METROCOLOR	**POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES**	Código:	MAN-33-002
		Versión:	002
		Fecha:	2018-09-07

1. Objetivo y Alcance.

Dar cumplimiento a lo dispuesto en la Ley N° 29733, Ley de Protección de Datos Personales (en adelante LPDP), y su reglamento. Aplica a todo el personal de Metrocolor S.A. (en adelante Metrocolor) que dé tratamiento a datos personales, así como a los proveedores de servicios que participan en el tratamiento de los datos personales. Es un deber de los trabajadores de Metrocolor conocer y aplicar la presenta política. Los presentes términos y condiciones aplican para cualquier registro de datos personales realizado para la vinculación a cualquier producto, servicio o beneficio que brinda Metrocolor.

2. Definiciones.

a. Datos personales.

Es aquella información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.

b. Titular de datos personales.

Persona natural a quien corresponde los datos personales.

c. Titular del banco de datos personales.

Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.

d. Datos sensibles.

Es aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales, la información relativa a la salud física o mental u otras análogas que afecten su intimidad.

e. Banco de datos personales.

Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.

f. Banco de datos personales no automatizado.

Conjunto de datos de personas naturales no computarizado y estructurado conforme a criterios específicos, que permita acceder sin esfuerzos desproporcionados a los datos personales, ya sea aquel centralizado, descentralizado o repartido de forma funcional o geográfica.

g. Banco de datos personales automatizado.

Conjunto de datos personales que reciben tratamiento a través de un sistema informático, computarizado. Están incluidos los bancos de datos que almacenan la información en soportes informáticos (discos duros, computadoras, DVD, etc.) y que se requiere para acceder a los datos utilizar cualquier tipo de herramienta aplicación o procedimiento informatizado.

h. Banco de datos complejo.

Sirven para el tratamiento de datos personales cuya finalidad se cumple en un plazo indeterminado o superior a un año. Sirven para el tratamiento de datos personales que es realizado en múltiples localizaciones (Oficinas o dependencias diferentes en la misma ciudad o ciudades diferentes, servicios tercerizados o similares). Puede incluir datos sensibles. Tiene como titular a una persona jurídica o entidad pública.

i. Responsable de la Seguridad General de los Bancos de Datos Personales.

Persona designada por el Titular de Banco de Datos Personales (Gerencia General) para ser el responsable del cumplimiento de esta política, coordinar y controlar la implementación y aplicación de las medidas de seguridad.

j. Derechos ARCO.

Son los derechos de Acceso, Rectificación, Cancelación y Oposición que posee el titular de los datos.

(1) Acceso: derecho a obtener la información que sobre ella tenga otro en un banco de datos.

(2) Rectificación (actualización, inclusión): derecho a que se modifiquen los datos que resulten ser parcial o totalmente inexactos, incompletos, erróneos, desactualizados o falsos.

(3) Cancelación (supresión): posibilidad de solicitar la supresión o cancelación de sus datos personales de un banco de datos personales cuando éstos hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hayan sido recopilados, o en los casos en los que no están siendo tratados conforme a la Ley y al reglamento.

(4) Oposición: posibilidad de oponerse, por un motivo legítimo y fundado, referido a una situación personal concreta, a figurar en un banco de datos o al tratamiento de sus datos personales, siempre que por una ley no se disponga lo contrario.

k. Tratamiento de datos personales.

Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

l. Transferencia de datos personales.

Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.

m. Encargado del banco de datos personales.

Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales.

n. Flujo transfronterizo de datos personales.

Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.

3. Responsabilidad.

a. Gerente General.

(1) Determinará la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.

(2) Deberá designar a la persona que velará por el cumplimiento de la presente Política y de la Ley de Protección de Datos Personales en Metrocolor.

(3) Aprobará la restauración de backups

b. Responsable de la Seguridad General de los Bancos de Datos Personales.

