PUBLICACIÓN

La Cooperativa dará a conocer a sus empleados y directivos, el Manual del SGSI y demás información relevante respecto a las políticas de seguridad aprobadas por el Consejo de Administración. Dicha información estará publicada en la Intranet (red interna) y será de uso exclusivo de empleados y directivos.

El público en general podrá consultar la información de interés respecto a la Política de Seguridad de la Información en la página web de la Cooperativa.

La Política de Medios Sociales y de Tratamiento de Datos estará disponible en la página web y redes sociales de la Cooperativa.

POLITICAS DE MEDIOS SOCIALES

CONTENIDO:

La Cooperativa del Magisterio CODEMA dispone de un portal web y tres canales oficiales en redes sociales, donde reposa información sobre eventos, horarios y puntos de atención, cursos, convenios, información corporativa y demás información relevante.

Considerando lo anterior, deberá tenerse en cuenta:

Las redes sociales contendrán, enlaces que apunten a la página web, para obtener información en profundidad sobre dicho contenido.

La presencia de cualquier servicio en una red social debe fomentar la participación sólo si permite el diálogo abierto con los ciudadanos.

El canal para remisión de sugerencias, reclamaciones o peticiones de información deberá ser a través del link contáctenos de la página web de la Cooperativa y no deberá ser sustituido por la comunicación a través de redes sociales.

COMENTARIOS:

Será decisión de la Cooperativa permitir o no la publicación de comentarios de la ciudadanía en su perfil en la red social. Igualmente, deberá tenerse en cuenta lo siguiente:

Deberán respetarse las opiniones de los ciudadanos, evitando cualquier tipo de enfrentamiento y buscando la mejor manera de responder al usuario educadamente, incluso ante opiniones vertidas contra la imagen corporativa.

En cualquier caso, deberá hacerse constar que la Cooperativa no se responsabilizará del contenido de los comentarios por parte de los ciudadanos en la red social.

Se deberá indicar en el perfil de la red social la política de eliminación de comentarios de los ciudadanos, la cual deberá tener en cuenta lo siguiente:

Comentarios que utilicen lenguaje claramente insultante, irreverente o despectivo.

Comentarios despectivos o discriminatorios por motivos de raza, edad, estado civil, discapacidad física o mental, orientación sexual, ideología política o religión o cualquier otra circunstancia personal o social.

Los comentarios de contenido sexual o que incluyen enlaces a contenido sexual.

Cualquier tipo de comentario de índole comercial o propagandística.

Comentarios que promuevan algún tipo de actividad ilegal.

Conversaciones privadas y personales entre particulares, así como mensajes que supongan ataques personales y sus respuestas.

Finalmente, la cooperativa se reserva el derecho de restringir o eliminar cualquier contenido que considere que viola esta política.

GRUPOS DE NAVEGACIÓN:

La Cooperativa del Magisterio CODEMA provee el servicio de internet para Directivos, trabadores y contratistas, con accesos limitados de acuerdo con el perfil del usuario y las funciones que desempeñan, estos accesos están controlados por el web filter del firewall que se tiene instalado y configurado en las oficinas y sedes vacacionales, estos grupos de navegación se encuentran distribuidos de la siguiente manera:

JEFES: Tienen acceso de navegación a todas la paginas de internet con restricción a páginas para adultos, contenido explicito y páginas maliciosas.

SEGURIDAD: Usuario de monitoreo con acceso de navegación a todas la paginas de internet con restricción a páginas para adultos, contenido explicito y páginas maliciosas.

SISTEMAS: Tienen acceso a internet incluyendo Hotmail y YouTube, con bloqueo de listas restrictivas.
USUARIOS ESPECIALES: Tienen acceso de navegación a las páginas de internet utilizadas para su labor diaria con restricción a: contenido para adultos, explicito y maliciosas.
CONTABILIDAD: Tienen acceso de navegación a las páginas de internet utilizadas para su labor diaria con restricción a: contenido para adultos, explicito y maliciosas.
USUARIOS: Tienen acceso a intranet, correo, consulta bancos con restricción a páginas para adultos, contenido explicito y páginas maliciosas.
CAJEROS: Tienen acceso a intranet, correo, con restricción a páginas para adultos, contenido explicito y páginas maliciosas.
LONGITUD MÍNIMA DE CONTRASEÑAS
ESTACIONES DE TRABAJO:
Las contraseñas deben cumplir con las siguientes características:
Tamaño de la contraseña: Debe ser de 8 caracteres, contener mínimo una mayúscula y un número.
Condiciones:
Incluir combinación de números, letras mayúsculas, minúsculas y caracteres especiales.
No deben ser nombres propios ni palabras de diccionarios, ni contraseñas cíclicas.
Los usuarios pueden realizar el cambio de la clave cuando lo deseen.
APLICATIVO CORE:
Las contraseñas deben cumplir con las siguientes características:
La clave debe ser encriptada.
La contraseña debe ser superior a 5 caracteres,
Debe contener caracteres especiales y al menos un número.
El sistema obliga a cambiarla cada tres meses informando a través de mensaje de alerta con anterioridad, su próximo vencimiento.
APLICATIVO DOCUNET
Las contraseñas deben cumplir con las siguientes características:
La clave debe ser encriptada.
La contraseña debe ser superior a 3 caracteres.
ACTIVIDADES DE CONTROL
Hace referencia a los mecanismos técnicos y analíticos que son establecidos por la Cooperativa, con el objeto de medir, dar seguimiento, minimizar riesgos y promover la mejora de los procesos. A continuación, se detallan los tipos de control:
Rectificar la información cuando sea incorrecta y comunicar lo pertinente.
La información sensible que se vaya a publicar en la página web y redes sociales de la Cooperativa deberá ser revisada por las áreas de control previo a su publicación, con el fin de prevenir publicidad engañosa y mitigar un posible riesgo reputacional o de contagio.
Se deberán identificar las aplicaciones que manejan información clasificada de la Cooperativa, con el fin de contemplar medidas de seguridad más fuertes antes de su tercerización.
Debe existir un monitoreo permanente con el fin de evaluar el cumplimiento de los acuerdos de niveles de servicio.
Se deberán establecer controles basados en estándares de configuración, para que las redes internas cumplan con las especificaciones de disponibilidad requeridas y así garantizar actividades de supervisión de la red.
La revisión de todos los equipos de la red deberá ser a través de la herramienta de software Zabbix, con el fin de mantener la disponibilidad y actualización del diagrama de red.
Se deberá efectuar labores de monitoreo sobre las transacciones realizadas en los sistemas de información, así como el uso de dispositivos en la red, para evidenciar actividades sospechosas o posibles fallas.
Todas las estaciones de trabajo deben tener activado el bloqueo automático luego de un período de ausencia o inactividad de 3 min.
Toda comunicación del correo electrónico interno podrá ser supervisada por el jefe inmediato, en caso de requerirse un seguimiento especial.

Se debe realizar auditorías a las terceras partes para evaluar la seguridad de la información y, como mínimo, se evaluarán integridad, disponibilidad, confidencialidad y calidad del servicio.

VULNERABILIDADES

Se prohíbe la explotación de vulnerabilidades de seguridad en cualquiera de los recursos de tecnología que tiene la Cooperativa.

El Oficial de Seguridad de la información podrá realizar las diferentes pruebas, con el propósito de identificar posibles vulnerabilidades en los activos de T.I.

En el caso de encontrar vulnerabilidades, se deberá reportar al Departamento de Sistemas encargado de administrar estos dispositivos para hacer la remediación inmediata. Así mismo se deberá presentar un reporte a Gerencia general.

La Cooperativa dispone de una herramienta de seguridad, la cual contiene una base actualizada de las vulnerabilidades con mayor impacto a nivel mundial que nos ayuda a identificar las posibles amenazas que se pueden llegar a presentar y así responder de forma inmediata con la remediación.

Por lo menos dos (2) veces al año, se deberá generar un informe consolidado de las vulnerabilidades encontradas. Los informes de los últimos dos (2) años deben contener sus planes de acción y sus remediaciones.

Realizar un análisis diferencial de vulnerabilidades, comparando el informe actual con respecto al inmediatamente anterior.

Las herramientas usadas en el análisis de vulnerabilidades deberán estar homologadas por el CVE (Common Vulnerabilitis and Exposures) y actualizadas a la fecha de su utilización.

