

POLITICA DE PROTECCIÓN DE DATOS PERSONALES	
IN-11001-29	Pág. 1 de 17

Contenido

1	INTRODUCCIÓN	2
2	DEFINICIONES Y CONCEPTOS	2
3	PRINCIPIOS LEY DE PROTECCIÓN DE DATOS	3
4	DISPOSICIONES GENERALES.....	4
5	TRATAMIENTOS DATOS PERSONALES	7
	Titular Responsable Encargado.....	9
6	SEGURIDAD DE LA INFORMACION.....	10
6.1	PROPÓSITO.....	10
6.2	INTRODUCCION	10
6.3	POLITICA DEL PROGRAMA DE SEGURIDAD DE INFORMACION.....	11
6.4	OBJETIVOS DEL PROGRAMA DE SEGURIDAD DE INFORMACION... 11	
6.4.1	Incorporar a la estrategia del negocio las mejores prácticas de seguridad de información de clase mundial.	12
6.4.2	Establecer prácticas para el control de acceso físico y lógico a las aplicaciones y sistemas que soportan los procesos del negocio.	12
6.4.3	Establecer medidas de prevención para mantener la continuidad de los procesos del negocio.....	12
6.4.4	Generar una cultura interna de clasificación y manejo de información propia y de terceros.	12
6.4.5	Minimizar el impacto de incidentes de seguridad de información siguiendo un control de cambios en ambientes productivos de sistemas de información.....	12
6.4.6	Asegurar el cumplimiento del marco normativo y legal aplicable en la operación de la empresa.....	12
6.4.7	Establecer auditorias y controles periódicos internos para el mantenimiento, revisión y mejora de los controles de seguridad dentro del PSI. 12	
6.5	ALCANCE	12
6.6	PROGRAMA DE SEGURIDAD DE INFORMACIÓN.....	12
6.6.1	Requisitos generales	12
6.7	Políticas y procesos a Implementar	13
6.8	ESTRUCTURA DEL CSI.....	13
6.9	AUDITORIAS INTERNAS AL PSI	14
6.10	PLAN DE CONTINUIDAD DE LA INFRAESTRUCTURA DE TI.....	14
7	EXCEPCIONES	14
8	BASE DE DATOS Y REGISTRO DE LA INFORMACION.....	15
9	INFORMACIÓN PARA EL REGISTRO	16

1 INTRODUCCIÓN

A partir de la entrada en vigencia de la ley 1581 de 2012 de protección de datos, la cual tiene por objeto desarrollar el Derecho Constitucional que tienen todas las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bases de datos o archivos; crea en COBRES DE COLOMBIA S.A.S. la necesidad de definir el manejo y control de la información registrada en estas bases, a través de la detección de las principales incidencias en la empresa en cuanto al ámbito de aplicación, de los deberes establecidos y a la adopción de mecanismos de protección para cumplimiento de la misma.

Con base en lo anterior se desarrolla el presente manual, en el cual se define los aspectos establecidos en la Ley para el cumplimiento de esta y establecer el control y seguimiento a través de un esquema de flujo de información.

2 DEFINICIONES Y CONCEPTOS

Para poder conocer y aplicar la Ley adecuadamente, es necesario tener claridad en algunos conceptos que constituyen un elemento fundamental para las disposiciones que la contienen y que se mencionan a continuación:

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

Base de datos: Conjunto organizado de datos personales que sea objeto de tratamiento.

Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Encargado del tratamiento: Persona natural o jurídica, pública o privada,

que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento.

POLITICA DE PROTECCIÓN DE DATOS PERSONALES	
IN-11001-29	Pág. 3 de 17

Responsable del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos

Titular: Persona natural cuyos datos personales sean objeto de Tratamiento.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Datos personales: se consideran datos personales los nombres y apellidos, el estado civil, la dirección, los datos laborales, los datos bancarios, las creencias religiosas, la orientación sexual entre otros.

Habeas data: es el Derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

3 PRINCIPIOS LEY DE PROTECCIÓN DE DATOS

Los principios de la protección de datos constituyen un pilar importante y son de obligatorio cumplimiento para el personal que interviene en el tratamiento de datos personales.