(1) Cumplir con los requerimientos exigidos por la Autoridad Nacional de Protección de Datos Personales, según la ley, su reglamento, directivas de seguridad y cualquier otro documento relacionado.

(2) Dar trámite a las solicitudes de los titulares de los datos y fomentará la protección de datos personales.

(3) Coordinar la actualización de la información relativa a los bancos de datos personales, de aplicar, registrando dichos cambios ante la Autoridad Nacional de Protección de Datos Personales.

(4) Gestionar la ejecución de las capacitaciones al personal de Metrocolor involucrado en el tratamiento de datos personales.

(5) Resolver cualquier duda respecto al tratamiento de datos personales dentro de Metrocolor.

(6) Recibir a los miembros de la Autoridad Nacional de Protección de Datos Personales, en caso de efectuarse fiscalizaciones, así como recibir, procesar y canalizar cualquier solitud que se pueda presentar por parte de la misma Autoridad o de cualquier titular de los datos personales.

(7) Gestionar la realización de auditorías periódicas al cumplimiento de la normativa.

(8) Comunicar al titular de los datos personales los incidentes que puedan afectar su integridad.

c. Jefe de Recursos Humanos

(1) Proteger los BDP contra acceso físico no autorizado.

(2) Autorizar a retirar o trasladar de datos personales, utilizando los mecanismos de seguridad implementados.

(3) Eliminar la información contenida en los BDP, cumpliendo el tiempo mínimo requerido por la Ley.

(4) Asegurar la recuperación de datos personales (en la medida de lo posible).

(5) Aprobar la restauración de copias de seguridad de los bancos de datos no automatizados.

(6) Designar o retirar los accesos a los sistemas que dan soporte a los bancos de datos.

(7) Ejecutar las capacitaciones al personal de Metrocolor.

d. Coordinador de Compras

(1) Proteger el BDP contra acceso físico no autorizado.

(2) Autorizar a retirar o trasladar de datos personales, utilizando los mecanismos de seguridad implementados.

(3) Eliminar la información contenida en los BDP

(4) Asegurar la recuperación de datos personales (en la medida de lo posible).

(5) Adecuar los contratos con terceros, de acuerdo a la Ley.

e. Coordinador de Ventas

(1) Proteger el BDP contra acceso físico no autorizado.

(2) Autorizar a retirar o trasladar de datos personales, utilizando los mecanismos de seguridad implementados.

(3) Eliminar la información contenida en los BDP

(4) Asegurar la recuperación de datos personales (en la medida de lo posible).

f. Coordinador de SST

(1) Proteger el BDP contra acceso físico no autorizado.

(2) Autorizar a retirar o trasladar de datos personales, utilizando los mecanismos de seguridad implementados.

(3) Eliminar la información contenida en los BDP

(4) Asegurar la recuperación de datos personales (en la medida de lo posible).

(5) Aprobar la restauración de copias de seguridad de los bancos de datos.

4. Políticas sobre principios rectores.

a. Legalidad.

La recopilación de los datos personales deberá realizarse conforme a lo establecido por la Ley de Protección de Datos Personales, la cual prohíbe la recopilación de dichos datos por medios fraudulentos, desleales o ilícitos.

b. Consentimiento.

Todo tratamiento de los datos personales deberá contar con el consentimiento o la autorización de la persona titular de los datos personales. Se considera que el tratamiento de los datos personales es lícito cuando el titular del dato personal hubiere prestado su consentimiento libre, previo, expreso, informado e inequívoco:

(1) Libre: Deberá de ser dado de manera voluntaria.

(2) Previo: Deberá de ser pedido con anterioridad a la recopilación de datos.

(3) Expreso e inequívoco: Deberá ser manifestado en condiciones que no admitan dudas de su otorgamiento.

(4) Informado: Cuando el titular de los datos se le comunique de manera clara, expresa, con lenguaje sencillo quién, por qué, y cómo van a ser tratados sus datos personales.