Los informes generados deberán tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre (www.mitre.org).

POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES PARA EL CUMPLIMIENTO DE LA LEY ESTATUTARIA 1581 DE 2012

La Protección de Datos Personales es un derecho basado en el principio de habeas data en el cual se reconoce el derecho a la intimidad y el respeto al buen nombre de los ciudadanos.

En Colombia la Ley 1581 de 2012 rige la Protección de Datos Personales y obliga a su cumplimiento, pues tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información consagrado en el artículo 20 de la misma.

Con el fin de cumplir las disposiciones de la Ley, la COOPERATIVA DEL MAGISTERIO en adelante CODEMA o el responsable, ha establecido esta Política de Tratamiento de Datos Personales la cual está a disposición de los Titulares de datos personales a los que hace tratamiento.

DATOS DEL RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES

COOPERATIVA DEL MAGISTERIO CODEMA
NIT. 860.025.596-6
Calle 39 B #19-15 Bogotá D.C., Colombia
Teléfono Fijo: (601) 3237505
info@codema.com.co
https://www.codema.coop

La Cooperativa Del Magisterio CODEMA como responsable del Tratamiento de datos personales incluye en su calidad de responsable a su equipo humano.

OBJETIVO

Informar a los Titulares de datos personales bajo responsabilidad de CODEMA y a la ciudadanía en general nuestros lineamientos para el tratamiento de sus datos personales cumpliendo la normatividad vigente y siguiendo las buenas prácticas en materia de Protección de datos Personales.

Dar a conocer los derechos de los titulares de los datos, los deberes del responsable y de sus Encargados.

ALCANCE

Bajo esta política se hará tratamiento a todas las bases de datos físicas y automatizadas (electrónicas o digitales) usadas por CODEMA en su calidad de responsable o de encargado cuando sea pertinente. Nuestros colaboradores, contratistas, proveedores y cualquier tercero cuyo trabajo incluya tratamiento de datos personales, deberá conocer y cumplir esta Política.

MARCO LEGAL APLICABLE

Constitución Política de Colombia 1991 artículos 15 y 20.
Sentencias de la Corte Constitucional C-1011 de 2008 y C-748 del 2011.
Ley Estatutaria 1581 de 2012, conocida como Ley de Protección de Datos Personales.
Decreto Único Reglamentario del Sector Comercio 1074 de 2015 Capítulo 25 y Capítulo 26 los cuales compilan los decretos 1377 de 2013 y 886 de 2014 respectivamente.
Circular Externa 01 del 8 de noviembre de 2016 de la Superintendencia de industria y comercio
Decreto 090 del 18 de enero de 2018 del Ministerio de Comercio, Industria y Turismo
Normas subsiguientes que regulan la Protección de Datos Personales en Colombia, establecidas por los entes autorizados.

DEFINICIONES

Los conceptos aquí descritos permiten comprender esta Política. Estas definiciones han sido tomadas de la Ley 1581 de 2012, Artículo 3°, del Decreto 1074 Capítulo 25 Título 1 Artículo 2.2.2.25.1.3. y del Glosario ChanneiPianet® Data Privacy Risk®.

Ámbito de aplicación: Los principios y disposiciones contenidas en la ley 1581 de 2012 serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

La ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

Autorización: Consentimiento previo, expreso e informado que da una persona para que otra persona o una empresa pueda llevar a cabo el Tratamiento de sus datos personales. También se reciben Autorizaciones por conductas inequívocas que permitan concluir que el Titular autoriza el Tratamiento de sus datos personales.

El responsable deberá conservar copia de la Autorización emitida por el Titular. En el caso de los menores de edad, la Autorización debe ser otorgada por sus padres o sus representantes legales.

Aviso de privacidad. Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las Finalidades del Tratamiento que se pretende dar a los datos personales.

Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento. Puede ser física o automatizada.

Base de Datos Física: La que está creada en medios físicos, por ejemplo, el Archivo (en papel) de expedientes laborales.

Base de Datos Automatizada: La que está en medios electrónicos o digitales. Aquí los datos pueden estar estructurados o no estructurados.

Bases de Datos NO cubiertas por la Ley 1581 de 2012: La ley exceptúa del régimen de protección de datos personales (i) los archivos y las bases de datos pertenecientes al ámbito personal o doméstico; (ii) los que tienen por finalidad la seguridad y la defensa nacional, la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo, (ii) los que tengan como fin y contengan información de inteligencia y contrainteligencia, (iba) los de información periodística y otros contenidos editoriales, (v) los regulados por la Ley 1266 de 2008 (información financiera y crediticia,

comercial, de servicios y proveniente de terceros países) y (vi) los regulados por la Ley 79 de 1993 (sobre censos de población y vivienda).

Biometría: estudio para el reconocimiento inequívoco de las personas basado en sus características físicas y conductuales únicas. Ejemplo: voz, rostro, iris, huella digital, entre otras. En el ámbito de la Protección de Datos Personales, los datos biométricos son categorizados como datos sensibles.

Canales de atención al titular: Son los canales de comunicación que hemos dispuesto para recibir consultas y reclamos respecto de tratamiento de datos personales.

Ciclo de Vida del Dato: se refiere a la vida útil del dato en nuestras bases de datos. Se compone por estas fases: captura, clasificación, tratamiento, transferencia o transmisión (si aplica) y supresión o eliminación.

Confidencialidad: es una propiedad que otorga el carácter de reservado a una información. Es decir que esta información no podrá ser divulgada o revelada a personas no autorizadas para conocerla.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Los datos personales pueden ser privados, públicos, semiprivados o sensibles.

Dato privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el Titular.

Dato público. Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Dato semiprivado: Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

Datos sensibles. Aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Derechos de niños, niñas y adolescentes: Sólo podrán tratarse aquellos datos de menores que sean de naturaleza pública. El tratamiento de datos no públicos requiere autorización. En el Tratamiento de Datos Personales se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

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.

Al hablar de los Encargados hacemos referencia a terceros (contratistas o proveedores) que nos apoyan en diversos procesos para los cuales requieren que les suministremos datos personales de nuestros Titulares. Ejemplo: entrenadores deportivos, firmas que apoyan el recaudo de cartera, entre otros.

Estos Encargados deben comprometerse a respetar nuestra Política y deben cumplir por su parte la Ley 1581 de 2012.

Finalidad del Tratamiento: Es la razón para la cual se usarán los datos personales. Debe ser legítima y los datos recaudados deben ser coherentes con la Finalidad.

Habeas Data: Principio constitucional (artículo 15 de la Constitución) que otorga el derecho a los ciudadanos a su intimidad personal y familiar y a su buen nombre. Indicando que el Estado debe respetarlos y hacerlos respetar.

De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

Oficial de Protección de Datos Personales 1 Analista de Protección de Datos Personales: Persona que cuenta con los conocimientos, preparación académica y experiencia para liderar el cumplimiento de la Ley

de Protección de Datos Personales en la empresa. Esta persona debe contar con el respaldo de la alta dirección y de toda la organización para el cumplimiento de su labor.
La Ley 1581 de 2012 indica que toda empresa debe contar con una persona o área a cargo de responder las consultas y reclamos a los titulares de datos personales. E**l** principio de Responsabilidad Demostrada o recolección, tratamiento se refiere a esta persona como Oficial de Protección de Datos Personales.
La Ley no establece que el Oficial de Protección de Datos Personales deba ser un empleado de la empresa, por lo cual puede ser un servicio en outsourcing.
Reclamo: manifestación por parte de un Titular de datos personales o de sus representantes legales de una inconformidad con el tratamiento dado a sus datos personales. En el reclamo el Titular solicita corregir, actualizar o suprimir sus datos, o revocar su autorización cuando la Ley así lo permite.
El proceso para que el Titular pueda ejercer sus derechos ante nuestra entidad es explicado en esta Política.
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.
RNBD: Es la sigla de **Registro Nacional de Bases de Datos.** Es el Directorio público de las bases de datos con información personal sujetas a Tratamiento que operan en Colombia.
En este registro NO se almacenan las bases de datos, sino que se informan las características de las bases de datos con datos personales que manejan los responsables de las misma.
Se debe registrar en el RNBD el tipo de datos que contienen las bases de datos, las Finalidades del Tratamiento, los canales que se han dispuesto para atender las consultas y reclamos de los ciudadanos, las políticas de tratamiento, las condiciones de seguridad, las transferencias y transmisiones de información que se realizan, entre otros aspectos.
Según la Superintendencia de Industria y Comercio, la utilidad principal del RNBD es crear consciencia sobre el manejo adecuado de la información personal contenida en bases de datos, y es la principal herramienta de supervisión que tiene la Superintendencia para ejercer la vigilancia y garantizar que en el manejo y administración de los datos personales se respeten los derechos de los ciudadanos.
Superintendencia de Industria y Comercio -SIC-: Entidad pública colombiana que vigila y controla el cumplimiento de la Ley 1581 de 2012.
Titular: Persona natural cuyos datos personales sean objeto de Tratamiento. Los titulares menores de 18 años deben ser representados por sus padres o representantes legales.
Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
El Tratamiento se interpretará entonces como cualquier acción que se ejerza sobre los datos personales, por ejemplo: recolectar los datos, procesarlos, actualizarlos, administrarlos, publicarlos, almacenarlos, compartirlos, eliminarlos, o cualquier otro uso, que en nuestro caso se hará bajo los lineamientos de la por ejemplo Ley 1581 de 2012.
Transferencia. La transferencia de datos tiene lugar cuando el responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.
Transmisión. Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la reali**z**ación de un Tratamiento por el Encargado por cuenta del responsable.

