

POLITICA DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES - MEXICO

1. OBJETIVO

Esta Política de Protección de Datos Personales ("Política") está elaborada conforme a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares ("LFPDPPP") y el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares ("Reglamento"), en su conjunto "Regulación de Datos Personales".

La Regulación de Datos Personales tiene como finalidad proteger los datos personales en posesión de los particulares y regular su tratamiento legítimo, controlado e informado a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

Con base en lo anterior, la presente política tiene como objetivo, establecer las directrices para la protección de los datos personales, según se define más adelante (los "Datos Personales"). Estas directrices tienen por objeto:

- Cumplir con las leyes y reglamentos aplicables para la protección de datos personales (Constitución Política de los Estados Unidos Mexicanos, LFPDPPP, su Reglamento, Lineamientos del Aviso de Privacidad, así como cualquier otra disposición legal que resulte aplicable);
- Proteger los derechos de los Titulares contra cualquier riesgo de violación de los Datos Personales, incluyendo sin limitar, acceso o uso no autorizado, modificación, destrucción o alteración de estos;
- Ser transparente en los procedimientos para el tratamiento de los Datos Personales;
- Promover la conciencia de la empresa y sus empleados con respecto a la protección de los Datos Personales y cuestiones de privacidad.

2. ALCANCE

Esta Política es aplicable a **Basal Monterrey, S.A. de C.V. y Bajo Cero Frigoríficos, S.A. de C.V.**, ("**Emergent Cold MX**", "**ECLA**" o "**Responsable**"), incluyendo a sus empleados, proveedores (o contratistas) que participen en el Tratamiento de datos personales que se realiza de candidatos, empleados,

clientes, prospectos de clientes, prestadores de servicios, socios comerciales, público en general (en adelante "Titular" o "Titulares").

Esta Política es complementaria a las políticas, lineamientos o estándares globales que rigen a Emergent Cold MX en materia de datos personales, en lo que no contravenga a la LFPDPPP. En caso de que alguna medida, como el cumplimiento de los derechos de los Titulares, involucre medidas de otras empresas del grupo Emergent Cold MX, debe haber comunicación y cooperación con la jurisdicción correspondiente.

3. DEFINICIONES

Los términos que no sean expresamente definidos en esta Política tendrán la definición que otorgue la Regulación de Datos Personales. Para los efectos de esta Política, los términos con mayúscula inicial que se relacionan a continuación tienen el siguiente significado:

- **Aviso de Privacidad:** Documento a disposición de la persona titular de la información de forma física, electrónica o en cualquier otro formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de estos.
- **Datos Personales:** Aquella información concerniente a una persona identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.
- **Datos Financieros y Patrimoniales:** Es la información sobre la capacidad económica de las personas físicas que hace referencia a los recursos que posee y a su capacidad para hacer frente a sus deudas, como pueden ser: información patrimonial, bienes muebles e inmuebles; información fiscal; historial crediticio; ingresos y egresos; cuentas bancarias; seguros; afores; fianzas, número de tarjeta de crédito, número de seguridad, entre otros. Al implicar su uso un riesgo importante para el titular, el Tratamiento de este tipo de datos requiere también consentimiento expreso de su titular.
- **Datos Personales Sensibles:** Aquellos datos personales que afecten a la esfera más íntima de la persona titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para esta. De manera enunciativa más no limitativa se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico,

estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

- **Delegado de Protección de Datos Regional (RDPO):** Persona designada al interior de la Compañía encargada de asegurar que esta cumpla con la regulación en materia de protección de datos personales para todos los países donde ECLA tiene operaciones, supervisando el tratamiento adecuado de los datos, gestionando las solicitudes de los titulares, evaluando riesgos, y notificando incidentes de seguridad a las autoridades y a los afectados cuando corresponda.
- **Delegado de Protección de Datos Local (LDPO):** Persona encargada en cada país de asegurar el cumplimiento de los parámetros regionales y específicos en cada país, supervisando el tratamiento adecuado de los datos, gestionando solicitudes, evaluando riesgos, y notificando incidentes de seguridad a las autoridades del país donde se ubica.
- **Departamento de Cumplimiento:** Equipo local y/o Corporativo designado por Emergent Cold LatAm, los cuales que tendrán como obligación dar trámite a las solicitudes de los Titulares, para el ejercicio de los Derechos ARCO y que fomentarán la protección de los Datos Personales al interior de la empresa.
- **Derechos ARCO:** Los derechos de los Titulares para Acceder, Rectificar, Cancelar y Oponerse al Tratamiento de sus Datos Personales.
- **Encargado:** Son todas aquellas personas físicas o jurídicas que traten Datos Personales por cuenta del Responsable.
- **Fuentes de Acceso Público:** Aquellos medios en donde la consulta de Datos Personales pueda realizarse por cualquier persona no impedida por una norma limitativa, o sin más exigencia que el pago de una contraprestación, derecho o tarifa, en su caso. No incluye a fuentes de acceso que tengan procedencia ilícita.
- **Secretaría de Anticorrupción y Buen Gobierno (o "SABG"):** Es la autoridad competente en materia de protección de datos personales en México.
- **Remisión:** Toda comunicación de Datos Personales, dentro o fuera del territorio mexicano, realizada entre el Responsable y el Encargado.
- **Responsable:** Aquella persona física o moral de carácter privado, que llevan a cabo (o decide) sobre el Tratamiento de los Datos Personales de un Titular. Para efectos de la presente Política, el Responsable del Tratamiento de los Datos Personales será Emergent Cold MX. También puede ser referido como "Sujeto Regulado".
- **Titular:** Persona física a la que corresponden los Datos Personales de que se traten.

- **Transferencia:** Toda comunicación de Datos Personales, dentro o fuera del territorio mexicano, realizada a persona distinta de la Titular, del Responsable o de la persona Encargada del tratamiento.
- **Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos Personales.

4. PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES:

De acuerdo con la Regulación de Datos Personales, los principios que regirán la recolección y el tratamiento de los Datos Personales a los que Emergent Cold MX tiene acceso serán los siguientes:

Principio de Consentimiento: Como regla general, se deberá contar con el consentimiento del titular para el tratamiento de sus datos personales. La solicitud del consentimiento deberá ir siempre ligada a las finalidades concretas del tratamiento que se informen en el aviso de privacidad, es decir, el consentimiento se deberá solicitar para tratar los datos personales para finalidades específicas, no en lo general. El consentimiento debe ser informado, por lo que previo a su obtención, es necesario que el titular conozca el aviso de privacidad.