- a) Principio de legalidad en materia de Tratamiento de datos: El Tratamiento a que se refiere la Ley es una actividad reglamentada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.
- b) Principio de finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.
- c) Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

POLITICA DE PROTECCIÓN DE DATOS PERSONALES	
IN-11001-29	Pág. 4 de 17

d) Principio de veracidad o calidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

e) Principio de transparencia: En el Tratamiento debe garantizarse el derecho del Titular a obtener del responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

f) Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la Ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la Ley; Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley.

g) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

h) Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de esta.

4 DISPOSICIONES GENERALES

De acuerdo con lo establecido en La Ley de protección de datos en su Título VI, existen unos deberes de obligatorio cumplimiento y que se detallan a continuación:

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

IN-11001-29

Pág. 5 de 17

Deberes de los Responsables del Tratamiento. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la Ley y en otras que rijan su actividad:

- a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del Derecho de hábeas data.
- b) Solicitar y conservar, en las condiciones previstas en la Ley, copia de la respectiva autorización otorgada por el Titular.
- c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.
- g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.
- h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la Ley.
- i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
- j) Tramitar las consultas y reclamos formulados en los términos señalados en la Ley.
- k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la Ley y en especial, para la atención de consultas y reclamos.

POLITICA DE PROTECCIÓN DE DATOS PERSONALES	
IN-11001-29	Pág. 6 de 17

- l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
- m) informar a solicitud del Titular sobre el uso dado a sus datos.
- n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
- o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Deberes de los Encargados del Tratamiento, Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la Ley y en otras que rijan su actividad:

- a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la Ley.
- d) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.
- e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la Ley.
- f) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente Ley y en especial, para la atención de consultas y reclamos por parte de los Titulares.
- g) Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la Ley.

POLITICA DE PROTECCIÓN DE DATOS PERSONALES	
IN-11001-29	Pág. 7 de 17

- h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;

- i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.

- j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.

- k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

- l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Parágrafo. En el evento en que concurren las calidades de Responsable del Tratamiento y Encargado del Tratamiento en la misma persona, le será exigible el cumplimiento de los deberes previstos para cada uno.

5 TRATAMIENTOS DATOS PERSONALES

El tratamiento de la información personal de los trabajadores se realiza exclusivamente para fines laborales, control de acceso porterías, **capacitaciones** y registro de contratistas, exceptuando las que indica la ley.

La información es suministrada a través de unos formatos y esta información es almacenada en una base de datos del **Responsable del tratamiento** a la cual pueden acceder las personas autorizadas en el manejo de dicha información

Definición de Roles para Base de Datos de Persona/

Responsable del Tratamiento: Representante Legal

Responsable del Tratamiento: **Encargado del área**

Encargado del tratamiento:

POLITICA DE PROTECCIÓN DE DATOS PERSONALES	
IN-11001-29	Pág. 8 de 17

***Encargados de los Sistemas de Gestión
Personal de Recursos Humanos***

Titular: Trabajador

Definición de Roles para Base de Datos de Visitantes:

Responsable del Tratamiento: ***Encargados de los Sistemas de Gestión***

Encargado del tratamiento:

***Encargados de los Sistemas de Gestión
Personal de Recursos Humanos***

Titular: Visitantes

Definición de Roles para Base de Datos de Contratistas:

Responsable del Tratamiento: ***Gerente de Operaciones/*** Jefe de Mantenimiento

Encargado del tratamiento:

Encargado de los Sistemas de Gestión

Titular: Contratistas

Definición de Roles para Base de Datos de Clientes Actuales y Potenciales.

Responsable del Tratamiento: Gerente Comercial

Encargado del tratamiento:

Ingeniero de Mercadeo y ventas

Analista Mercadeo

Definición de Roles para Base de Datos de Proveedores:

Responsable del Tratamiento: ***Jefe de Compras***

Encargado del tratamiento:

Analista de Compras

Definición de Roles para Base de Datos de Transportistas:

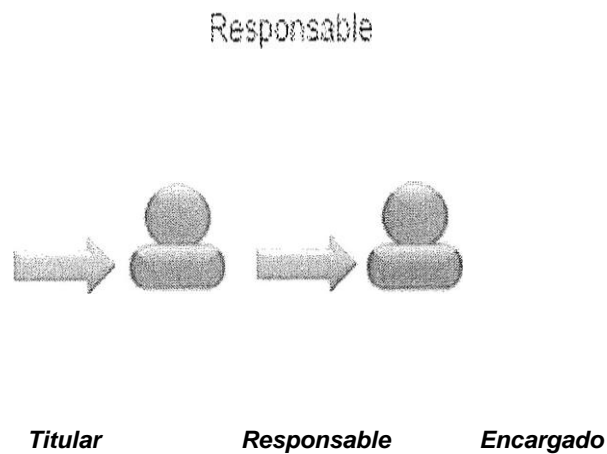
Responsable del Tratamiento: Jefe de Distribución