PRINCIPIOS RECTORES PARA EL TRATAMIENTO DE DATOS PERSONALES
Tal como lo indica Ley 1581 de 2012 en su Título 11 artículo 4º, los principios que seguimos en el tratamiento de los datos personales de manera armónica e integral, son:

Fuente de la imagen: Guías de la Superintendencia de Industria y Comercio

Principio de legalidad en materia de Tratamiento de datos: El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.
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.
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.
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.
Principio de transparencia: En el Tratamiento debe garantizarse el derecho del Titular a obtener del responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley.
Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley.
Principio de seguridad: La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su responsable o acceso no autorizado o fraudulento.
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 presente ley y en los términos de la misma.

CATEGORÍAS ESPECIALES DE DATOS:

TRATAMIENTO DE DATOS SENSIBLES

La Ley 1581 de 2012 (Título 11 artículo 5) denomina datos sensibles a aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Se prohíbe el Tratamiento de datos sensibles (Ley 1581 de 2012 Título 111 artículo 6), excepto cuando:

El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;

El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;

El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una 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;

El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;

El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

Casos en los que CODEMA hará Tratamiento a datos SENSIBLES:

En el ámbito laboral en actividades de teletrabajo, trabajo en casa, reuniones virtuales, videoconferencias, asambleas virtuales. En procesos de Seguridad y Salud en el Trabajo -SST-, atención en salud, video vigilancia, control de acceso. Cuando haga recaudo de información de salud exigida por las autoridades, entre otras actividades donde se capten datos biométricos y otros catalogados como sensibles.

Control de temperatura, exámenes médicos y otras medidas impuestas por el gobierno nacional y autoridades locales para control de enfermedades que puedan afectar la salud pública, por ejemplo, para la prevención y control del COVID-19.

Sólo se manejarán datos sensibles cuando sean indispensables para el cumplimiento legal de contratos laborales, comerciales y demás, o cuando sean requeridos para cumplir la misión empresarial. En cualquier caso, se hará el Tratamiento con total respeto por la normatividad vigente de Protección de Datos Personales.

DERECHOS DE LOS NIÑOS, NIÑAS Y ADOLESCENTES

En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes. Queda proscrito (prohibido) el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública o cuando el Tratamiento cumpla con estos requisitos:

Que responda y respete el interés superior de los niños, niñas y adolescentes.

Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

Todo Responsable o Encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos según los principios y obligaciones establecidos en la Ley 1581 de 2012.

DERECHOS DE LOS TITULARES

El Titular de los datos personales tendrá los siguientes derechos (Ley 1581 de 2012 TÍTULO IV Artículo 8):

Conocer, actualizar y rectificar sus datos personales frente a los responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos,

fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado;
Solicitar prueba de la autorización otorgada al responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 1O de la presente ley;
Ser informado por el responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que les ha dado a sus datos personales;
Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen;
Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución;
Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

AUTORIZACIÓN del Titular. (Ley 1581 de 2012 TÍTULO IV Artículos 9 y 10) Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.

CASOS EN QUE NO ES NECESARIA LA AUTORIZACIÓN

La autorización del Titular no será necesaria cuando se trate de:
Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;
Datos de naturaleza pública;
Casos de urgencia médica o sanitaria;
Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;
Datos relacionados con el Registro Civil de las Personas.
Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la Ley 1581 de 2012.
Los datos personales que se encuentren en fuentes de acceso público, con independencia del medio por el cual se tenga acceso, entendiéndose por tales aquellos datos o bases de datos que se encuentren a disposición del público, pueden ser tratados por cualquier persona siempre y cuando, por su naturaleza, sean datos públicos. (Decreto 1074 de 2015 Capítulo 25 Artículo 2.2.2.25.2.2)
CODEMA captará la autorización en medios físicos, digitales o electrónicos. Por ejemplo, a través de una firma física, aceptación en formato electrónico, verbal, en video, por medio de una señal biométrica como la huella digital o la voz, entre otros.
La autorización también se puede dar por una conducta inequívoca del Titular de los datos, excepto en la captación de datos sensibles o de menores de edad.

TRATAMIENTO DE LA INFORMACIÓN

Todos los miembros de la Cooperativa, al realizar las actividades propias de su cargo, asumirán las responsabilidades y las obligaciones que se tienen en el manejo adecuado de la información personal, desde su recolección, almacenamiento, uso, circulación y hasta su disposición final.
Los directivos y trabajadores no podrán tomar decisiones que tengan un impacto significativo en la información personal, o que tengan implicaciones legales, con base exclusivamente en la información que arroja el sistema de información, por lo que deberán validar la información a través de otros instrumentos físicos o de manera manual, y, si es necesario, de manera directa por parte del titular del dato, en los casos en que así sea necesario.
Únicamente los directivos, trabajadores y contratistas autorizados pueden introducir, modificar o anular los datos contenidos en las bases de datos o documentos objeto de protección. Los permisos de acceso de los usuarios son concedidos por el Gerente Administrativo, contando previamente con el concepto de viabilidad del Oficial de Seguridad de la Información, los cuales serán previamente definidos por los líderes de los procesos donde se requiera el uso de información personal.

Cualquier uso de la información diferente al establecido, será previamente consultado con el Oficial de Protección de Datos Personales y el Oficial de Seguridad de la Información.

FINALIDADES

¿Para qué usamos los datos personales de los Titulares? El uso dependerá del tipo de Titular de datos y su relación con CODEMA.

El tratamiento de datos se realizará exclusivamente para las finalidades autorizadas y previstas en la presente Política y en las autorizaciones específicas otorgadas por parte del titular. De la misma forma se realizará Tratamiento de Datos Personales cuando exista una obligación legal o contractual para ello, siempre bajo los lineamientos de las políticas de Seguridad de la Información.

En todos los casos los datos personales podrán ser tratados con la finalidad de adelantar los procesos de control y auditorías internas y externas y evaluaciones que realicen los organismos de control. Así mismo, los datos personales serán tratados de acuerdo con el grupo de interés y en proporción a la finalidad o finalidades que tenga cada tratamiento, como se describe a continuación:

TITULARES EMPLEADOS Y COLABORADORES

El Tratamiento de estos datos tiene como finalidad cumplir a cabalidad con el contrato laboral lo cual implica verificación de identidad, actualización de datos de contacto y ubicación, control de acceso y control de acceso biométrico (si aplica), seguridad, registro en plataformas tecnológicas, comunicación, encuestas, seguimiento a funciones, actividades y responsabilidades laborales, así como el análisis del desempeño laboral.

Además, se cubren las actividades necesarias para el cumplimiento de la normatividad vigente de Seguridad y Salud en el Trabajo (SST), exámenes médicos de ingreso, exámenes periódicos y exámenes médicos de egreso; atención y prevención en salud. Servicios de alimentación y transporte (si aplica), actividades de bienestar, actividades lúdicas o deportivas, programación de viajes, auxilios, seguros, análisis del desempeño. Pagos de nómina, cumplimiento de requisitos relacionados con el Sistema General de Seguridad Social y demás obligaciones que surjan del contrato laboral.