- **Principio de Legalidad:** El principio de licitud obliga al responsable a que el tratamiento sea con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional.
- **Principio de Información:** ECLA deberá dar a conocer al titular la información relativa a la existencia y características principales del Tratamiento a que serán sometidos sus Datos Personales a través del Aviso de Privacidad, de conformidad con lo previsto en la LFPDPPP y su Reglamento.
- **Principio de Calidad:** Se cumple con el principio de calidad cuando los Datos Personales tratados sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.
- **Principio de Finalidad:** Los Datos Personales solo podrán ser tratados para el cumplimiento de la finalidad o finalidades establecidas en el Aviso de Privacidad.

- **Principio de Lealtad:** El principio de lealtad establece la obligación de tratar los Datos Personales privilegiando la protección de los intereses del Titular y la expectativa razonable de privacidad.
- **Principio de Proporcionalidad:** Solo podrán ser objeto de Tratamiento que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido.
- **Criterio de Minimización:** ECLA deberá realizar esfuerzos razonables para que los Datos Personales tratados sean los mínimos necesarios de acuerdo con la finalidad del tratamiento que tenga lugar.
- **Principio de Responsabilidad:** Este principio consiste en que el Responsable tiene la obligación de velar y responder por el tratamiento de los Datos Personales que se encuentren bajo su custodia o posesión, o por aquellos que haya comunicado a un Encargado, ya sea que este último se encuentre o no en territorio mexicano.

Es necesario tener en cuenta que los nombres de los principios aquí incluidos son meramente descriptivos y a efectos de clasificación, y esto no afectará el alcance que la Regulación de Datos Personales le atribuye a cada uno.

5. DIRECTRICES PARA EL TRATAMIENTO DE DATOS PERSONALES

5.1. FUENTES DE DATOS

Emergent Cold MX podrá obtener Datos Personales ya sea de manera directa, indirecta o a través de Fuentes de Acceso Público, y en este último caso, Emergent Cold MX respetará la expectativa razonable de privacidad, entendida como la confianza que tiene el Titular de que los datos proporcionados serán tratados conforme a lo acordado en la Regulación de Datos Personales; el responsable debe privilegiar esa expectativa y no obtener datos por medios engañosos o fraudulentos.

- Al tratar datos provenientes de “fuentes de acceso público”, el responsable debe corroborar que la fuente cumple las condiciones legales y, aun así, respetar la expectativa razonable de privacidad y la finalidad prevista; además, debe informar su aviso de privacidad a la persona Titular en el primer contacto. (Cfr. Art. 3 fr. X y Art. 9 fr. II LFPDPPP; Art. 7 y 29 Reglamento).
- Si fuera imposible o desproporcionado informar individualmente (por número de titulares o antigüedad de datos), procede gestionar medidas

compensatorias de comunicación masiva con el contenido del aviso de privacidad. (Cfr. Arts. 32–35 del Reglamento.)

- Para efectos prácticos, esta es una lista orientativa del tipo de datos personales que puede recabar Emergent Cold MX en el curso de sus actividades:

Categoría de Titular	Categorías de Datos Personales	Ejemplos de Datos Específicos
Empleados y Personal	• Datos de identificación • Datos de contacto • Datos laborales • Datos patrimoniales y financieros • Datos sensibles (salud, biométricos) • Datos académicos	• Nombre, RFC, CURP, INE/IFE, fecha de nacimiento, estado civil • Domicilio, teléfono, correo electrónico • Puesto, área, historial laboral, evaluaciones de desempeño • Número de cuenta bancaria, salario, deducciones • Certificados médicos, exámenes de salud ocupacional, datos biométricos y huellas dactilares para control de acceso • Títulos, certificaciones (ej. manejo de montacargas, manejo de sustancias refrigerantes)
Clientes Corporativos (Contactos)	• Datos de identificación • Datos de contacto • Datos laborales • Datos comerciales	• Nombre completo, cargo en la empresa • Correo electrónico corporativo, teléfono móvil/oficina • Empresa que representa, área o departamento • Historial de servicios contratados, preferencias de servicio
Proveedores y de Contactos Proveedores	• Datos de identificación • Datos de contacto • Datos patrimoniales y financieros • Datos laborales	• Nombre, RFC (personas físicas con actividad empresarial) • Dirección, teléfono, correo electrónico • Datos bancarios para pagos • Empresa que representa, función

Transportistas y Operadores Logísticos	• Datos de identificación • Datos de contacto • Datos de licencias y certificaciones • Datos de tránsito y ubicación • Datos sensibles (salud)	• Nombre, identificación oficial, RFC • Teléfono móvil, correo electrónico • Licencia de conducir, certificaciones de transporte de carga refrigerada • Datos de GPS/geolocalización de unidades, registros de entrada/salida • Certificados médicos para operadores
Visitantes	• Datos de identificación • Datos de contacto • Datos de acceso • Imágenes (videovigilancia)	• Nombre, identificación oficial, empresa que representa • Teléfono de contacto • Hora y fecha de ingreso/salida, áreas visitadas, motivo de visita • Grabaciones de cámaras de seguridad en instalaciones
Candidatos Empleo	• Datos de identificación • Datos de contacto • Datos académicos • Datos laborales • Datos sensibles (según proceso de selección)	• Nombre, edad, RFC, CURP • Domicilio, teléfono, correo electrónico • CV, títulos, certificados, historial académico • Referencias laborales, experiencia previa • Resultados de exámenes psicométricos, socioeconómicos (si aplica)
Beneficiarios de Empleados	• Datos de identificación • Datos de contacto • Datos de parentesco	• Nombre completo, parentesco con el empleado • Dirección, teléfono • Documentos que acrediten el vínculo familiar
Usuarios de Plataformas Digitales	• Datos de identificación • Datos de contacto • Datos de navegación	• Nombre, usuario • Correo electrónico, teléfono • Dirección IP, cookies, logs de actividad • Contraseñas (encriptadas), patrones de uso del portal/app

	• Credenciales de acceso	
--	--------------------------	--

5.2. RESPONSABLES EN EL TRATAMIENTO DE DATOS

- **Titular de los Datos Personales:**

Es la persona física a quien refieren y pertenecen los datos personales que son objeto de tratamiento. Por tanto, es la única persona que se considera como dueña (titular) de los datos personales, aunque éstos estén en posesión de un tercero para su tratamiento.

- **Responsable del tratamiento de los Datos Personales:**

Emergent Cold MX es la entidad responsable que decide sobre el tratamiento de los datos personales, es decir, la que establece las finalidades del tratamiento o el uso que se le dará a los datos personales, el tipo de datos que se requieren, a quién y para qué se comparten, cómo se obtienen, almacenan y suprimen los datos personales, y en qué casos se divulgarán, entre otros factores de decisión.

- **Encargado del tratamiento de los Datos Personales:**

Los proveedores, agentes, y prestadores de servicios con quienes Emergent Cold MX tenga celebrada una relación contractual, mediante la cual se trata datos personales a nombre y por cuenta de Emergent Cold MX, son considerados Encargados.