Tratándose de datos sensibles, el consentimiento deberá ser otorgado por escrito, a través de una firma manuscrita, firma digital o cualquier otro mecanismo de autenticación que garantice la voluntad inequívoca del titular.

Por otro lado, tomar en consideración que siempre que los datos personales sean suministrados por un tercero, ese tercero debe contar con la autorización del titular que le permita compartir dicha información con Metrocolor.

c. Finalidad.

Toda recopilación de datos personales deberá tener una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no deberá extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.

Se considerará que una finalidad está determinada cuando haya sido expresada con claridad, sin lugar a confusión y cuando de manera objetiva se especifica el objeto que tendrá el tratamiento de los datos personales. Tratándose de banco de datos personales que contengan datos sensibles, su creación solo puede justificarse si su finalidad además de ser legítima, es concreta y acorde con las actividades o fines explícitos del titular del banco de datos personales.

Tomar en consideración que si Metrocolor requiere utilizar datos personales con una finalidad distinta a la originalmente informada y autorizada por su titular, se deberá obtener del titular de los datos una nueva autorización.

Por otro lado, los profesionales que realicen el tratamiento de algún dato personal, además de estar limitados por la finalidad de sus servicios, se encuentran obligados a guardar secreto profesional.

d. Proporcionalidad.

Todo tratamiento de datos personales deberá ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.

e. Calidad.

Los datos personales que vayan a ser tratados deberán ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados. Deberán conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento.

f. Seguridad.

El titular del banco de datos personales y el encargado de su tratamiento deberá adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deberán ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.

g. Disposición de recurso.

Todo titular de datos personales deberá contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales. Metrocolor deberá reconocer y garantizar a los titulares de los datos personales los siguientes derechos ARCO:

(1) Acceso: derecho a obtener la información que sobre ella tenga otro en un banco de datos.

(2) Rectificación: derecho a que se modifiquen los datos que resulten ser parcial o totalmente inexactos, incompletos, erróneos, desactualizados o falsos.

(3) Cancelación: posibilidad de solicitar la supresión o cancelación de sus datos personales de un banco de datos personales cuando éstos hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hayan sido recopilados, o en los casos en los que no están siendo tratados conforme a la Ley y al reglamento.

(4) Oposición: posibilidad de oponerse, por un motivo legítimo y fundado, referido a una situación personal concreta, a figurar en un banco de datos o al tratamiento de sus datos personales, siempre que por una ley no se disponga lo contrario.

h. Nivel de protección adecuado.

Para los casos de flujo transfronterizo de información de datos personales, se deberá garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, equiparable a lo previsto por esta Ley o por los estándares internacionales en la materia.

5. Políticas sobre medidas de seguridad organizativas.

a. Se deberá desarrollar una estructura organizacional con roles y responsabilidades de acuerdo a la proporcionalidad de los datos a proteger. Para ello, Metrocolor deberá designar formalmente un responsable de seguridad del banco de datos personales, quien coordinará la implementación y aplicación de las medidas de seguridad. El rol de responsable de seguridad del banco de datos personales debe asignarse a una persona que tenga las capacidades y autoridad necesaria para el desarrollo de sus funciones.

b. Se deberá llevar un control y registro de los operadores con acceso al banco de datos personales con el objetivo de poder identificar la trazabilidad del personal con acceso en determinado momento. Para ello, en el caso de bancos de datos automatizados, se deberá contar con controles de accesos lógicos y con registros de auditoría. Para el caso de bancos de datos no automatizados, se deberá contar con un registro manual de las personas que tienen acceso y hacen uso de los mismos.

c. Se deberá revisar periódicamente la efectividad de las medidas de seguridad adoptadas y registrar dicha verificación en un documento adjunto al banco de datos personales.

d. Se deberán adecuar los sistemas de gestión, o aplicaciones existentes que intervengan en el tratamiento de datos personales, conforme a la Ley N° 29733, Ley de Protección de Datos Personales, y su reglamento.

