ficheros en los que se traten datos de carácter personal.

**- Nivel medio**: Aplicable a los ficheros en los que se traten datos de carácter personal relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, DANE entre otros.

Si en un fichero se trataran un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad de la persona sobre la que se recaban, deberán adoptarse algunas medidas de este nivel.

**- Nivel alto:** Se aplica si en el fichero se tratan datos sensibles de carácter personal relativos a la ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual entre otros.

**¿Qué nivel de medidas de seguridad tienen que aplicarse?**

En función de los datos que se encuentran actualmente en los ficheros, INALAMBRIA INTERNACIONAL S.A, conforme a la clasificación indicada en el punto anterior, aplica los niveles de medidas de seguridad correspondientes.

De modificarse los datos recogidos en los ficheros se debe proceder a actualizar la información correspondiente y verificar el nivel de medidas de seguridad a aplicar.

# GUÍA PRÁCTICA PROTECCIÓN DE DATOS PERSONALES

El presente documento tiene por objeto brindar instrucciones para la Protección de Datos Personales al interior de la empresa. A tal fin, en primer lugar se indican los documentos y en segundo lugar, por cada uno de dichos documentos se relatan las cuestiones prácticas a considerar para proceder a aplicar la normativa sobre protección de datos.

Es necesario que tenga presente que esta guía brinda los elementos necesarios para cumplir con la normativa vigente sobre protección de datos, siendo necesario los responsables encargados del tratamiento del fichero y aquellos que tienen acceso a datos personales adopten las medidas necesarias, tal y como se indica a lo largo de los documentos que aquí se adjuntan.

Los documentos que componen la presente guía son los siguientes:

**1. Documento Interno de Seguridad Básico:** En este documento se encuentran todas las normas que obligatoriamente deberá cumplir el personal de INALAMBRIA INTERNACIONAL S.A que tenga acceso a los datos de carácter personal y a los sistemas de información, referidos a los ficheros definidos en este documento.

**2. Documento Interno de Seguridad Alto:** Contempla todas las normas que obligatoriamente deberá cumplir el personal de INALAMBRIA INTERNACIONAL S.A que tenga acceso a los datos de carácter personal y a los sistemas de información, referidos a los ficheros definidos en este documento.

**3. Avisos de Privacidad:** En este Documento encontrará los adhesivos, que se deberán poner en aquellos lugares en donde se tengan cámaras de vigilancia, los avisos de seguridad para las comunicaciones de la empresa y el aviso de seguridad para las bases de datos que se tenían con anterioridad a la implementación.

**4. Protocolo de atención al interesado:** En este documento se presenta el esquema a seguir cuando un ciudadano ejerza alguno de sus derechos relativos a la Protección de Datos.

**5. Políticas de tratamiento Web:** En este apartado se encuentran las diferentes autorizaciones que se deben solicitar para el tratamiento de datos por vía web.

**6. Clausulas legales:** Incluye los modelos requeridos tanto para la recolección de datos como para la firma de contratos en los que se va a hacer cesión de datos personales.

**7. Manual de políticas y procedimientos:** En este documento se encuentra compilada y explicada la implementación realizada.

## DOCUMENTOS INTERNOS DE SEGURIDAD DOCUMENTOS I Y II

**¿Qué son los documentos de seguridad?**

Los documentos de seguridad son un instrumento obligado por la normativa, no disponer de ellos supone una infracción.

Este instrumento tiene como fin recoger las reglas de seguridad que tienen que cumplir los responsables encargados del tratamiento de los ficheros para proteger los datos de carácter personal.

Se publican **dos documentos de seguridad** que corresponden a los niveles de seguridad de los ficheros que tiene INALAMBRIA INTERNACIONAL S.A (básico y alto). Atendiendo al nivel de seguridad de los ficheros, cada persona que tenga acceso a estos deberá cumplir y conocer el documento de seguridad del nivel correspondiente.

**¿Qué se debe hacer con los documentos de seguridad?**

En el caso de recibir una inspección por parte de la Superintendencia de Industria y Comercio, se deben presentar los documentos de seguridad para así demostrar que la sociedad cumple con normatividad vigente sobre el particular.

**¿Quién debe conocer el contenido de los documentos de seguridad?**

Estos documentos de seguridad deben ser conocidos por toda persona de INALAMBRIA INTERNACIONAL S.A que tenga acceso a datos personales que estén en un fichero o lista de personas ya sea de forma digital o física. De acuerdo al fichero de datos a que tengan acceso deberán conocer y aplicar el documento de seguridad correspondiente.

**¿En qué partes se divide un documento de seguridad?**

Los documentos de seguridad se componen de **dos partes:**

**1. Teórica:** Recoge las reglas que exige la Ley Estatutaria 1581 de 2012 de Protección de Datos Personales y el decreto 1377 de 2013. Esta parte teórica se caracteriza por ser fija **el responsable encargado del tratamiento del fichero no debe modificarla en ningún aspecto.**

**2. Anexos:** Esta parte es dinámica, y se debe modificar siempre que haya un cambio en la información que contiene cada fichero.