- **Equipo Regional de Cumplimiento y Legal:**

Emergent Cold MX cuenta con un equipo regional de Cumplimiento quien se encuentra a cargo de la protección, manejo y registro de los Datos Personales, entre otras, sus obligaciones son:

- ✓ Difundir el contenido de esta Política al interior de la organización.
- ✓ Garantizar el cumplimiento de los principios de protección de Datos Personales y el ejercicio de los derechos de los Titulares.
- ✓ Realizar capacitaciones y programas de concientización en materia de datos personales.

El correo electrónico para la recepción de las solicitudes de Derechos ARCO definido dentro de los Avisos de Privacidad como medio de contacto es:

- Correo electrónico: datospersonales@emergentcold.com

ECLA podrá apoyarse de consultores externos para realizar las funciones del Departamento de Cumplimiento y Legal.

5.3. AVISO DE PRIVACIDAD

El Tratamiento estará siempre limitado al fin establecido en el Aviso de Privacidad que Emergent Cold MX ponga a disposición del Titular. Dicho Aviso de Privacidad deberá cumplir en todo momento con lo establecido en la Regulación de Datos Personales y conforme a los Lineamientos al Aviso de Privacidad, publicados por la Secretaría de Economía y los cuales entraron en vigor a partir del 17 de abril de 2013 (en lo que no se opongan a la LFPDPPP), salvo que se emitan nuevos criterios o lineamientos que replacen a dichos Lineamientos).

Entre los elementos mínimos que debe contener un Aviso de Privacidad, se encuentran los siguientes:

- Identidad y domicilio del responsable.
- Datos personales que se tratarán, identificando los sensibles.
- Finalidades del tratamiento, distinguiendo las que requieren consentimiento.
- Opciones y medios para limitar el uso o divulgación de los datos.
- Medios y procedimientos para ejercer derechos ARCO.
- Procedimiento y medio para comunicar cambios al aviso.
- Mecanismos y procedimientos para revocar el consentimiento.

Independientemente de lo anterior, Emergent Cold MX podrá publicar en su sitio web o en lugares visibles el Aviso de Privacidad, en función de la categoría de la persona Titular de datos personales. Enseguida se propone una tabla con recomendaciones prácticas para cumplir con los criterios de la “puesta a disposición” del aviso de privacidad:

Escenario operativo	Medio recomendado de puesta a disposición	Momento de presentación	Evidencia de cumplimiento
Recepción/guardia en almacenes (alta de visitantes y contratistas)	Aviso “simplificado” impreso en mostrador y cartel; QR/URL al aviso integral; formatos de	Antes o al momento de recabar datos de ingreso	Foto del cartel en sitio; copias controladas del formato de registro; bitácora

	registro con casilla de consentimiento cuando aplique		de actualizaciones del aviso
Control de acceso con biométricos (huella/rostro) a cámaras de frío	Pantalla en el dispositivo con aviso "corto", "simplificado"; vínculo al integral; consentimiento expreso habilitado en la interfaz	Antes de la captura biométrica	Capturas de pantalla del flujo; registro de versión del aviso y logs de consentimiento
Videovigilancia en patios de maniobra y muelles	Carteles visibles en accesos y áreas de CCTV con aviso "corto" y QR/URL al aviso integral	Previo al ingreso a zonas videovigiladas	Fotografías georreferenciadas de señalética; matriz de ubicaciones de letreros
Operación de transporte con geolocalización de unidades y operadores	Aviso "integral" en contrato/alta del operador; "simplificado" en app/MDT de la unidad; checkbox de consentimiento cuando aplique	Antes de activar el rastreo o entregar el equipo	Contratos firmados con referencia de versión del aviso; registros de aceptación en app
Portal web B2B/B2C (solicitudes de cotización, tracking, tickets)	Banner o pop-up inicial con aviso "simplificado" y enlace permanente en footer al "integral"	En el primer uso y antes de enviar formularios	Capturas de interfaz; registro de versiones y fechas de publicación
Cotizaciones y servicio por correo electrónico	Pie de correo con aviso "simplificado" y enlace al "integral"	En el primer contacto o junto con la primera solicitud de datos	Plantillas aprobadas; control de cambios del pie legal
Atención telefónica (altas, soporte,	Aviso "corto" leído por el agente; opción de enviar	Al inicio o antes de solicitar datos	Guiones con sello de versión; grabaciones que

seguimiento de embarques)	SMS/correo con el "integral"		muestren la lectura del aviso
Reclutamiento	Aviso "integral" en vacantes, formatos de candidatura y ferias; "simplificado" en anuncios; consentimiento para datos sensibles si aplica	Antes o al momento de recabar CV/pruebas	Copia de convocatorias con enlace; recibos de aviso firmados
Proveedores y terceros que ingresan a sitio (mantenimiento, calibración, etc.)	Aviso "simplificado" en la recepción/formulario de acceso; "integral" en órdenes de compra/contratos	Antes del registro de entrada o firma del contrato	Contratos con referencia a la versión del aviso; acuses de recibo

Notas de implementación

- Se debe definir la modalidad del Aviso de Privacidad más apropiado:
 - ✓ "Integral" donde se formaliza la relación (contratos, portales).
 - ✓ "Simplificado" donde se captan datos rápidamente (recepción, aplicaciones).
 - ✓ "Corto" cuando el espacio/tiempo es limitado (CCTV, telefonía).
- Asegurarse de que todo aviso "simplificado" o "corto" permita conocer el contenido del aviso "integral" de forma clara y accesible (URL y QR funcionales). La puesta a disposición no exime de proveer el medio para conocer el integral.
- Conserva evidencia: capturas de pantalla, fotos de cartelera, guiones, grabaciones, copias controladas y bitácoras de versión del aviso. Esto facilita demostrar cumplimiento ante requerimientos de la autoridad.

5.4. CONSENTIMIENTO

El Tratamiento está sujeto al otorgamiento del consentimiento por parte del Titular, por lo que queda estrictamente prohibido llevar a cabo cualquier Tratamiento fuera de los estándares establecidos en la presente Política, el Aviso de Privacidad proporcionado al Titular, y sin contar con el consentimiento del Titular correspondiente.

El consentimiento puede ser tácito, excepto en los casos que se señalan más adelante, y se entiende que el Titular lo otorga siempre que este no se oponga al Tratamiento de sus Datos Personales, al presentarle o poner a su disposición el Aviso de Privacidad de Emergent Cold MX.

- **Clasificación de datos personales en función del tipo de consentimiento**

La LFPDPPP establece la siguiente clasificación por tipo de dato personal a efecto de identificar el consentimiento necesario para el tratamiento de los datos personales, de acuerdo con lo establecido por los artículos 7 y 8 de la LFPDPPP.