Encargado del Tratamiento: Supervisor de Distribución

Tipos de Tratamiento

POLITICA DE PROTECCIÓN DE DATOS PERSONALES	Pág. 9 de 17
IN-11001-29	

El tratamiento de datos conlleva a alguno de los esquemas presentados a continuación:



Premisas.

Informar al interesado previamente al tratamiento de los datos que no estén bajo el principio de finalidad.

Solicitar solo los datos necesarios y guardar la confidencialidad de la información.

Facilitar a las personas el derecho al acceso, rectificación y actualización de la información.

Tratamiento de una solicitud de revisión o reclamación

En caso de presentarse alguna solicitud de revisión o reclamación de la información se debe tener en cuenta lo siguiente:

VI. Toda persona que tenga acceso a las bases de datos debe firmar una autorización de confidencialidad de la información.

VII. Validar la autorización expresa del empleado para los datos de información solicitada.

POLITICA DE PROTECCIÓN DE DATOS PERSONALES	
IN-11001-29	Pág. 10 de 17

VIII. En caso de tener la autorización debidamente firmada, se procede a suministrar la información.

IX. En caso de no tener la autorización expresa se debe avisar al solicitante y al empleado.

X. Al momento de recibir las solicitudes de actualización o de rectificación de la información esta debe ser procesada a más tardar a los cinco (5) días siguientes a la recepción de dicha solicitud.

XI. Llevar registro de las solicitudes de información.

XII. Llevar registro de las solicitudes de reclamación.

El canal para este tratamiento es el punto de atención ubicado en las oficinas de Cobres de Colombia y el correo electrónico.

Toda solicitud de revisión o reclamación debe presentarse por escrito informando expresamente que dato o información no coincide con lo reportado y adjuntando soporte de la información suministrada a Cobres de Colombia

6 SEGURIDAD DE LA INFORMACION

6.1 PROPÓSITO

Se definió un Programa de Seguridad de Información (PSI) que Cobres de Colombia ha establecido con el fin de garantizar la confidencialidad, integridad y disponibilidad de sus activos de información y procesos de negocio.

6.2 INTRODUCCION

Aplicado de acuerdo con el alcance definido en este documento. La organización de Cobres de Colombia forma parte del alcance del PSI es responsable de generar las acciones y establecer los controles necesarios para satisfacer los requerimientos de Seguridad de Información (confidencialidad, integridad y disponibilidad) de sus activos.

POLITICA DE PROTECCIÓN DE DATOS PERSONALES	
IN-11001-29	Pág. 11 de 17

6.3 POLITICA DEL PROGRAMA DE SEGURIDAD DE INFORMACION

La política de seguridad de la información fue establecida por la Gerencia General y es considerada un soporte básico para lograr en tiempo y forma los objetivos del PSI establecidos.

La política de seguridad de la información se revisará anualmente o antes si se considera necesario por el Comité de Gerencia.

Cualquier cambio será informado a todo el personal a través de los mecanismos de comunicación de Cobres de Colombia.

A continuación, se enuncia la política de seguridad de información de Cobres de Colombia:

"En Cobres de Colombia S.A.S estamos comprometidos con la continuidad de nuestros procesos de negocio, reduciendo el riesgo a un nivel aceptado por la organización e impulsando una cultura de clasificación de información, a fin de proteger la confidencialidad, integridad y disponibilidad de la información propia y de terceros, cumpliendo el marco normativo y legal aplicable".