También usaremos los datos para la coordinación y cubrimiento audiovisual cuando haya participación del talento humano en representación de CODEMA en actividades locales o internacionales. Para comunicación, publicaciones y producciones audiovisuales. Para desarrollar reportes exigidos por entidades públicas o por cumplimiento normativo.

Usaremos los datos de los hijos de nuestros EMPLEADOS para hacer las afiliaciones que exige la ley a servicios de salud, caja de compensación familiar, entre otros. También podremos usar estos datos y los de hijos de colaboradores para extender invitaciones a actividades de entretenimiento, lúdicas, artísticas, deportivas, entre otras que desarrollemos en pro del bienestar de nuestro equipo humano y sus familias. Estas actividades pueden tener cubrimiento audiovisual para el registro y divulgación de las mismas.

En caso de datos biométricos capturados a través de sistemas de videovigilancia o grabación su tratamiento tendrá como finalidad la identificación, seguridad y la prevención de fraude interno y externo.

TITULARES CANDIDATOS

Las FINALIDADES del tratamiento de datos de CANDIDATOS a empleos en CODEMA serán las necesarias para el proceso de selección, como evaluación de la hoja de vida, verificación de referencias, exámenes de conocimientos y aptitud, exámenes médicos de ingreso, verificación de soportes académicos y los demás requeridos según el cargo.

Si la persona no es seleccionada para la vacante actual, pero se evidencia potencial, el responsable decidirá la conservación de los documentos y resultados para una posible vinculación posterior.

TITULARES EX EMPLEADOS

Las FINALIDADES del tratamiento de datos de Ex Empleados serán las requeridas para garantizar el suministro de información que la normatividad laboral exija para atender certificaciones laborales, reclamos laborales o derecho a la pensión. También conservaremos datos con fines históricos, por buenas prácticas empresariales o por otras normas legales.

TITULARES ASOCIADOS

Las FINALIDADES del tratamiento de datos de ASOCIADOS son las relacionadas con el conocimiento del asociado en diversos aspectos con el fin de prestarle los diversos servicios suministrados por CODEMA: ahorro, crédito, turismo, auxilios, capacitación, deporte, entre otros.
Por lo tanto, usaremos sus datos para procesos y actividades como: Verificación de identidad, gestión comercial y de mercadeo, comunicaciones, investigación de mercados, informes a entidades de supervisión y control, verificación de referencias, análisis estadísticos, control de acceso, control biométrico, seguridad, video vigilancia, asignación de turnos, análisis de crédito, facturación, cobro, servicio al cliente, encuestas, actualización de datos y cumplimiento tributario.
También se usarán los datos para: invitaciones y participación en entrenamientos y competencias deportivas, evaluación de desempeño deportivo, suministro de uniformes; Coordinación de servicios turísticos; Capacitación y evaluación en los diversos programas ofrecidos por el Instituto de CODEMA; Soportes para análisis de entrega de auxilios por diversos conceptos, entre otros propósitos inherentes a la misión de CODEMA y a los servicios tomados por sus beneficiarios.

TITULARES BENEFICIARIOS

La Finalidad del tratamiento de los datos de beneficiarios es la entrega de beneficios a través de los servicios prestados por CODEMA tal como lo ilustramos en el ítem de Titulares Afiliados.

TITULARES TERCEROS (CONTRATISTAS Y PROVEEDORES)

Las FINALIDADES de CONTRATISTAS y PROVEEDORES son netamente de verificación de identidad, procesos de selección de ofertas, comunicaciones, investigación de mercados, verificación de referencias, análisis estadísticos, control de acceso, control biométrico, seguridad, video vigilancia, actualización de datos, desarrollo de contratos, pagos, cumplimiento tributario, procesos de pedidos, despachos y garantías, entre otras inherentes a la relación comercial y contratos entre las partes. Expedir las certificaciones contractuales solicitadas por los contratistas de la Entidad o solicitudes de los entes de control.

OTROS TITULARES

Las finalidades con los demás grupos de Titulares serán las propias de la naturaleza de la relación y se recaudarán los datos mínimos necesarios para el cumplimiento de las obligaciones entre las partes y para satisfacer los objetivos de comunicación entre las mismas.

TEMPORALIDAD: DURACIÓN DEL TRATAMIENTO DE DATOS.

Los datos personales de los Titulares se conservarán por el tiempo necesario según las finalidades del tratamiento, o por el tiempo exigido por la normatividad vigente en materia laboral, solidaria y comercial, por obligación contractual, por exigencia contable, fiscal, por procesos jurídicos, históricos, por normas de calidad, por normas de gestión documental, por buenas prácticas empresariales y demás normas exigidas por la Ley o prácticas indicadas en la Autorización.

TRANSMISIÓN Y TRANSFERENCIA DE DATOS PERSONALES.

CODEMA podrá transferir o transmitir datos personales a terceros (proveedores o contratistas) que le provean servicios necesarios para el cumplimiento de su misión, se adoptarán las medidas necesarias para que las personas que tengan acceso a sus datos personales cumplan con la presente Política y con los principios de protección de datos personales y obligaciones establecidas en la Ley 1581 de 2012.
Según la Ley 1581 de 2012, TÍTULO VIII Artículo 26, se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que esta ley exige a sus destinatarios. Esta prohibición no regirá cuando se trate de:
Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia;
Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública;
Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable;
Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad;

Transferencias necesarias para la ejecución de un contrato entre el Titular y el responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular, además, deberán incluirse las siguientes obligaciones en cabeza del respectivo encargado:
Dar Tratamiento, a nombre del responsable, a los datos personales conforme a los principios que los tutelan.
Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales.
Guardar confidencialidad respecto del tratamiento de los datos personales.
Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
Parágrafo 1°. En los casos no contemplados como excepción en el presente artículo, corresponderá a la Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el Superintendente queda facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.
Parágrafo 2°. Estas disposiciones serán aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266 de 2008 referente a Habeas Data financiero.

CANALES DE ATENCIÓN DE CONSULTAS Y RECLAMOS
COOPERATIVA DEL MAGISTERIO, CODEMA
Calle 39 B #19-15 Bogotá D.C., Colombia
Teléfono Fijo: (601) 3237505
pqrs@codema.com.co
Las consultas y reclamos se atenderán de lunes a viernes de 8:00a.m. a 12:00 m. y de 2:00 p.m. a 5:00 p.m.
Las redes sociales no son un canal dispuesto por nuestra organización para radicar consultas y reclamos.

PROCEDIMIENTO PARA ATENDER LOS DERECHOS DE LOS TITULARES
El Titular puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir información y/o revocar la autorización otorgada, a través de consultas o reclamos. Las consultas o reclamos que el Titular nos presente deberán contener como mínimo la siguiente información:
Nombres y apellidos del Titular y/o su representante legal y/o su causahabiente.
Su consulta o reclamos de forma clara y completa.
Soportes de su consulta o reclamo.
Datos de identificación y contacto: Nombre completo, número de documento de identidad, correo electrónico, dirección física y número telefónico tanto del Titular como de sus causahabientes o representantes legales si son estos los que lo representan. Si es un reclamo por favor adjunte copia de su documento de identidad.
Relación del Titular con nosotros (responsable). Ejemplo. Ex empleado, cliente, etc. d. Firma del documento de reclamo.
Las consultas y reclamos se atenderán a través de los canales oficiales (ver ítem 14).

PLAZOS DE RESPUESTA A CONSULTAS Y RECLAMOS:
CONSULTAS
Las consultas serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recepción.
Si por las exigencias de la consulta u otra razón nos es imposible atender la consulta dentro de los 10 días hábiles, antes de este plazo, informaremos al interesado los motivos que nos impiden responder y solicitaremos un plazo máximo de cinco (5) días hábiles siguientes al vencimiento para responder.
Es importante que la consulta esté clara y completa, para evitar demoras por aclaraciones. Si el área de Protección de Datos Personales no es la competente para responder la consulta, le remitirá la consulta al área correspondiente y le informará al interesado.
Es importante recordar que las consultas se recibirán a través de nuestros canales oficiales (ver ítem 14). Las redes sociales no son un canal oficial para radicar consultas.

RECLAMOS

El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo.

Es fundamental que el reclamo esté claro, completo y que se adjunten los documentos que lo soportan, además de la copia del documento de identidad del Titular o de su representante legal.