Tipo de dato personal	Forma del Consentimiento
Generales	Tácito (e.g., Opt-out)
Financieros y Patrimoniales	Expreso
Sensibles	Expreso y por escrito

- **Consentimiento para el Tratamiento de Datos Patrimoniales o Financieros**

Se requiere obtener el consentimiento expreso por parte del Titular cuando del mismo se recaben Datos Financieros o Patrimoniales, los cuales pueden consistir en estados de cuenta, números de cuenta, sueldos, créditos solicitados, entre otros de similar naturaleza.

- **Consentimiento para el Tratamiento Sensibles**

Es principio de ECLA abstenerse de crear bases de datos con Datos Personales Sensibles a menos que sea en atención a finalidades concretas y acordes a las actividades o fines de Emergent Cold MX, en apego a las demás políticas internas.

Para la recolección y el Tratamiento Sensibles, Emergent Cold MX deberá obtener consentimiento expreso y por escrito del Titular. Si el Titular ha brindado su consentimiento expreso y por escrito a Emergent Cold MX, se entiende que ha consentido el uso de sus Datos Personales Sensibles.

5.5. TRANSFERENCIA DE DATOS PERSONALES

Derivado del Tratamiento de Datos Personales, en algunas ocasiones es necesaria la remisión o transferencia de estos. Dentro de los contratos celebrados entre Emergent Cold MX con terceros, se deberán establecer cláusulas o anexos complementarios que contengan, al menos, los requisitos mínimos que exigen la Regulación de Datos Personales, tal como se explica enseguida:

5.5.1. Remisiones (Comunicaciones con Encargados).

De conformidad con lo establecido en el Reglamento, las remisiones consisten en la comunicación de Datos Personales entre Emergent Cold MX (el responsable) y el Encargado, dentro o fuera del territorio mexicano. Las remisiones nacionales e internacionales de Datos Personales entre la compañía y un encargado no requerirán ser informadas al Titular ni contar con su Consentimiento.

Dentro del curso de sus negocios, Emergent Cold MX podrá realizar remisiones, en apego a lo establecido por la Regulación de Datos Personales en México.

Los Acuerdos de Remisión de Datos (o cláusulas) deben incluir las siguientes obligaciones aplicables a los encargados del tratamiento:

- Tratar los datos personales únicamente de conformidad con las instrucciones del responsable del tratamiento;
- Abstenerse de tratar los datos personales para fines distintos de los indicados por el responsable del tratamiento;
- Aplicar medidas de seguridad de conformidad con la normativa aplicable;
- Mantener la confidencialidad con respecto a los datos personales tratados;
- Suprimir los datos personales tratados una vez que se haya cumplido la relación jurídica con el responsable del tratamiento o siguiendo las instrucciones de este, siempre que no exista ninguna disposición legal que exija la conservación de los datos personales;
- Abstenerse de transferir datos personales, salvo en el caso de que el responsable del tratamiento así lo determine, la comunicación se derive de una subcontratación o cuando lo exija la autoridad competente;
- No subcontratar proveedores de tratamiento sin el consentimiento previo por escrito del responsable del tratamiento.

5.5.2. Transferencias (Comunicaciones con Terceros).

De conformidad con la Regulación de Datos Personales, las transferencias consisten en la comunicación de Datos Personales realizada a personas distintas a Emergent Cold MX (el responsable) o al Encargado del Tratamiento. Ya se trate de una transferencia de datos local o transfronteriza (internacional), los requisitos mínimos para permitir las transferencias de datos son los siguientes:

- Consentimiento del titular (salvo que se aplique una excepción legal, artículo 36 de la LFPDPPP).
- Adoptar salvaguardias contractuales (por ejemplo, acuerdos de transferencia de datos, normas corporativas vinculantes ("BCR"), cláusulas contractuales estándar ("SCC")).
- El responsable del tratamiento deberá informar en el Aviso de Privacidad, los fines de la transferencia, una cláusula que indique si la transferencia de datos requiere el consentimiento o si se aplica una excepción autorizada por el interesado y, al menos, la categoría del destinatario de los datos (por ejemplo, proveedor de servicios). Asimismo, los Avisos de Privacidad indican aquellos casos en los que no será necesario el consentimiento del interesado para la transferencia de sus Datos Personales, de conformidad con lo dispuesto en el artículo 36 de la LFPDPPP.
- Durante las transferencias, el tratamiento se realizará de conformidad con las disposiciones del Aviso de Privacidad aplicable.
- ECLA se asegurará de que el destinatario de los Datos Personales sea un sujeto regulado por la normatividad de protección de datos en su calidad de responsable del Tratamiento, indicándole que debe tratar los Datos Personales únicamente según lo acordado en el correspondiente Aviso de Privacidad comunicado.

5.5.3. Transferencias de datos entre empresas del mismo grupo

La transferencia de datos personales a cualquier empresa del mismo grupo corporativo del responsable del tratamiento (por ejemplo, empresas matrices, filiales o afiliadas bajo el control común del mismo grupo del responsable del tratamiento) requiere la celebración de normas corporativas vinculantes ("BCR"), acuerdos de datos entre empresas o similares, a menos que las empresas del grupo estén sujetas a las mismas normas de protección de datos, que deben cumplir con la normativa mexicana de protección de datos.

5.5.4. Obligaciones del tercero receptor

El receptor de los datos deberá: (a) tratar los datos personales de conformidad con el Aviso de privacidad, y (b) asumir las mismas obligaciones que el responsable del tratamiento (que es el exportador de datos).

5.5.5. Recepción de Datos Personales

En caso de que un tercero Responsable ajeno a Emergent Cold MX transfiera Datos Personales a Emergent Cold MX, esta deberá solicitarle, a dicho tercero, el Aviso de Privacidad bajo el cual el Titular autorizó su Tratamiento, debiendo verificar que dicha Transferencia se encuentre contemplada en el mismo.

Emergent Cold MX podrá ser considerada como Encargado, cuando el Tratamiento sea por cuenta del tercero Responsable. En este caso, Emergent Cold MX deberá dar Tratamiento a los Datos Personales transferidos por el tercero Responsable conforme al Aviso de Privacidad que le sea proporcionado.

5.5.6. Excepciones al consentimiento para la transferencia de datos.

Sujeto a un análisis caso por caso, podría aplicarse una excepción al consentimiento para la transferencia de datos (véase el artículo 36 de la LFPDPPP). Dichas excepciones aplican en caso de que la Transferencia: (i) esté prevista en una ley o tratado en el que México sea parte; (ii) sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios; (iii) sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del Responsable, o a una sociedad matriz o cualquier sociedad del mismo grupo del Responsable que opere bajo los mismos procesos y políticas internas; (iv) sea necesaria por virtud de un contrato celebrado o por celebrarse en interés del Titular, por el Responsable y un tercero; (v) sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia; (vi) sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y (vii) sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el Responsable y el Titular.