Aprobado por:

Yolanda Ramirez Muriel

Gerente General

Septiembre 2015

6.4 OBJETIVOS DEL PROGRAMA DE SEGURIDAD DE INFORMACION

Los objetivos del PSI son:

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

IN-11001-29

Pág. 12 de 17

- 6.4.1 Incorporar a la estrategia del negocio las mejores prácticas de seguridad de información de clase mundial.
- 6.4.2 Establecer prácticas para el control de acceso físico y lógico a las aplicaciones y sistemas que soportan los procesos del negocio.
- 6.4.3 Establecer medidas de prevención para mantener la continuidad de los procesos del negocio.
- 6.4.4 Generar una cultura interna de clasificación y manejo de información propia y de terceros.
- 6.4.5 Minimizar el impacto de incidentes de seguridad de información siguiendo un control de cambios en ambientes productivos de sistemas de información.
- 6.4.6 Asegurar el cumplimiento del marco normativo y legal aplicable en la operación de la empresa.
- 6.4.7 Establecer auditorias y controles periódicos internos para el mantenimiento, revisión y mejora de los controles de seguridad dentro del PSI.

6.5 ALCANCE

El Programa de Seguridad de Información abarca todos los activos e infraestructura de TI que soportan los procesos de negocio de Cobres de Colombia.

6.6 PROGRAMA DE SEGURIDAD DE INFORMACIÓN**6.6.1 Requisitos generales**

Cobres de Colombia está estableciendo e implementado un Programa de Seguridad de Información (PSI), el cual es operado, monitoreado, revisado, mantenido y mejorado continuamente, lo anterior con el objetivo de alcanzar los niveles apropiados de confidencialidad, integridad y disponibilidad de la información que requiere la organización.

Para el diseño e implementación del PSI, se adoptó un enfoque de procesos basado en el llamado modelo PHVA o Círculo de la Mejora Continua (PHVA _Planear, Hacer, Verificar, Actuar,). Es este también es utilizado por la Norma ISO

POLITICA DE PROTECCIÓN DE DATOS PERSONALES	Pág. 13 de 17
IN-11001-29	

27001 :2005 para el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de Información:

Bajo esta práctica de mejora continua se definen las siguientes fases:

Planear: Establecimiento y Gestión de PSI

Hacer: Implementación y Operación del PSI

Verificar: Monitoreo y Revisión del PSI

Actuar: Mantenimiento y Mejora del PSI

6.7 Políticas y procesos a Implementar

Nombre	Identificador
Política de Clasificación de Información	PL-SI-002
Política de Control de Accesos a Datos	PL-SI-003
Política de Control de Cambios de TI	PL-SI-004
Política de Auditoría Interna de Seguridad de Información	PL-SI-005
Proceso de Clasificación de Información	PR_ SI 002
Proceso de Control de Accesos a Datos	PR_ SI _003
Proceso de Control de Cambios de TI	PR_ Si -004
Proceso de Auditoría Interna de Seguridad de Información	PR_ S I -005

6.8 ESTRUCTURA DEL CSI

La Gerencia General de Cobres de Colombia se compromete al establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora del PSI mediante el CSI, para proteger la información de la compañía relacionada con el alcance definido.

La estructura del CSI está conformada en los siguientes niveles:

Comité de Gerencia

Gerentes de áreas

Jefes de Procesos

Áreas de Soporte al CSI

Comité Gerencia	Comité de Seguridad de Información (CSI)
-----------------	--

POLITICA DE PROTECCIÓN DE DATOS PERSONALES	Pág. 14 de 17
IN-11001-29	

Gerente Comercial y Operaciones	Comité de Seguridad de Información (CSI)
Encargados de los sistemas de gestión	Comité de Seguridad de Información (CSI)

6.9 AUDITORIAS INTERNAS AL PSI

Los procesos, áreas y servicios que conforman el alcance son auditados **cuando sea requerido**, estas auditorías internas son en materia de seguridad de información con el propósito de determinar si el PSI:

- a. Es conforme con los requisitos de seguridad de información identificada y establecida por Cobres de Colombia, así como leyes y regulaciones relevantes.
- b. Se ha implementado, se mantiene y se ejecuta de forma efectiva.
- c. Se desarrolla conforme se esperaba.

6.10 PLAN DE CONTINUIDAD DE LA INFRAESTRUCTURA DE TI

Se está gestionando la Continuidad de Negocio de Cobres de Colombia mediante los siguientes planes de **soporte de infraestructura tecnológica, mediante servicios del área de sistemas de Centelsa:**

Nombre	Identificador
Intranet	DR-SI-001
Sistema Peoplesoft	DR-SI-003

Y en Cobres de Colombia,

Nombre	Identificador
Sistema SAP	Estrategia de backup SAP Centelsa CNC
Backup Intranet	M.DE.400.008 CEN

7 EXCEPCIONES

No se requiere autorización para suministrar la información en los siguientes Casos:

POLITICA DE PROTECCIÓN DE DATOS PERSONALES	
IN-11001-29	Pág. 15 de 17

- a. Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- b. Datos de naturaleza pública.
- c. Casos de urgencia médica o sanitaria.
- d. Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- e. Datos relacionados con el Registro Civil de las Personas.