Por ejemplo, cuando varía el contenido de un fichero porque se le añade un campo nuevo, se debe actualizar el contenido del Anexo que describe el contenido lógico de los ficheros para que quede constancia de que se ha creado un campo y que el fichero es distinto de cómo era cuando se rellenó el Anexo correspondiente en el documento de seguridad.

En la parte dinámica de los documentos de seguridad distinguimos los siguientes Anexos, dependiendo de que se trate del documento de seguridad de nivel básico o alto:

**NOTIFICACIONES a LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE HABER PROCEDIDO A LA INSCRIPCIÓN DE CADA UNO DE LOS FICHEROS.**

Para efectos de los trámites de registro de las Bases de Datos ante la Superintendencia de Industria y Comercio – SIC, se propone la siguiente tabla por cada fichero de nivel básico o alto

según sea el documento de seguridad en la que se recoge un resumen de la información que se ha proporcionado al Registro nacional de Protección de Datos.

En cada uno de los ficheros se debe hacer constar **el Código de inscripción del fichero, el número de salida y la fecha en la que se realizó la inscripción**. Datos todos estos que serán facilitados cuando se confirme la inscripción por el Registro General de Protección de Datos.

| DATOS DE INSCRIPCIÓN | |
|---|---|
| Nombre de inscripción | |
| Código de Inscripción | |
| Fecha de inscripción | |

En el caso de que el fichero sea Modificado en un futuro deberán rellenarse las casillas que figuran bajo el epígrafe de DATOS DE MODIFICACIÓN.

| DATOS DE MODIFICACIÓN | |
|---|---|
| Nombre de inscripción | |
| Código de Inscripción | |
| Nº Registro Salida | |
| Fecha de modificación | |
| Apartados modificados | |
| Persona física que notifica | |

Al final de cada tabla se hace referencia a la PERSONA QUE EFECTÚA LA NOTIFICACIÓN, información ésta que también deberá ser completada una vez se realice esta actividad.

| PERSONA FÍSICA QUE EFECTÚA LA NOTIFICACIÓN | |
|---|---|
| Nombre y apellidos | |
| Documento de identidad | |
| Puesto desempeñado | |
| Dirección profesional | |
| Teléfono | |

## FICHEROS Y SU DESCRIPCIÓN.

Deben contener la información básica del fichero como es su nombre, ubicación, finalidad, descripción del contenido y encargado del tratamiento del fichero entre otros.

En tal sentido, se deben enunciar las medidas de seguridad de obligatorio cumplimiento. En el apartado de Observaciones se explican las medidas de seguridad que deben ser implementadas por el responsable encargado del tratamiento del fichero.

## CONTENIDO LÓGICO DE CADA FICHERO.

El contenido lógico de los ficheros , es decir la información de los campos de la base de datos, se determinará conforme a las instrucciones del área responsable, validados por la Dirección Legal.

## INVENTARIO DE SOPORTES FÍSICOS EN LOS QUE SE ALMACENAN DATOS DE CARÁCTER PERSONAL.

El control del inventario se realizará mediante una tabla a través de la cual podrá el responsable encargado del tratamiento del fichero efectuar el inventario de los soportes, tal y como exige el Reglamento de la LEPD.

## DELEGACIÓN DE AUTORIZACIONES Y AUTORIZACIONES NECESARIAS PARA EL TRATAMIENTO DE DATOS PERSONALES.

Cada área proporcionará los modelos las autorizaciones relativas al tratamiento de datos fuera de los locales de ubicación del fichero y a la recuperación de los datos, puesto que el Reglamento de la LEPD obliga al responsable encargado del tratamiento del fichero a autorizar por escrito su tratamiento fuera del local en que se halle el fichero.

## CIRCULARES COMUNICADAS A TODA PERSONA QUE TIENE ACCESO A DATOS PERSONALES

Se prepararán los modelos de circulares que deben ser comunicadas por el responsable encargado del tratamiento del fichero del tratamiento del fichero a todas las personas que tienen acceso a los datos contenidos en él, circular informando el registro y manejo de incidencias y circular sobre seguridad de datos personales para las personas que tienen acceso a los ficheros.

**Adicionalmente a los procedimientos indicados, en el documento Interno de seguridad Alta se contemplan los siguientes registros:**

## - REGISTRO DE ENTRADA DE SOPORTES

## - REGISTRO DE SALIDA DE SOPORTES

## OBSERVACIÓN FINAL

**Cuando exista un tratamiento de datos por cuenta de terceros se deberán aplicar las mismas políticas cláusulas contempladas en el presente documento.**

Desde el punto de vista de la protección de datos, y siendo una obligación del responsable encargado del tratamiento del fichero el mantener informado al personal de la obligación de cumplir las medidas de seguridad, queremos advertir de la necesidad de controlar los usos que sin estar previstos puedan realizarse de los ficheros como pueden ser:

- Uso de ordenadores personales de los trabajadores, en los que se encuentren datos de carácter personal.
- Retirar de la empresa ordenadores portátiles u otro tipo de dispositivos donde se archiven datos de carácter personal.
- Acceso no autorizado a archivos físicos donde se encuentren registrados datos de carácter personal.
- Acceso a ficheros personales de un trabajador por otro trabajador.