Si bien en determinados casos se aplica una excepción al consentimiento, obtener el consentimiento al tratar datos sensibles o financieros mitigaría los riesgos asociados a la interpretación de la Autoridad de Protección de Datos en relación

con las excepciones al consentimiento, ya que esta se muestra reacia a aplicar excepciones.

5.5.7. Requisitos del servicio en la nube.

Aplican requisitos particulares adicionales a los proveedores de servicios en la nube, entre los que se incluyen: (a) aplicar políticas de protección de datos personales; (b) subcontratación transparente; (c) abstenerse de incluir condiciones que autoricen o permitan al proveedor asumir la propiedad o titularidad de la información en la que se presta el servicio; (d) mantener la confidencialidad con respecto a los datos personales; (e) notificar los cambios en la política de privacidad o en sus condiciones de servicio; (f) permitir al responsable del tratamiento limitar el tipo de tratamiento en relación con el servicio; (g) establecer y mantener medidas de seguridad adecuadas; (h) suprimir los datos con arreglo a las normas de conservación de datos aplicables; y (i) impedir el acceso no autorizado.

5.6. DERECHOS ARCO

Emergent Cold MX garantizará los derechos de Acceso, Rectificación, Cancelación y Oposición ("Derechos ARCO"), con los que cuentan los Titulares en México, los cuales se describen a continuación:

DERECHO	CONCEPTO	EJEMPLO DE CUMPLIMIENTO
Acceso	Obtener del Responsable los Datos Personales, así como información relativa a las condiciones y generalidades de su Tratamiento.	Poner a disposición del Titular los Datos Personales por cualquier medio previsto en el Aviso de Privacidad.
Rectificación	Modificar los Datos Personales cuando sean inexactos o incompletos.	Corregir o completar los Datos Personales de que se indiquen.

Cancelación	El cese del Tratamiento, total o parcial de los Datos Personales, cuando el Titular considere que los mismos no están siendo tratados conforme a los principios y deberes que establece la Ley y su Reglamento.	Bloquear los Datos Personales de que se traten mediante medidas de seguridad adecuadas hasta el plazo de prescripción legal o contractual que originó el Tratamiento de dichos Datos Personales y notificárselo al Titular en la respuesta a la solicitud de cancelación. Una vez transcurrido el periodo de bloqueo, suprimirlos de todo registro que se tuviere bajo las medidas de seguridad adoptadas.
Oposición	Negativa del Titular al Tratamiento de sus Datos Personales para evitar un perjuicio justificado en su contra, o bien con relación a ciertos fines en específico.	Generar listados de exclusión propios de Emergent Cold MX, con los Datos Personales sobre los que se haya solicitado el ejercicio de este derecho.

5.6.1. Procedimiento para el Ejercicio de los Derechos ARCO

El procedimiento para el ejercicio de los Derechos ARCO será sencillo y gratuito, debiendo cubrir los Titulares únicamente los gastos de envío, reproducción y, en su caso, certificación de documentos.

Los Titulares podrán ejercer sus Derechos **ARCO** a través de los Medios de Contacto presentando:

- Nombre y domicilio u otro medio para comunicarle la respuesta a su solicitud;
- Los documentos que acrediten su identidad o, en su caso, la representación legal;

- La descripción clara y precisa de los Datos Personales respecto de los que se solicita ejercer alguno de los Derechos ARCO;
- La manifestación expresa para revocar su consentimiento al Tratamiento de sus Datos Personales y, por tanto, para que no se usen; y
- Cualquier otro elemento que facilite la localización de los Datos Personales.

Emergent Cold MX llevará un control de entrada de solicitudes que le sean presentadas, para dar respuesta a ellas en un plazo no mayor a 20 (veinte) días hábiles contados a partir de su correcta recepción. Dichos plazos podrán ser ampliados una sola vez por un periodo igual, con causa justificada comunicada al Titular.

En caso de recibir solicitudes con información incompleta o errónea, así lo indicará el Responsable al Titular en un plazo no mayor a 5 (cinco) días hábiles contados a partir de su recepción, para que este lo corrija en un plazo no mayor a 10 (diez) días hábiles contados a partir del día siguiente en que reciba el requerimiento.

El Responsable deberá dar respuesta a toda solicitud, independientemente de que los Datos Personales a que se refiera se encuentren o no en sus registros; asimismo, las respuestas versarán únicamente respecto de los Datos Personales que se hayan especificado en la solicitud respectiva. Cada respuesta que realice el Responsable, deberá ser clara y en lenguaje comprensible para la población media, limitando su contenido única y exclusivamente a los Datos Personales del Titular que la haya solicitado y en ningún momento deberá contener información parcial o total de cualquier otro Titular o tercero.

Independientemente al procedimiento de Derechos ARCO establecido en ley, para la debida atención y manejo de solicitudes de Derechos ARCO, Emergent Cold MX adoptará un procedimiento interno que será supervisado por el Departamento de Cumplimiento y Legal.

Especialmente teniendo en cuenta las situaciones en las que se atienden las solicitudes de los Titulares en relación con el tratamiento de datos personales sujetos a la legislación de otros países, consulte la política de Emergent Cold MX de la jurisdicción correspondiente.

5.6.2. Negativa para el Ejercicio de los Derechos ARCO

ECLA únicamente podrá negar el ejercicio de los Derechos ARCO, ya sea parcial o totalmente, en caso de que: (i) el Titular no acredite su personalidad sobre la titularidad de los Datos Personales; (ii) Emergent Cold MX no cuente con la información solicitada; (iii) el ejercicio de los mismos afecte directamente derechos de terceros; (iv) exista algún impedimento legal; o (v) ya se haya dado respuesta a dicha solicitud de ejercicio previamente.

El caso de que Emergent Cold MX, en su carácter de Responsable, niegue el ejercicio de cualquiera de los Derechos ARCO, deberá justificar su respuesta, así como informar al Titular el derecho que le asiste para solicitar el inicio del procedimiento de protección de derechos ante la SABG.

En el caso del derecho de oposición, este no procederá y podrá ser negado su ejercicio por el Responsable en caso de que el Tratamiento sea necesario para el cumplimiento de una obligación legal que deba cumplir el Responsable.

Ningún empleado, personal o funcionario de Emergent Cold MX se encuentra facultado a negar una solicitud para ejercer los Derechos ARCO de un Titular, salvo aquellos cuyas actividades dentro de Emergent Cold MX consistan en dar trámite y analizar temas relativos a la recolección, tratamiento y almacenamiento de los Datos Personales.

En caso de contravenir a lo dispuesto en esta política, tendrá consecuencias que serán determinadas por Emergent Cold MX.