e. Se deberán adecuar los procesos del negocio involucrados en el tratamiento de datos personales a los requisitos establecidos en la Ley N° 29733, Ley de Protección de Datos Personales, y su reglamento.

f. Se deberá contar con procedimientos documentados adecuados que incluyan el tratamiento de datos personales, para las áreas claves de Metrocolor que tienen relación con flujo de información personal, detallando, entre otros aspectos, la descripción de los datos personales tratados, origen y procedimiento de obtención de los mismos, formatos utilizados, persona responsable de la custodia y tratamiento, ubicación, sistemas utilizados.

g. Se deberá desarrollar un programa de creación de conciencia y entrenamiento en materia de protección de datos personales. Se recomienda que estos entrenamientos tengan una frecuencia anual y estén dirigidos a todo el personal de Metrocolor. Los temas mínimos a ser tratados en dichos entrenamientos serán:

(1) Conceptos claves sobre la Ley de Protección de Datos Personales y la Autoridad Nacional de Protección de Datos.

(2) Principios rectores de la Ley de Protección de Datos Personales;

(3) Bancos de datos de Metrocolor y áreas que le dan tratamiento;

(4) Derechos ARCO.

h. Se deberá desarrollar un procedimiento de auditoría respecto de las medidas de seguridad implementadas, teniendo como mínimo una auditoría anual. Se recomienda que esta auditoría sea proporcionada por una firma externa. Los resultados de la auditoría deben iniciar la implementación de acciones correctivas.

i. Se deberá desarrollar un procedimiento de gestión de incidentes para la protección de datos personales. Se deberá incluir como parte de dicho procedimiento, los pasos a seguir para informar al encargado del banco de datos y al titular de los datos personales los incidentes que le afecten. Entre la información que se debe proporcionar, incluir como mínimo:

(1) Naturaleza del incidente.

(2) Datos personales comprometidos.

(3) Recomendaciones al titular de datos personales

(4) Medidas correctivas implementadas.

j. Se deberá desarrollar un procedimiento de asignación de privilegios de acceso al banco de datos personales y su correspondiente registro de acceso. Esto aplica tanto para bancos de datos sistematizados, como no sistematizados.

6. Políticas sobre medidas de seguridad jurídicas.

a. Se deberán elaborar formatos de consentimiento para el tratamiento de datos personales, de conformidad con la finalidad para la cual son acopiados.

b. Se deberá desarrollar y mantener actualizado un documento de compromiso de confidencialidad en el tratamiento de datos personales, para todo el personal de Metrocolor, relacionado al tratamiento de datos personales, el cual subsista aún después de finalizar la relación contractual con Metrocolor.

c. Cuando el tratamiento de datos personales se realice por un tercero, se deberá contar con un convenio o un contrato, que contemple cláusulas de confidencialidad y de eliminación de datos:

(1) Confidencialidad de la información.

Esta obligación subsiste aun después de finalizadas las relaciones con el titular del banco de datos. Asimismo, se establece que cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, estos no pueden aplicarse o utilizarse con un fin distinto al que figura en el contrato.

(2) Eliminación de datos.

Una vez ejecutada la prestación del servicio, los datos personales tratados deben ser suprimidos. En caso se requiera conservarlos, se deberá contar con las medidas de seguridad adecuadas hasta por un plazo de 2 años.

7. **Políticas sobre medidas de seguridad técnicas**

a. Acceso no autorizado al banco de datos personales.

I. Se deberá controlar la asignación y el uso de contraseñas de los usuarios de los sistemas de información que realizan tratamiento de datos personales mediante la adopción de las siguientes medidas:

(1) Solicitar a los usuarios que mantengan en secreto las contraseñas asignadas.

(2) Cuando se utilice un servidor de autenticación, éste debe almacenar las contraseñas de manera cifrada.