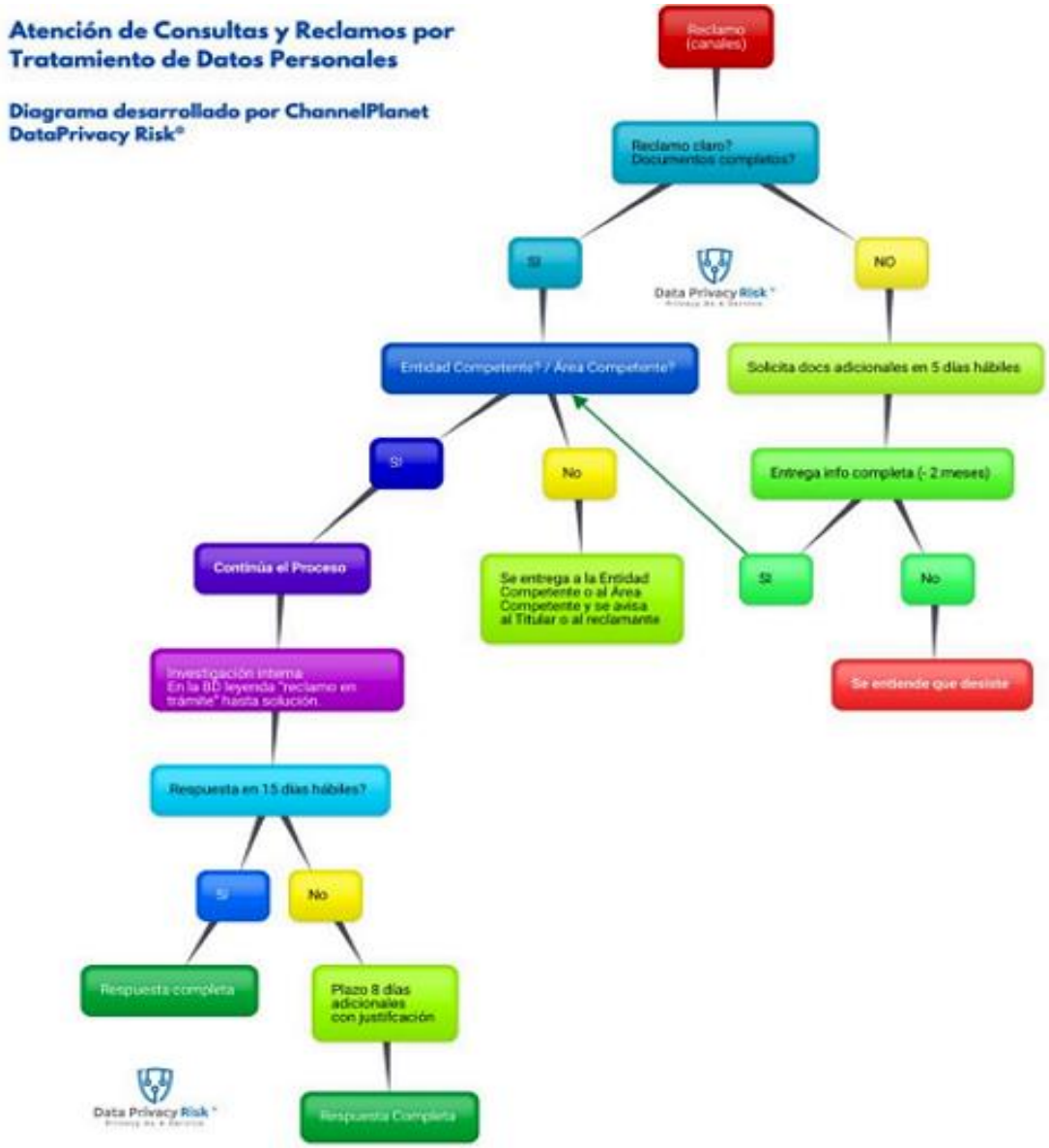
Si el área de Protección de Datos Personales no es la competente para responder el reclamo, le remitirá la solicitud al área correspondiente y le informará al reclamante.

Si al revisar el reclamo, los documentos no están completos, durante los 5 días siguientes a su recepción, se le solicitará al Titular adjuntar los documentos faltantes. En caso de que pasen dos meses y el Titular no responda este requerimiento se entenderá que desistió de su reclamo.

En el término de dos (2) días hábiles contados desde la recepción del reclamo colocaremos en la base de datos donde se encuentren los datos personales del Titular, la leyenda "reclamo en trámite" y el motivo del mismo. Mantendremos esta leyenda hasta que el reclamo sea respondido y el proceso haya concluido.

Cuando no nos sea posible responder a cabalidad el reclamo dentro del plazo informaremos al interesado los motivos de la demora y la fecha en que atenderemos su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Es importante recordar que los reclamos se recibirán a través de nuestros canales oficiales (ver ítem 14). Las redes sociales no son un canal oficial para radicar reclamos. Para una fácil comprensión del proceso compartimos el siguiente diagrama:



REQUISITO DE PROCEDIBILIDAD.

Según el Artículo 16 de la Ley 1581 de 2012 elTitular o causahabiente sólo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante el responsable del Tratamiento o Encargado del Tratamiento.

REGISTRO NACIONAL DE BASE DE DATOS

Dando cumplimiento al artículo 25 de la Ley 1581 de 2012 y al Capítulo 26 del Decreto Único Reglamentario del sector Comercio, Industria y Turismo 1074 de 2015, registramos las Bases de Datos Personales sobre las que somos responsables del Tratamiento y la Política de Tratamiento de Datos Personales vigente, en el Registro Nacional de Bases de Datos -RNBD-.

La definición del **RNBD** se incluyó en la sección Definiciones de esta Política (ítem 5).

AVISO DE PRIVACIDAD

La Cooperativa establece como aviso de privacidad el siguiente párrafo, el cual debe estar configurado en todas las licencias de correo electrónico al final de cada mensaje enviado:

En cumplimiento del Régimen General de Habeas Data, regulado por la Ley 1581 de 2012 y sus Decretos reglamentarios, la Cooperativa del Magisterio CODEMA informa lo siguiente: El presente correo electrónico puede contener información confidencial o legalmente protegida y está destinado única y exclusivamente

para el uso del destinatario(s) previsto para su utilización específica. Si la información adjunta en este correo electrónico, no está relacionada con el objeto social de la Cooperativa, se entenderá como personal y de ninguna manera son autorizados. Si usted no es el destinatario a quien se desea enviar este mensaje y lo recibió por error, favor notificar al remitente de inmediato y desecharlo de su sistema. Se le informa que está prohibida su divulgación, revisión, transmisión, difusión o cualquier otro tipo de uso de la información aquí contenida. Para conocer más de nuestra Política de Tratamiento de Datos Personales diríjase a la página web www.codema.com.co.

CONTROL DE ACCESO Y VIDEO VIGILANCIA

CONTROL ACCESO

Las áreas donde se ejecutan procesos relacionados con información confidencial o restringida deben contar con controles de acceso que sólo permitan el ingreso a los colaboradores autorizados y que permita guardar la trazabilidad de los ingresos y salidas.

VIDEO VIGILANCIA

La Entidad cuenta con cámaras de video vigilancia que tienen como finalidad dar cumplimiento a las políticas de seguridad física, cumpliendo con los parámetros establecidos en la Guía para la Protección de Datos Personales en Sistemas de Videovigilancia, expedidos por la SIC como autoridad de control.

Las imágenes deberán ser conservadas por un tiempo máximo de 90 días. En caso que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

PROCESOS DE REVISIÓN Y AUDITORÍAS DE CONTROL

La Cooperativa realizará procesos de revisión o auditorías en materia de protección de datos personales verificando de manera directa o a través de terceros, que las políticas y procedimientos se han implementado adecuadamente en la Entidad.

Con base a los resultados obtenidos, se diseñarán e implementarán los planes de mejoramiento (preventivos, correctivos y de mejora) necesarios.

Estos procesos de revisión deberán realizarse con una periodicidad mínima de un año o de forma extraordinaria ante incidentes graves que afecten a la integridad de las bases de datos personales.

Los resultados de la revisión junto con los eventuales planes de mejoramiento serán presentados por el Oficial de Protección de Datos Personales al Comité de Seguridad de la información para su valoración y posterior presentación ante el Consejo de Administración para la respectiva aprobación.