8 BASE DE DATOS Y REGISTRO DE LA INFORMACION

Cobres de Colombia de acuerdo con la normatividad vigente en esta materia, hará el registro ante el Registro Nacional de Bases de Datos (RNBD) administrado por la Superintendencia de Industria y Comercio, el cual es el directorio de las bases de datos sujetas a tratamiento que operan en el país y es de libre consulta para los ciudadanos.

Base de Datos de Trabajadores: Es la base de datos automatizada que contiene datos de las personas vinculadas laboralmente con Cobres de Colombia y cuya finalidad es el cumplimiento de disposiciones legales y manejo de procesos internos. El tratamiento de los datos con fines diferentes a los derivados de la relación laboral deberá contar con la aprobación del titular a través del formato de autorización y recolección de uso de datos personales implementado por Cobres de Colombia para este tratamiento.

Base de Datos Visitantes: Es la base de datos manual que contiene datos de las personas que visitan e ingresan a las instalaciones de la compañía y cuya finalidad es el cumplimiento de las disposiciones legales y el cumplimiento de protocolos de seguridad establecidos por la compañía.

Base de Datos Contratistas: Es la base de datos manual que contiene datos de los contratistas de Cobres de Colombia y cuya finalidad es el cumplimiento de las disposiciones legales y manejo de procesos internos de salud y seguridad en el trabajo y de seguridad física de la compañía.

Base de datos de Clientes Actuales y potenciales: Es la base de datos manual que contiene datos personales de los Clientes actuales y potenciales de Cobres de Colombia y cuya finalidad es el suministrar información de actualidad y novedades sobre productos o servicios que ofrece Cobres de Colombia.

Base de datos de proveedores: Es la base de datos automatizada que contiene datos de los proveedores de la compañía y cuya finalidad es el cumplimiento de

POLITICA DE PROTECCIÓN DE DATOS PERSONALES	
IN-11001-29	Pág. 16 de 17

las disposiciones legales y el cumplimiento de los procedimientos establecidos por la compañía.

Bases de datos Transportistas: Es la base de datos manual que contiene datos de los transportistas de la compañía y cuya finalidad es el cumplimiento de las disposiciones legales y el cumplimiento de los procedimientos establecidos por la compañía.

Bases de datos Directorio Activo: Es la base de datos automatizada que contiene datos de los usuarios de sistemas de la compañía y cuya finalidad es tener acceso a la red y correos corporativos.

9 INFORMACIÓN PARA EL REGISTRO

Este registro se debe realizar en la página de la superintendencia de Industria y comercio en el siguiente enlace:

BASES DE DATOS	REGISTRO
Obtención de datos y manejo de la información. Base Datos de personal Base Datos Visitantes Base Datos Contratistas Base Datos Clientes Actuales y Potenciales. Base Datos Proveedores Base Datos Transportistas. Base Datos Directorio Activa.	Información requerida para el Registro Nacional de Datos Bases 1. Datos Responsable del tratamiento de las bases de datos 2. Datos Encargado(s) del tratamiento de la base de datos. 3. Canales para que los titulares ejerzan sus derechos. 4. Nombre Bases de Datos 5. Forma de tratamiento de la base de datos (Manual y/o automatizada) 6. Política de Tratamiento de la información

POLITICA DE PROTECCIÓN DE DATOS PERSONALES	Pág. 17 de 17
IN-11001-29	

4. HISTORIAL DE CAMBIOS.

FECHA	ELABORACION, No: MODIFICACION	MOTIVO	FIRMA NOTIFICADO	POSEEDOR
06-11-2019	1	Nueva codificación y actualización de cargos		

ELABORADO POR: JEFE METROLOGIA			
FECHA DE VIGENCIA: 17 agosto 2015			
Revisado por: Gerente Comercial		Aprobado por: Gerente Operaciones	
NUMERO MODIFICACIÓN: 1	DE	REEMPLAZA A: IN-11-29	FECHA DE MODIFICACIÓN: 13/NOV/2019