(3) Permitir que el usuario cambie la contraseña asignada cuando lo considere necesario.

(4) Requerir el uso de contraseñas que contengan al menos 8 dígitos y que sean alfanuméricas (mayúsculas, minúsculas y números) y al menos incluyan un carácter especial.

(5) Cuando el acceso al sistema esté expuesto en entornos públicos (intranet, internet o similares), se debe bloquear al usuario luego de cinco intentos fallidos de autenticación consecutivos.

II. Se deberá revisar periódicamente que los privilegios de acceso a los datos personales correspondan al personal autorizado.

(1) Esta revisión debe generar un registro de revisión que evidencie la realización de dicha revisión.

(2) El periodo de revisión depende de las políticas organizacionales y el tipo de datos personales que contenga el banco de datos personales.

(3) Esta debe realizarse por lo menos semestralmente.

III. Se deberá proteger el banco de datos personales contra acceso físico no autorizado mediante algún mecanismo de bloqueo físico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados (en caso de banco de datos personales no autorizado.

IV. En el caso de utilizar mecanismos informáticos para el tratamiento de datos personales se deberá proteger el banco de datos personales contra acceso lógico no autorizado mediante algún mecanismo de bloqueo lógico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados.

V. El titular del banco de datos personales, o quien este designe, deberá autorizar o retirar el acceso de usuarios que realicen tratamiento de datos personales. Dicha autorización debe registrarse.

VI. Se deberán identificar los accesos realizados a los datos personales para su tratamiento, considerando al menos, los siguientes campos:

(1) Fecha y hora del acceso

(2) Persona o personas que realiza(n) el acceso

(3) Identificador del titular de los datos personales a tratar (mediante mecanismo de disociación aplicado)

(4) Motivo del acceso.

b. Alteración no autorizada del banco de datos personales

I. Todo traslado de datos personales hacia lugares fuera de los ambientes en donde se ubica el banco de datos personales deberá contar con la autorización del titular del banco de datos personales o quien éste designe para ello.

II. Todo traslado de datos personales deberá considerar lo siguiente:

(1) Todos los traslados de información contenida en los bancos de datos deberán ser autorizados por el Supervisor de Seguridad de la información designado. Ello deberá quedar formalmente establecido mediante un acuerdo entre cualquiera de los anteriores y el titular del banco de datos.

(2) Los datos en soporte físico deben estar contenidos en un contenedor que evite su acceso y legibilidad, así como un mecanismo de verificación de la no vulneración del contenedor.

(3) Los datos contenidos en soporte informático deben transportarse previa encriptación y un mecanismo de verificación de la integridad (checksum MD5, firma digital o similar).

II. Cuando se requiera eliminar la información contenida en un medio informático removible, se deberán utilizar mecanismos seguros de eliminación que incluyan el borrado total de la información y/o la destrucción del medio, de forma tal que, no permitan la recuperación de dichos datos.

(1) Asimismo, el titular del banco de datos personales deberá designar a las personas autorizadas a eliminar la información de datos personales contenida en los medios informáticos removibles.

(2) El titular del banco de datos personales, cuando sea el caso, deberá designar a las personas autorizadas a generar y/o eliminar las copias o reproducciones de los datos personales.

III. Se deberán implementar las siguientes medidas para preservar la confidencialidad de los datos personales:

(1) Utilizar impresoras, fotocopiadoras, scanner u otros equipos de reproducción autorizados.

(2) Supervisar el proceso de copia o reproducción de los documentos. No dejar desatendido el equipo.

(3) Retirar los documentos originales y las copias del equipo inmediatamente después de finalizada la copia o reproducción.

IV. El titular del banco de datos personales, o quien éste designe, deberá asignar o retirar el privilegio o privilegios (datos a tratar o tarea a realizar) para el tratamiento de datos personales a usuarios autorizados.

V. Dicha operación deberá ser registrada. Los datos a registrar deben incluir como mínimo:

(1) Usuario (en sistemas informáticos el identificador de usuario).