VIGENCIA DE LA POLÍTICA

Esta Política ha sido desarrollada con el apoyo de ChanneiPianet SAS y sus servicios DataPrivacyRisk®. Está vigente desde marzo de 2021 y reemplaza cualquier versión anterior existente.

Cuando haya cambios sustanciales informaremos a nuestros Titulares**,** sin embargo, la Política vigente estará disponible en nuestra página web. También puede solicitarla a través de nuestros canales de atención.

ACUERDO DE CONFIDENCIALIDAD

Entre los suscritos a saber **MANUEL GERMAN MARTÍNEZ MARTÍNEZ**, identificado con cedula de ciudadanía N° 5.836.333 expedida en Ambalema (Tolima), actuando en calidad de Representante Legal de la Cooperativa del Magisterio CODEMA con Nit-860.025.596-6, quien en adelante se denominara **LA PARTE REVELADORA** y _____, mayor de edad, identificado(a) con la cédula de ciudadanía N.º _____de _____, quien para efectos del presente instrumento se denominará **LA PARTE RECEPTORA**, hemos convenido celebrar el presente acuerdo de confidencialidad, teniendo en cuenta las siguientes:

CONSIDERACIONES

Que son parte integral del presente acuerdo las siguientes definiciones:

- **Información Confidencial:** Significa cualquier información escrita, oral, visual, por medios electrónicos o digitales de propiedad de **LA PARTE REVELADORA** o sobre la cual posea algún tipo de derecho. Se entenderá incluida en la Información Confidencial cualquier copia de esta, pero no se limita a todo tipo de

información, notas, datos, análisis, conceptos, hojas de trabajo, compilaciones, comparaciones, estudios, resúmenes, registros preparados para o en beneficio de **LA PARTE RECEPTORA** que contengan o de alguna forma reflejen dicha información.

- **Parte Reveladora:** Se constituye en parte reveladora a **LA COOPERATIVA** o sus Representantes, Directivos y trabajadores que suministre información por cualquiera de los mecanismos previstos en este Acuerdo.
- **Parte Receptora:** Se constituye en parte receptora los directivos, trabajadores y terceros con quien la Cooperativa tenga vinculo comercial y/o laboral y que reciban cualquier información.

Para efectos de la interpretación del presente acuerdo se tendrán en cuenta las siguientes:

CLÁUSULAS

PRIMERA. – OBJETO: El objeto del presente acuerdo es fijar los términos y condiciones bajo los cuales la parte receptora mantendrá la confidencialidad de los datos e información suministrada por la parte reveladora.

SEGUNDA. – CONFIDENCIALIDAD: Las partes acuerdan que cualquier información suministrada, facilitada o creada por cualquier PARTE, en el transcurso del contrato, será mantenida en estricta confidencialidad, en virtud de lo anterior la parte receptora se obliga a no revelar, divulgar, exhibir, mostrar y/o comunicar la información que reciba de la parte reveladora, ni a utilizarla en su favor o en el de terceros, y en consecuencia a mantenerla de manera confidencial y privada y a proteger dicha información para evitar su divulgación no autorizada.

Se considera también información confidencial:

I. Aquella que como conjunto o por la configuración o estructuración exacta de sus componentes, no sea generalmente conocida entre los expertos en los campos correspondientes.

II. La que no sea de fácil acceso, y

III. Aquella información que sea sujeta a medidas de protección razonables, de acuerdo con las circunstancias del caso, a fin de mantener su carácter confidencial.

En virtud del Acuerdo, **LA PARTE RECEPTORA** se obliga a no revelar, divulgar, exhibir, mostrar, copiar, reproducir y/o comunicar la Información Confidencial que reciba de **LA PARTE REVELADORA**, ni a utilizarla en favor de terceros y a proteger dicha información para evitar su divulgación no autorizada.

LA PARTE RECEPTORA no podrá revelar públicamente ningún aspecto de la Información Confidencial sin el consentimiento previo y por escrito del Representante Legal de la Cooperativa.

TERCERA. – MODIFICACIÓN O TERMINACIÓN: Este acuerdo solo podrá ser modificado o darse por terminado con el consentimiento previo, expreso por escrito y firmado de las partes involucradas.

CUARTA. – USO DE LA INFORMACION CONFIDENCIAL: La información confidencial sólo podrá ser utilizada para los fines señalados en el presente acuerdo. **LA PARTE RECEPTORA** no podrá hacer uso de la Información Confidencial en detrimento de **LA PARTE REVELADORA**. Se podrá revelar o divulgar la Información Confidencial únicamente en los siguientes eventos:

I. Que se revele con la aprobación previa y escrita del Representante Legal de la Cooperativa.

II. Que la revelación y/o divulgación de la información confidencial se realice en desarrollo o por mandato de una ley, decreto, acto administrativo, sentencia u orden de autoridad competente en ejercicio de sus funciones legales. En este caso, **LA PARTE RECEPTORA** se obliga a avisar inmediatamente haya tenido conocimiento de esta obligación de revelación y/o divulgación a **LA PARTE REVELADORA**, para que pueda tomar las medidas necesarias para proteger la información confidencial, y de igual manera se compromete a tomar las medidas para atenuar los efectos de tal divulgación y se limitará a divulgar únicamente la información efectivamente requerida por la autoridad competente.

III. Que la información confidencial esté o llegue a estar a disposición del público o sea de dominio público por causa diferente a un acto u omisión de **LA PARTE RECEPTORA**;

IV. Que la información confidencial haya estado en posesión de **LA PARTE RECEPTORA** antes de que hubiese recibido la misma por medio de **LA PARTE REVELADORA** o que no hubiese sido adquirida por **LA PARTE REVELADORA**, o de cualquier tercero que tuviere un compromiso de confidencialidad con respecto a **LA PARTE REVELADORA**.

QUINTA. – FINALIDADES DE LA INFORMACIÓN: LA PARTE RECEPTORA solo podrá hacer uso de la información suministrada por **LA PARTE REVELADORA** para la ejecución de actividades propias de su cargo, las señaladas en el contrato y/o funciones previamente aprobadas por el Consejo de Administración.

SEXTA. – CALIDAD DE LA INFORMACIÓN: LA PARTE REVELADORA no garantiza, ni expresa ni implícitamente, que la Información Confidencial sea exacta o perfecta.

LA PARTE REVELADORA queda liberada de cualquier responsabilidad que se derive de errores u omisiones contenidos en la información confidencial.

SÉPTIMA. – PROPIEDAD Y DEVOLUCIÓN DE LA INFORMACIÓN: La información entregada por **LA PARTE REVELADORA** es propiedad exclusiva de ésta y deberá ser tratada como confidencial y resguardada bajo este entendido por **LA PARTE RECEPTORA**, durante el término que se fija en el presente Acuerdo.

LA PARTE REVELADORA podrá solicitar a **LA PARTE RECEPTORA** la devolución o destrucción de la información confidencial que haya recibido, incluidas, pero no limitadas a todas las copias, extractos y otras reproducciones de la información confidencial, los cuales deberán ser devueltos o destruidos dentro de los treinta (30) días siguientes a la terminación del acuerdo. La destrucción de la información confidencial debe ser certificada por **LA PARTE RECEPTORA** a **LA PARTE REVELADORA**.

En todo caso, el hecho de no recibir una comunicación en el sentido a que alude el párrafo anterior, no libera a la parte receptora de su deber de custodia, en los términos señalados en el presente acuerdo.

OCTAVA. – RESOLUCIÓN DE DIFERENCIAS: Las diferencias surgidas en relación con la celebración, interpretación, ejecución y/o terminación de este acuerdo de confidencialidad y divulgación de la información confidencial, se solucionarán entre las partes en primera instancia a través de arreglo directo. Ocurrido un hecho que origina una controversia cualquiera de las partes podrá tomar la iniciativa de enviar a la otra parte, a más tardar dentro de los tres (3) días siguientes, un aviso de inicio de la etapa de arreglo directo o contado a partir del día en que se dio origen al hecho que causo la controversia si no hubo tal aviso, no se ha podido solucionar la controversia, cualquiera de las partes será libre de acudir a la jurisdicción ordinaria. Las controversias a las que se refiere esta cláusula no podrán versar sobre obligaciones de pago pendientes, en cuyo caso, la parte acreedora podrá acudir directamente a la jurisdicción ordinaria, sin necesidad de agotar la etapa de arreglo directo.