- **Restricciones para el ejercicio de los derechos.** El ejercicio de los derechos ARCO podrá restringirse por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceras personas, en los casos y con los alcances previstos en las leyes aplicables en la materia, o bien mediante resolución de la autoridad competente debidamente fundada y motivada.
- **Personas facultadas para el ejercicio de los derechos ARCO.** Los derechos ARCO se pueden ejercer por:

1. El titular de los datos personales, previa acreditación de su identidad, a través de la presentación de copia de su documento de identificación y habiendo exhibido el original para su cotejo, o bien, realizando su validación a través de una videoconferencia, o
2. Por el representante del titular, previa acreditación de su identidad, la del titular y la existencia de la representación a través de un instrumento público o carta poder firmada ante dos testigos o declaración en comparación personal o a través de videoconferencia del titular.

Medios para el ejercicio de derechos ARCO. El titular tendrá que seguir el procedimiento indicado en los avisos de privacidad de la organización, sin embargo, la organización es consciente de que el titular de los datos personales puede realizar la solicitud para el ejercicio de sus derechos ARCO a través de cualquiera de los colaboradores de la organización, y que si bien, no sigue lo establecido en los avisos de privacidad, la organización procurará su atención oportuna.

Costos.

- a. El ejercicio de los derechos ARCO es gratuito, por lo que el titular solamente deberá cubrir los gastos de envío y reproducción, y en su caso, certificación.
- b. No obstante, lo anterior, si el mismo titular reitera su solicitud en un periodo menor a 12 meses, los costos de reproducción no pueden ser mayores a 3 días de Unidad de Medida y Actualización vigente, a menos que existan modificaciones sustanciales en el aviso de privacidad que motiven las nuevas consultas.

Acreditación de la identidad. Las solicitudes deberán ser acompañadas de una copia simple de una identificación oficial del Titular o representante legal.

Se aceptarán como identificaciones oficiales:

- a. Tratándose de mexicanos por nacimiento o naturalizados.
 - Credencial para votar vigente, expedida por el Instituto Nacional Electoral (antes Instituto Federal Electoral).
 - Pasaporte vigente.

- Cédula profesional vigente con fotografía. Quedan exceptuadas las cédulas profesionales electrónicas.
 - Credencial del Instituto Nacional de las Personas Adultas Mayores vigente.
 - En el caso de menores de edad, la credencial emitida por Instituciones de Educación Pública o Privada con reconocimiento de validez oficial con fotografía y firma, o la Cédula de Identidad Personal emitida por el Registro Nacional de Población de la Secretaría de Gobernación, vigente.
- b. Tratándose de extranjeros.
- Documento migratorio vigente que corresponda, emitido por autoridad competente (en su caso, prórroga o refrendo migratorio).

Los representantes legales en caso de acreditar deberán presentar:

- Carta poder simple suscrita ante dos testigos, anexando copia simple de sus identificaciones oficiales.
- Documento suscrito por un Notario Público.
- Acudiendo el titular y su representante a declarar en comparecencia ante el responsable.

Personas en el caso de menores de edad, a través del acta de nacimiento del menor.

Solicitudes de derechos ARCO de datos personales de personas en estado de interdicción o incapacidad legal:

- Documento que acredite la identidad del titular de los datos personales.
- Instrumento legal de designación del tutor.
- Identificación oficial del tutor.
- Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela, y que no se encuentra dentro de lo alguno de los supuestos legales de suspensión o limitación de esta.

Solicitudes de derechos ARCO de datos personales de personas fallecidas:

- Identificación oficial de la persona a quien pertenecían los datos personales.
- Acta de defunción correspondiente.

- Documento(s) que acrediten el interés jurídico de quien presenta la solicitud; aquél donde el titular de los datos personales hubiere expresado fehacientemente su voluntad de que esta persona ejerza los derechos ARCO con relación a sus datos personales, o el mandato judicial que en su caso exista para dicho efecto.
- Documento de identificación oficial de quien presenta la solicitud.

Quienes pueden solicitarlo son, de manera enunciativa mas no limitativa:

- El albacea.
- Los herederos.
- Los legatarios.
- Cualquier persona que haya sido designada previamente por el titular para ejercer los derechos ARCO en su nombre.

Se acreditará con copia simple del documento delegatorio, pasado ante la fe de notario público o suscrito ante dos testigos.

Se entenderá por interés jurídico aquel derecho subjetivo derivado de una ley que permite a una persona actuar a nombre de otra que por su situación le es imposible.

En ambos supuestos, se deberá acompañar una carta en la cual se expresen los motivos por los cuales solicita el acceso, rectificación, cancelación u oposición de los datos de la persona.

IMPORTANTE: La identidad del titular y su representante, así como la personalidad ultima descrita, deberán quedar debidamente acreditadas previo al ejercicio del derecho de que se trate, en caso de que resulte procedente mediante la presentación de documentos originales antes señalados para su cotejo. También podrán ser admisibles los instrumentos electrónicos por medio de los cuales sea posible identificar fehacientemente al titular, u otros mecanismos de autenticación permitidos por otras disposiciones legales o reglamentarias, o aquéllos previamente establecidos por ECLA.

5.7. TRATAMIENTO AUTORIZADO

De acuerdo con la Regulación de Datos Personales, el tratamiento automatizado sin intervención humana es aquél que está destinado a evaluar, analizar o predecir determinados aspectos personales del Titular (en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento), sin que exista la intervención de una persona humana. Por ejemplo, ocurre un tratamiento automatizado sin intervención humana cuando se determina la elegibilidad de una persona para acceder a servicios de renta de auto, a través de decisiones algorítmicas.

En caso de que Emergent Cold MX realice un tratamiento automatizado sin intervención humana, deberá observar los siguientes lineamientos:

- **Información/Transparencia:** Informar de manera clara y accesible a los Titulares (preferentemente, a través del aviso de privacidad) sobre la existencia del tratamiento automatizados sin intervención humana, así como la finalidad del tratamiento y los mecanismos para que el Titular pueda oponerse o solicitar el cese del tratamiento, en caso de que dicho tratamiento le produzca (al Titular) efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades.
- **Licitud, Consentimiento y Finalidad:** Garantizar que todo tratamiento automatizado tenga una base legal válida (consentimiento, cumplimiento de contrato, obligación legal, ejercicio de un derecho) y una finalidad determinadas y claras que justifiquen el tratamiento.
- **Proporcionalidad, Minimización y Calidad:** Limitar el tratamiento a los datos estrictamente necesarios y mantenerlos actualizados y exactos, evitando decisiones basadas en información incorrecta o desactualizada.
- **Lealtad (expectativa razonable de privacidad y no discriminación):** Procurar que el tratamiento automatizado sin intervención humana privilegie la protección de los intereses de la persona Titular y la expectativa razonable de privacidad y que no generarán discriminación injustificada ni afecten a grupos vulnerables.
- **Medidas de seguridad:** Implementar medidas de seguridad para proteger los datos personales que estén involucrados en un tratamiento automatizado, Como parte de estas medidas, Emergent Cold MX podrá:

(a) realizar revisiones o auditorías periódicas de los procesos que implican un tratamiento automatizado, así como los canales para que los Titulares ejerzan sus derechos.