(2) Privilegio asignado o retirado al usuario.

(3) Fecha y hora de asignación y/o retiro de privilegios del usuario.

(4) Usuario que realiza la asignación y/o retiro de privilegios (en sistemas informáticos el identificador de usuario).

c. Pérdida del banco de datos personales.

I. Se deberán realizar copias de respaldo de los datos personales para permitir su recuperación en caso de pérdida o destrucción, teniendo en consideración lo siguiente:

(1) Toda copia de respaldo de los datos personales deberá estar protegida mediante técnicas de cifrado y almacenada en un local seguro y distante al ambiente principal de tratamiento de datos, para garantizar su disponibilidad frente a un desastre en el ambiente principal (considerar el almacenamiento en una localización diferente o remota).

(2) La frecuencia y el periodo de conservación de los respaldos deberá ser acorde con la finalidad del tratamiento a realizar y el impacto de la pérdida en los derechos del titular de los datos personales.

(3) Cuando sea pertinente, se deberán incorporar mecanismos que garanticen la continuidad del tratamiento de datos personales, principalmente cuando la finalidad tenga un alto impacto en relación con los titulares de datos personales o el bien común.

II. Toda recuperación de datos personales, desde su copia de respaldo, deberá contar con la autorización del encargado del banco de datos personales.

III. Se deberán realizar pruebas de recuperación de los datos personales respaldados para comprobar que las copias de respaldo pueden ser utilizadas en caso de ser requerido. Estas

pruebas deben realizarse por lo menos en forma semestral y se deberán documentar los resultados de las pruebas incluyendo:

(1) Fecha y hora de la prueba.

(2) Nombre de la persona que realizó la prueba.

(3) Banco de datos personales recuperado.

(4) Archivo recuperado y fecha de los datos recuperados.

(5) Tiempo de recuperación.

(6) Resultados de las pruebas.

(7) Acciones tomadas en caso de pruebas insatisfactorias.

d. Tratamiento no autorizado del banco de datos personales:

I. Todo banco de datos personales no automatizado deberá mantener los datos personales independizados, de modo que pueda referirse unívocamente a un titular de datos personales sin exponer información de otro.

II. El titular del banco de datos personales deberá informar al titular de datos personales los incidentes que afecten significativamente sus derechos patrimoniales o morales, tan pronto se confirme el hecho. La información mínima que se deberá proporcionar incluye:

(1) Naturaleza del incidente.

(2) Datos personales comprometidos.

(3) Recomendaciones al titular de datos personales.

(4) Medidas correctivas implementadas.

III. Los equipos utilizados para el tratamiento de los datos personales deberán recibir mantenimiento preventivo y correctivo de acuerdo a las recomendaciones y especificaciones del proveedor para asegurar su disponibilidad e integridad. El mantenimiento de los equipos deberá ser realizado por personal autorizado.

IV. Los equipos utilizados para el tratamiento de los datos personales deberán contar con software de protección contra software malicioso (virus, troyanos, spyware, etc.), para proteger la integridad de los datos personales. El software de protección deberá ser actualizado frecuentemente de acuerdo a las recomendaciones y especificaciones del proveedor.

V. La información de datos personales que se transmite electrónicamente deberá ser protegida para preservar su confidencialidad e integridad, teniendo en consideración lo siguiente:

(1) Transporte electrónico de datos personales en forma cifrada, lo cual puede realizarse mediante el cifrado de la información antes de su transmisión o mediante el uso de protocolos de comunicación cifrados (Ejemplo: VPN, correo electrónico cifrado, FTP seguro, entre otros).

(2) Uso de firmas digitales para validar la identidad del emisor de la información.

VI. Para los casos de flujo transfronterizo de datos personales, el receptor o importador de datos personales deberá implementar las medidas de seguridad definidas por el emisor o exportador de datos personales en el documento de seguridad.