Está cláusula está entendida sin perjuicio que las partes pacten un compromiso de conformidad con lo estipulado en la Ley 1563 de 2012, para llevar la resolución de las diferencias específicas a un tribunal de arbitramento que será designado de acuerdo con los términos que se establezcan en el respectivo acuerdo.

El incumplimiento de alguna de las prohibiciones, divulgación, copia, distribución de información considerada confidencial, acarreará una sanción que se establece en _____SMMLV, sin perjuicio de las demás acciones para lograr satisfacer el monto de la pérdida, perjuicio o afectación patrimonial sufrida. El consejo de administración de la Cooperativa deberá fijarlo mediante acta.

NOVENA. – PROHIBICIÓN DE CESIÓN: Este acuerdo de confidencialidad debe beneficiar y comprometer a las partes y no puede ser cedido, vendido, asignado, ni transferido, bajo ninguna forma y a ningún título, sin contar con la autorización previa y escrita de la otra Parte.

DECIMA. – DISPOSICIONES VARIAS:

- **I.** Este documento representa el acuerdo completo entre las partes y sustituye cualquier otro verbal o escrito celebrado anteriormente entre ellas, sobre la materia objeto del mismo.
- **II.** Si alguna de las disposiciones de este acuerdo llegare a ser ilegal, inválida o sin vigor bajo las leyes presentes o futuras o por un Tribunal, se entenderá excluida. Este acuerdo será realizado y ejecutado, como si dicha disposición ilegal, inválida o sin vigor, no hubiera hecho parte del mismo y las restantes disposiciones aquí contenidas conservarán idéntico valor y efecto.

DÉCIMA PRIMERA. – LEY APLICABLE: El presente Acuerdo se regirá e interpretará de conformidad con las leyes de Colombia y quedarán excluidas las reglas de conflictos de leyes que pudiesen remitir el caso a las leyes de otra jurisdicción.

DÉCIMA SEGUNDA. – PERFECCIONAMIENTO Y VIGENCIA: El presente acuerdo se perfecciona con su firma y estará vigente desde la fecha de su suscripción y durará mientras se encuentren vigentes las relaciones entre las partes involucradas y en todo caso seguirá vigente hasta luego de terminadas estas relaciones por un término adicional de cinco (5) años.

En constancia se suscribe el presente Acuerdo, en Bogotá D.C., a los _____
PARTE RECEPTORA:

FIRMA: _____
NOMBRE: _____
C.C. No: _____

PARTE REVELADORA:

MANUEL GERMAN MARTÍNEZ MARTÍNEZ
REPRESENTANTE LEGAL
Cooperativa del Magisterio CODEMA

POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

MARCO LEGAL

La Cooperativa del Magisterio CODEMA ha proyectado su Plan Estratégico con base en su objeto social y en la normatividad vigente descrita en circulares y anexos establecidos por la Supersolidaria y demás entes de control. En materia de seguridad de la información, ha definido sus políticas aplicando la normatividad que se enuncia a continuación:

LEY 527 DE 1999:

Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

LEY ESTATUTARIA 1266 DE 2008 Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

LEY ESTATUTARIA 1581 DE 2012 tiene por objeto garantizar la protección del derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política.

DECRETO 1377 DE 2013 tiene por objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27001:2013. Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un Sistema de Gestión de la Seguridad de la Información (SGSI).

OBJETIVO:

La Política de Seguridad de la Información tiene por objetivo la protección de los activos de información de la Cooperativa del Magisterio CODEMA frente a las amenazas internas o externas que se puedan presentar, preservando los principios de disponibilidad, confidencialidad, e integridad.

ALCANCE

Esta política abarca todas las áreas que hacen parte de la Cooperativa del Magisterio CODEMA, los procesos internos y externos que hacen parte de la funcionalidad de la misma y quienes la integran: directivos, empleados, asociados, aprendices y contratistas. Comprende el adecuado uso de los activos de información como base de datos, soportes físicos y electrónicos.

NIVEL DE CUMPLIMIENTO

La Cooperativa del Magisterio CODEMA, define e implementa el Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
Corresponde velar por su estricto cumplimiento a la Gerencia General de la Cooperativa del Magisterio CODEMA y al Oficial de Seguridad de la Información.

TÉRMINOS Y DEFINICIONES

Los términos en este documento serán utilizados de acuerdo a las siguientes definiciones:

Activos de información: Son activos de la información toda clase de dispositivos tecnológicos, programas, archivos, bases de datos, documentación física y sistemas de información.

Acuerdo de Confidencialidad: Convenio o cláusula de confidencialidad, donde los directivos, trabajadores y terceras partes, manifiestan su voluntad de mantener la confidencialidad de la información de la Cooperativa.

Amenaza: Circunstancia desfavorable que puede ocurrir de forma natural, accidental o intencionada y que deriva en un incidente de seguridad. Tiene consecuencias negativas sobre los activos provocando su funcionamiento incorrecto o pérdida de valor.

Autenticación: Es el procedimiento de comprobación de la identidad de un usuario al tratar de acceder a un recurso de procesamiento o sistema de información.

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
Aviso de privacidad: Documento físico, electrónico o en cualquier otro formato, generado por el responsable, que es puesto a disposición del Titular para el Tratamiento de sus datos personales, el cual comunica al Titular la información relativa a la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las características del Tratamiento que se pretende dar a los datos personales.
Base de Datos: Recopilación organizada de datos almacenada de forma electrónica en un sistema informático.
Biometría: Método de reconocimiento de personas basado en sus características fisiológicas como huellas dactilares, retinas, iris o cara, también de comportamiento como firma, forma de andar y tecleo.
Centros de cómputo: Son zonas específicas para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos.
CERT/CSIRT: Es el Centro de Respuesta a emergencias informáticas. Su función es recibir, revisar y responder a informes de Incidentes de Seguridad Informática.
Ciberseguridad: Conjunto de tecnologías, procesos y prácticas diseñados para proteger redes, computadoras, programas y datos de ataques, daños o accesos no autorizados. En un contexto informático, incluye seguridad cibernética y física.
Cifrado: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información de la Cooperativa.
Certificado digital: Archivo digital generado por una entidad denominada Autoridad Certificadora (CA) que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet.
Cookie: Archivo que almacena datos de comportamiento de un sitio web y que se colocan en el equipo del usuario. De esta forma el sitio web puede consultar la actividad previa del usuario.
Confidencialidad: Es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
Custodia del activo de información: Es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.
Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Pueden ser datos numéricos, alfabéticos, gráficos, visuales, biométricos, auditivos, perfiles o de cualquier otro tipo.
Dato semiprivado: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general.
Dato Privado: Es el dato que por su naturaleza íntima o reserva sólo es relevante para el titular.
Datos sensible: Son aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garantice n los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y a los datos biométricos.
Disponibilidad. Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.
Filtración: En ciberseguridad, la filtración es la acción de que un delincuente rompa los filtros de seguridad informática para llevar a cabo el objetivo de su ataque.
Firewall: Dispositivo tecnológico que tiene como función proteger la red interna de una compañía de accesos no autorizados del exterior vía Internet.
Fuga de datos: Es la pérdida de la confidencialidad de la información privada de una persona o empresa. Información que, a priori, no debería ser conocida más que por un grupo de personas, en el ámbito de una organización, área o actividad, y que termina siendo visible o accesible para otros.
Habeas data: Derecho de las personas naturales a conocer, actualizar y rectificar toda la información que se relacione con ellas y que se almacene en bases de datos, incluido el derecho de supresión.
Hacking ético: Es el conjunto de actividades para ingresar a las redes de datos y voz de la Cooperativa con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.
Incidente de seguridad: Es un evento adverso, confirmado o bajo sospecha, que afecta a un sistema de información, a una red, o la violación, o inminente amenaza de violación de la Política de Seguridad de la Información.
Integridad: Es la garantía de exactitud y fiabilidad de la información.
Intranet: Es una herramienta utilizada para dar a conocer a todos los empleados, funcionarios y contratistas información de interés general, como el acceso a los desprendibles de pago, publicados por el Departamento de talento humano.
Licencia de software: Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.
Medio removible: Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