(b) realizar una evaluación de impacto a la protección de datos personales cuando el tratamiento automatizado pueda implicar un alto riesgo para los derechos y libertades de los Titulares.

(c) contar con un registro detallado, en donde se documente cada proceso automatizado, incluyendo la descripción del flujo de datos, los sistemas y algoritmos utilizados, la finalidad, la base legal, los tipos de datos tratados y los efectos potenciales sobre los Titulares.

(d) Registrar las medidas implementadas para mitigar riesgos, como revisiones manuales, intervención humana, anonimización, controles de acceso y auditorías.

- **Derechos de los Titulares:** Permitir que los Titulares ejerzan su derecho de oposición y, en su caso, soliciten el cese del tratamiento automatizado sin intervención humana que produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, salvo que el tratamiento sea necesario para cumplir una obligación legal. El proceso para el ejercicio de estos derechos será el mismo que aplica para el ejercicio de Derechos ARCO. Además, Emergent Cold MX deberá mantener un registro de las solicitudes de los Titulares que estén relacionadas con decisiones automatizadas y las acciones tomadas en respuesta.

5.8. MEDIDAS DE SEGURIDAD

La seguridad de los Datos Personales tiene como objetivo proteger contra situaciones accidentales o ilegales de destrucción, pérdida, alteración, comunicación o cualquier forma de procesamiento indebido, además del procesamiento discriminatorio de la información.

ECLA como Responsable del Tratamiento, adoptará las medidas físicas, administrativas y técnicas necesarias para garantizar la seguridad y confidencialidad de los Datos Personales, con el fin de evitar su daño, pérdida, destrucción, robo, extravío, alteración y/o tratamiento no autorizado.

Asimismo, se realizará la relación de las medidas de seguridad que se instauren y que serán aplicadas al Tratamiento, las cuales serán revisadas de tiempo en tiempo por los funcionarios y empleados de Emergent Cold MX.

Como parte de las medidas de seguridad para la protección de datos personales, Emergent Cold MX adoptará las siguientes:

5.8.1. Roles y responsabilidades

Las siguientes áreas de Emergent Cold MX son responsables de la implementación de esta Política. El Consejo de Gerentes es responsables de poner a disposición los recursos adecuados para garantizar la implementación y el cumplimiento de esta Política local y de tomar las medidas adecuadas en caso de incumplimiento.

- El equipo legal y cumplimiento local es responsable de:
 - ✓ Colaborar con las demás áreas en la implementación de esta Política y de los procesos relacionados.
 - ✓ Brindar asesoramiento y capacitación en materia de protección de datos personales como respecto a esta Política y su implementación.
 - ✓ Identificar los períodos de bloqueo que son aplicables para cada categoría de titular de datos personales de los que se realiza el tratamiento de datos personales.
 - ✓ Revisar y mantener actualizado esta Política.
 - ✓ Controlar el cumplimiento de esta Política y supervisar la resolución de cuestiones de incumplimiento significativas.
 - ✓ Identificar las reformas en materia de protección de datos personales que impacten en esta Política.
 - ✓ Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.

El equipo Legal local podrá apoyarse del equipo de Cumplimiento Regional, conforme sea necesario.

- El área de Recursos Humanos es responsable de:
 - ✓ Colaborar con las demás áreas en la implementación de esta Política y de los procesos relacionados.
 - ✓ Coordinar las capacitaciones internas en materia de protección de datos personales y retención de registros, con respecto a esta Política y su implementación.
 - ✓ Gestionar las sanciones disciplinarias a los empleados como consecuencia del incumplimiento de esta Política.
- El área de Seguridad de la Información es responsable de:
 - ✓ Identificar acciones de mejora para adoptar las medidas de confidencialidad y seguridad para la protección de datos personales.

- ✓ Dirigir las iniciativas de seguridad de la Información o funciones para mejorar la posición de seguridad de la información y proteger la confidencialidad, la integridad y la disponibilidad de los datos electrónicos.
- ✓ Proporcionar coordinación y apoyo para los procesos de respuesta de vulneraciones de seguridad de datos personales, entre ellos la respuesta cibernética, la gestión de vulnerabilidades, la respuesta ante incidentes de seguridad de la información y los recursos forenses.
- Los Data Owners (por área) son responsables de:
 - ✓ Analizar cualquier cambio sobre los objetos y finalidades de los procesos e información bajo su responsabilidad que involucren Datos Personales.
 - ✓ Identificar los períodos de bloqueo que son aplicables para cada categoría de titular de datos personales de los que se realiza el tratamiento de datos personales
 - ✓ Comunicar al Departamento de Cumplimiento y Legal la gestión del Inventario de Datos Personales cualquier inserción, eliminación o cambio de Datos Personales o de sus Finalidades.
 - ✓ Atender acciones correctivas al Inventario de Datos Personales.
 - ✓ Vigilar el cumplimiento de los periodos de conservación y retención de la información a su cargo y ejecutar o solicitar la eliminación de la información según corresponda.
- Los System Owners (por sistema) son responsables de:
 - ✓ Asegurar que los aplicativos cuenten con los mecanismos adecuados para poner en disposición los Avisos de Privacidad correspondientes, así como para recabar el consentimiento expreso de los Titulares, cuando así corresponda.
 - ✓ Asegurar la implementación y ejecución de medidas de protección técnicas y administrativas, cuando corresponda.
 - ✓ Asegurar mecanismos para el cumplimiento de los periodos de conservación y retención aplicables, así como la eliminación correspondiente en los aplicativos bajo su responsabilidad.
- Los empleados son responsables de:
 - ✓ Conocer, comprender y cumplir con los requisitos y el espíritu del presente documento.
 - ✓ Participar y completar con éxito las capacitaciones requeridas en materia de protección de datos personales y retención de registros.
 - ✓ Comprender las consecuencias de no cumplir con los requisitos y el espíritu del presente documento.