VII. La aceptación de la implementación de las medidas de seguridad por parte del receptor o importador de datos personales deberá establecerse por escrito mediante cláusulas contractuales u otro instrumento jurídico.

VIII. En relación a la seguridad en servicios de tratamiento de datos personales por medios tecnológicos tercerizados, se deberán de tener en cuenta las siguientes medidas:

(1) Que el proveedor no tenga acceso a la información de datos personales que utilicen su infraestructura.

(2) Que el proveedor no brinde acceso a terceros a los datos personales que utilicen su infraestructura.

(3) La destrucción o imposibilidad de recuperación de los datos alojados en el servicio una vez concluida la relación con el proveedor.

(4) Uso de canales seguros para la transferencia de datos personales.

(5) Garantizar el cumplimiento de las medidas de seguridad en todos los lugares en donde se encuentre distribuida la infraestructura del proveedor.

IX. Todo evento identificado que afecte la confidencialidad, integridad y disponibilidad de los datos personales, o que indique un posible incumplimiento de las medidas de seguridad establecidas, deberá ser reportado inmediatamente al encargado del banco de datos personales.

X. Se deberá realizar una auditoría sobre el cumplimiento de la Ley de Protección de Datos Personales en Metrocolor, bajo responsabilidad del titular del banco de datos personales. Para el caso de bancos de datos complejos y críticos, esta deberá ser realizada por una firma externa, mientras que para el caso de bancos de datos intermedios, está podrá ser realizada a través de revisiones internas a cargo de un responsable designado por el titular de los bancos de datos.

XI. Se deberán realizar acciones correctivas y de mejora continua, a partir de la realización de las auditorías de cumplimiento de la Ley de Protección de Datos Personales en Metrocolor.

e. Sobre el Aviso de Privacidad.

En Metrocolor contamos con Avisos de Privacidad a través de los cuales se informará a los titulares de los datos personales, de forma previa a la recopilación de los datos personales, qué información se recabará de ellos y con qué fines.

8. Información de contacto.

I. Si se cuenta con alguna consulta o duda con respecto a la presente política, el trabajador de Metrocolor deberá comunicarse con la persona responsable de la protección de datos personales dentro de Metrocolor.

II. El titular de los datos puede revocar el consentimiento que ha otorgado a Metrocolor. Para el tratamiento de sus datos personales contactando al correo electrónico <datospersonales@metrocolor.com>, indicando su nombre completo, datos de contacto y especificando la revocación que solicita.

III. El titular de los datos personales puede ejercitar los derechos de acceso, rectificación, cancelación y oposición al tratamiento de sus datos personales (derechos “ARCO”), por sí o mediante representante legal debidamente acreditado, enviando una solicitud al correo electrónico que deberá contener por lo menos:

(1) Nombre y domicilio u otro medio para comunicar la respuesta a su solicitud.

(2) Los documentos que acrediten su identidad o, en su caso, la representación legal.

(3) La descripción clara y precisa de los datos personales respecto de los que se solicita ejercer alguno de los derechos ARCO.

(4) La manifestación expresa del derecho ARCO que desee ejercer.

(5) Cualquier otro elemento que facilite la localización de los datos personales.

IV. El responsable de Protección de Datos deberá recibiría la solicitud de ejercicio de derechos ARCO y deberá darle trámite de acuerdo al procedimiento establecido. Se deberá entregar al titular o su representante legal una constancia de confirmación de la ejecución del acceso, rectificación, cancelación y oposición solicitada.

[1] Ley de Protección de Datos Personales: TÍTULO I PRINCIPIOS RECTORES .

Elaborado por:	Revisado Por:	Aprobado por:

Jhonatan Arias Saravia Coordinador de Tecnologías de Información	Jhonatan Arias Saravia Coordinador de Tecnologías de Información	Dante Scottini Gerente General

Jhonatan Arias Saravia @ 2018-09-10, 10:49:32