En todos estos casos los trabajadores deben observar las medidas de seguridad que corresponda de la misma forma que se describen en los documentos de seguridad.

## AVISOS DE PRIVACIDAD

En este Documento encontrará los adhesivos, que se deberán poner en aquellos lugares en donde se tengan cámaras de video vigilancia, avisos de seguridad para las comunicaciones de la universidad y el aviso de seguridad para las bases de datos que se tenían con anterioridad a la implementación con el fin de que esta queden regularizadas conforme a la ley.

## PROTOCOLO DE ATENCIÓN AL INTERESADO

El protocolo de atención al interesado se administrará desde el sistema de PQR que ya tiene implementada la empresa a cargo de la Dirección Legal y tiene por objeto facilitar al responsable:

1. Modelos de cartas a utilizar para ejercer los derechos que le otorga la ley. (Rectificación, cancelación u oposición).

2. Modelo de cartas para la contestación de derechos.

3. Normas internas de actuación con relación al tratamiento de datos de carácter personal. Documento 4 “Protocolo de atención al interesado”

**Ejercicio de un derecho**

Si alguien, bien sea un trabajador u otra persona de quien la sociedad tiene datos de carácter personal, ejercitase sus derechos, se debe proceder de la siguiente manera:

1. Leer detenidamente el apartado correspondiente al derecho ejercido, atendiendo a las explicaciones que se le dan en el mismo.

2. Comprobar que la solicitud de ejercicio del derecho contiene todos los requisitos que se indican en el apartado correspondiente del Protocolo.

3. Si no fuera así, facilitar al interesado el modelo de solicitud de ejercicio de derecho que se proporciona.

4. Para responder al ejercicio del derecho, se recomienda hacer uso del modelo de carta de respuesta al ejercicio del derecho de acceso completando los apartados con la información que corresponda.

5. Tener en cuenta que la respuesta al ejercicio del derecho de acceso tiene que hacerse dentro de los plazos que se indican en el Protocolo.

## POLITICAS DE TRATAMIENTO WEB

En este apartado se encuentran las diferentes autorizaciones que se deben solicitar para el tratamiento de datos por vía web como son:

- Autorización para comunicaciones electrónicas (correos)-
- Cláusula informativa (para stikers, publicidad o web)
- Cláusula de autorización web.

## CLAUSULAS LEGALES

Cuando se procede a recoger datos de carácter personal es necesario informar al titular de los mismos del uso que se va a hacer de estos y por tal razón se debe:

Incluir en el formulario que se utilice para recoger los datos de carácter personal (físico o digital) una cláusula informativa para la cesión o comunicación de datos.

Para utilizar la cláusula informativa modelo recuerde que tiene que indicar la finalidad concreta y determinada para la que se comunican los datos.

Si el responsable encargado del tratamiento del fichero comunica los datos a una tercera entidad, tiene que pedir el consentimiento al dueño de los datos e incluir en el formulario que se utilice para recoger los datos de carácter personal (físico o digital), la cláusula que se le proporciona, adecuándola al caso concreto.

En todos los casos, INALAMBRIA INTERNACIONAL S.A debe pedir el consentimiento del interesado para la comunicación o cesión de datos.

Por lo tanto, el responsable encargado del tratamiento del fichero en este caso debe:

1. Incluir una cláusula informativa solicitando el consentimiento del interesado, pudiendo hacer uso del modelo que se le proporciona en el documento 6.1 Cláusula informativa para la cesión o comunicación de datos.

2. Para utilizar la cláusula informativa modelo recuerde que tiene que indicar:
a) Quién es el cesionario o destinatario de la cesión o comunicación.
b) La finalidad concreta y determinada para la que se comunican los datos

Cuando INALAMBRIA INTERNACIONAL S.A contrata con una tercera empresa la prestación de un servicio que implica necesariamente el tratamiento de datos bajo su responsabilidad, debe incorporar en el contrato una cláusula que recoja el compromiso del tercero de tratar los datos con el mismo nivel de protección que emplea la Universidad

Para ello los pasos que debe seguir son los siguientes:

Debe incluir la cláusula especificando lo que hace referencia a la entidad que presta el servicio a INALAMBRIA INTERNACIONAL S.A.

En el caso de que sea la compañía quien preste el servicio a un tercero y este servicio implique el manejo de datos personales bajo responsabilidad de este tercero se debe:

Incluir la cláusula correspondiente realizando las concreciones que en él se especifican referentes a la entidad a la que se presta el servicio.

**Acceso a los datos de carácter personal por empresas externas**

En relación con el acceso a los datos por terceros, tiene que constar que este cumpla con los requisitos exigidos por la LEPD. En este sentido, es necesario que se compruebe que el contrato que se firme con dicha entidad contenga una cláusula que cumpla con dichos requisitos o, en otro caso, que se incluya esta mediante la elaboración de un otrosí.