Parche de seguridad: Conjunto de cambios que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos.
Perfiles de usuario: Son grupos que concentran varios usuarios que requieren autorizaciones para acceder a los recursos tecnológicos o a los sistemas de información.
Plan de contingencia: Estrategia constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil de los sistemas de información que soportan los procesos de negocio considerados críticos en el Plan de Continuidad de Negocio de la Cooperativa.
Plan de continuidad: Conjunto de planes de actuación, de emergencia, de finanzas, de comunicación y planes de contingencias destinados a mitigar el impacto provocado por la concreción de determinados riesgos sobre la información y los procesos de negocio de la Cooperativa.
Propietario de la información: Es la unidad organizacional o proceso donde se crea y administra la información.
Respaldo: Es una copia de seguridad de los datos originales de un sistema de información, que se realiza con el fin de disponer de un medio de recuperación, en caso de que los sistemas sufran daños o pérdidas accidentales.
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.
Seguridad de la Información: Protección que se brinda a los activos de información mediante medidas preventivas con el fin de asegurar la continuidad del negocio y evitar la materialización de los riesgos
Spam: Correos electrónicos que llegan a las cuantas de los usuarios, sin que estos los hayan solicitado. En general portan propaganda y son enviados de remitentes desconocidos.
Titular: Persona natural cuyos datos personales sean objeto de tratamiento.
Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.
Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el encargado por cuenta del responsable.
Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
Suplantación de identidad: Actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude o acoso (cyberbulling).
Usuario: Es la persona natural o jurídica que tiene interés en el uso de la información de carácter personal.
Virus: Código malicioso que se propaga o infecta insertando una copia de sí mismo en otro programa para convertirse en parte de él. Un virus no puede ejecutarse por sí mismo, requiere que el programa que lo aloja sea ejecutado para poder realizar sus operaciones.
Vulnerabilidades: Son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la cooperativa (amenazas), las cuales se constituyen en fuentes de riesgo.

GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

La Cooperativa define y pone en marcha el SGSI como un componente integral de sus prácticas de buen gobierno, proporcionando una dirección estratégica en las actividades, que permitan garantizar el logro de los objetivos propuestos y la gestión de los riesgos de seguridad de la información.

ESTRATEGIA DE SEGURIDAD

Con el propósito de dar cumplimiento a lo establecido por la Superintendencia de la Economía Solidaria referente a seguridad de la información, la Cooperativa determina las siguientes estrategias:
Definición de políticas y procedimientos.
Socialización.
Capacitación.
Seguimiento.
Retroalimentación.
Actualización y mejoras continuas.

RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión de riesgos es un proceso encaminado a minimizar las vulnerabilidades y posibles pérdidas de información que pueden llegar a materializarse y afectar económica y reputacionalmente a la Cooperativa. Para tal efecto, se determinan los posibles riesgos, y los niveles de aseguramiento, los cuales se encuentran inmersos en el Anexo N° 4 del Manual SARO y en el Manual de Matriz de Riesgos.

PRINCIPIOS FUNDAMENTALES

El Sistema de seguridad de la información de la Cooperativa aplicará de manera integral los siguientes principios:

DISPONIBILIDAD: Establece que la información debe estar disponible para su uso en todo momento, para ser usada o vista solo por personal autorizado.

INTEGRIDAD: Consiste en salvaguardar la exactitud y estado completo de los activos de información, es decir que la información solo pueda ser modificada por personal autorizado.

CONFIDENCIALIDAD: Establece que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta política está orientada a fortalecer los mecanismos de seguridad de los activos de información e infraestructura tecnológica, permitiendo la implementación de procesos que conlleven a prevenir la materialización de riesgos de seguridad informática y su remediación inmediata. En consecuencia, la Cooperativa del Magisterio CODEMA define en el presente documento los lineamientos para la atención adecuada de estos eventos.

OBJETIVOS DE LA POLITICA DE LA SEGURIDAD

Establecer directrices generales relacionadas con seguridad de la Información.

Cumplir con todos los requisitos estatutarios, reglamentarios y contractuales que estén orientados a la seguridad de la información.

Establecer los niveles de acceso a la información corporativa, brindando confidencialidad, integridad y disponibilidad.

Fortalecer la cultura de seguridad de la información en trabajadores, asociados, beneficiarios de los asociados, proveedores, contratistas, aprendices, practicantes y demás usuarios externos de CODEMA.

Gestionar los riesgos de seguridad de la información de acuerdo con las directrices de la Cooperativa, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información.

Establecer un modelo organizacional de Seguridad de la Información, definiendo los roles y responsabilidades de los que intervienen en esta política.

Apoyar al modelo de continuidad del negocio y plan estratégico.

Mantener la política de Seguridad de la Información actualizada, a efectos de asegurar su vigencia y eficacia.

Informar las conductas que afecten la seguridad de la información

Proteger los activos de información.

CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Activos físicos:

Edificios, centros de cómputo, servidores, equipos, armarios de red (Racks), cableado, escritorios, cajoneras, archivadores, dispositivos de identificación y autenticación, control de acceso del personal. circuito cerrado de TV.

Controles del entorno de TI:

Alarmas, sistema de refrigeración, supresión contra incendio, sistemas de alimentación ininterrumpida, alimentación de potencia y de red.

Hardware de TI:

Estaciones de trabajo, computadores de escritorio y portátiles, dispositivos de almacenamiento, servidores, mainframes, módems, dispositivos de comunicaciones, impresoras, scanner, fotocopiadoras y equipos multifunción.

Documentación:

Manuales de Procedimientos, programas, guías, formatos, manuales y demás documentación física de propiedad de la Cooperativa del Magisterio.

Activos de servicios de T.I:

Servicios de autenticación de usuario y administración de procesos de usuario, aplicaciones, Firewalls, servidores proxy, servicios de red, servicios web, servicios inalámbricos, antivirus, antispyware, antispam, detección y prevención de intrusiones, seguridad, FTP, bases de datos, correo electrónico y mensajería instantánea, herramientas de desarrollo, contratos de soporte y mantenimiento de software.

Recursos humanos:

Internos: Trabajadores: Directivos, empleados.

Externos: Consultores externos o asesores especialistas, trabajadores temporales, pasantes, proveedores y asociados.

CLASIFICACIÓN DE LA INFORMACIÓN

La información de CODEMA se clasifica según su confidencialidad, integridad y disponibilidad de acuerdo con la sensibilidad e importancia de la misma.

SEGÚN SU CONFIDENCIALIDAD

Pública: Información entregada o publicada sin restricciones, que puede ser conocida y utilizada sin que esto conlleve a un impacto negativo para la Cooperativa.

Interno: Es aquella información dirigida a los miembros de la Cooperativa, cuya divulgación, uso, alteración o destrucción podría resultar en pérdidas, materialización de eventos de riesgo, impactando la credibilidad, reputación u otros asuntos relacionados con la privacidad.

Confidencial: Información que por su contenido solo interesa a quienes va dirigida y cuya divulgación no autorizada puede ocasionar perjuicios a la Cooperativa o a una persona.

Reservado: Información cuya divulgación no autorizada puede ser perjudicial para los intereses o prestigio de la Cooperativa, proporcionar ventajas a la amenaza actual o potencial, o causar bajas o pérdidas graves.

SEGÚN SU INTEGRIDAD

No puede repararse y ocasiona pérdidas graves para la Cooperativa.

Difícil reparación y pérdidas significativas.

Puede repararse, pérdidas leves.

No afecta la operación y puede repararse fácilmente.

SEGÚN SU DISPONIBILIDAD

Críticos: la interrupción es de minutos y hasta 12 horas y podría ocasionar pérdidas graves de información relevante para la Cooperativa.

Urgente: la interrupción es hasta por 24 horas y podría ocasionar pérdidas significativas de información relevante para la Cooperativa.

Importante: interrupción hasta por 72 horas y podría ocasionar pérdidas leves de información relevante para la Cooperativa.

Normal: interrupción de hasta siete días y podría ocasionar pérdidas de información no relevante para la Cooperativa.

No esenciales: la interrupción es superior a 30 días y podría ocasionar pérdidas de información no relevante para la Cooperativa

ROTULADO DE LA INFORMACIÓN

Todos los documentos físicos o digitales expedidos por CODEMA, deberán ser rotulados de acuerdo con el esquema definido en las tablas de clasificación documental. Los mismos contemplarán los activos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información:

Copia.

Almacenamiento.

Transmisión por correo, fax, correo electrónico.

Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos).

El responsable de Seguridad Informática definirá un procedimiento para el rotulado y manejo de la información el cual hará parte del sistema de gestión de la seguridad informática (SGSI), de acuerdo con el esquema de clasificación definido.