- ✓ Guardar confidencialidad en cualquier fase del tratamiento de los datos personales, incluso después de finalizar la relación con el titular.
- ✓ Verificar que los encargados también guarden confidencialidad de los datos personales que tratan a nombre y por cuenta de Emergent Cold MX, aun después de concluida la relación con éste.
- ✓ Al recibir una solicitud para compartir datos de los clientes o información clasificada como confidencial, ya sea a solicitud de otra área o por un tercero, el empleado debe validar que esté autorizado para efectuarla y que esta sea necesaria, por lo que previo a su transferencia debe consultar a el área de Legal a fin de evitar un daño a los clientes, colaboradores y Emergent Cold MX.
- ✓ Proteger la información confidencial de la Compañía, sus empleados, clientes, socios comerciales y otras partes interesadas, durante todo su ciclo de vida, desde que se crean hasta su eliminación segura.
- ✓ Procesar y compartir datos personales solo por motivos específicos, legítimos y necesarios y solo en la medida en que sea necesario.
- ✓ Acceder, utilizar y divulgar información confidencial solo cuando sea necesario y esté autorizado por un propósito legítimo del negocio.
- ✓ Respetar los derechos de privacidad y preferencias de las personas cuyos datos procesamos.
- ✓ Consultar con el área Legal, antes de transferir datos al exterior a otros países (inclusive información de terceros u otras entidades del Grupo Emergent Cold LatAm).
- ✓ Informar de manera oportuna y de buena fe, sobre incumplimientos y/o violaciones en la seguridad de los datos, a través de los canales de gestión adecuados.
- ✓ Cuando se participe en un proyecto estratégico, donde se maneje información confidencial o altamente confidencial, se debe asegurar de consultar al área legal para que validen la necesidad de generar convenios de confidencialidad.
- ✓ Vigilar el cumplimiento de los periodos de conservación y retención de la información a su cargo y ejecutar o solicitar la eliminación de la información según corresponda.
- ✓ Clasificar y resguardar correctamente todos los documentos, bases de datos, contratos, y cualquier otra información que contenga datos personales que recabamos para la operación de la organización.
- ✓ Atender a las acciones necesarias para la protección de datos personales y retención de registros.

5.8.2. Medidas físicas

Emergent Cold MX mantendrá bajo resguardo y acceso restringido todos los archivos que contengan Datos Personales, ya sea bajo llave en caso de expedientes físicos, o bien bajo clave en caso de archivos electrónicos, o mediante cualquier otro tipo de contraseña o sello de confianza que limite el acceso y Tratamiento de estos.

Queda prohibido llevar a cabo el Tratamiento, archivar o crear bases de datos que contengan los Datos Personales, en contravención a esta Política, la LFPDPPP, el Reglamento o cualquier otro ordenamiento aplicable a Emergent Cold MX, por lo que el empleado, personal o funcionario de Emergent Cold MX que contravenga esta política, será responsable de las violaciones, sanciones o delitos establecidos en la Ley, que resultaren aplicables, así como de las que por dicha violación le sean imputables a Emergent Cold MX. Lo anterior, sin perjuicio de las medidas internas que Emergent Cold MX determine tomar como consecuencia.

5.8.3. Inventarios

Emergent Cold MX contará con un registro o inventario de datos personales tratados y de sistemas del tratamiento de datos personales, conforme a las recomendaciones que emita la SABG o, en su defecto, en prácticas internacionales.

5.8.4. Análisis de brechas.

Emergent Cold MX, de tiempo en tiempo, deberá realizar un análisis en el que determine si las medidas establecidas son suficientes para estar en apego a la LFPDPPP, su Reglamento, y a esta política, debiendo, asimismo, estar en constante vigilancia y supervisión del cumplimiento de estas.

ECLA se basará en las guías o recomendaciones que emita la SABG o, en su defecto, en prácticas internacionales, para realizar el análisis de brecha, en el cual se logre diferenciar entre aquellas medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los Datos Personales.

5.8.5. Revisiones y auditorías periódicas.

Emergent Cold MX podrá contratar a un consultor o auditor externo para la realización de auditorías y/o revisiones al programa de Datos Personales de manera periódica (e.g. una vez al año). Como resultado de dichas revisiones y/o auditorías, el consultor o auditor externo entregará a Emergent Cold MX recomendaciones para mejorar el cumplimiento

o para mejorar o adoptar las medidas de seguridad aplicables para la protección de datos personales.

Los resultados de las revisiones y/o auditorías serán informadas por el Departamento de Cumplimiento y Legal a todos y cada uno de los empleados, funcionarios y/o directivos de Emergent Cold MX involucrados en el tratamiento de Datos Personales.

Asimismo, el equipo de Compliance revisará el contenido de esta Política, de manera periódica, así como de los demás documentos que forman parte del programa de cumplimiento con la Regulación de Datos Personales, con la finalidad de identificar la necesidad de realizar modificaciones. Esta Política también deberá ser revisada y actualizada, en caso de que se reforme alguna ley, lineamiento, reglamento o disposiciones relacionadas con el Tratamiento que le resulte aplicable.

5.8.6. Capacitaciones en temas de tratamiento de datos personales.

ECLA ha implementado un programa de capacitación anual. Todos los empleados, directivos y/o funcionarios de Emergent Cold MX que se encuentren involucrados en el Tratamiento, deberán asistir de forma obligatoria a dichas capacitaciones.

La persona o personas que determine ECLA como miembros del Departamento de Cumplimiento y Legal, para el buen desempeño de sus actividades deberán contar con la capacitación necesaria para tratar los Datos Personales recabados, por lo que además de apegarse a esta política, de tiempo en tiempo deberán tomar capacitaciones, ya sea que estas sean brindadas directamente por Emergent Cold MX o sean capacitaciones que la SABG ponga a disposición del público en general. Por otro lado, para cumplir con las obligaciones normativas, relativas a la tramitación de las solicitudes de los titulares, para el ejercicio de los Derechos ARCO, así como para fomentar la protección de datos personales al interior de la Organización, se podrá contratar a un prestador de servicios externo para asistencia con las obligaciones relacionadas las tareas de capacitación y entrenamientos.

5.9. PROCEDIMIENTO EN CASO DE VULNERACIONES DE SEGURIDAD

En caso de que ECLA se vea expuesto a una vulneración de seguridad de datos personales, llevará a cabo el siguiente procedimiento:

Deberá informar a los Titulares las vulneraciones de seguridad que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto confirme que ocurrió la vulneración y haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, y sin dilación alguna, a fin de que los Titulares

afectados puedan tomar las medidas correspondientes. Dicha notificación deberá incluir la siguiente información:

- La naturaleza del incidente;
- Los Datos Personales comprometidos;
- Las recomendaciones al Titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
- Las acciones correctivas realizadas de forma inmediata, y
- Los medios donde puede obtener más información al respecto.

Por lo anterior, es obligación de la Compañía notificar de forma inmediata al departamento jurídico y al Departamento de Compliance Regional en caso de ocurrir alguna de las siguientes vulneraciones a los Datos Personales, en cualquier fase de su Tratamiento:

- La pérdida o destrucción no autorizada;
- El robo, extravío o copia no autorizada;
- El uso, acceso o Tratamiento no autorizado, o
- El daño, la alteración o modificación no autorizada.

En caso de que la vulneración de seguridad tenga como resultado la afectación significativa de los derechos patrimoniales y/o morales de los Titulares, el equipo de Cumplimiento y Legal deberán tomar las acciones que correspondan, pudiendo este último apoyarse de cualesquiera de las áreas de Emergent Cold MX que considere pertinentes o, bien, de consultores externos.

El equipo Legal local deberá evaluar los reportes que reciba de cualquier área o departamento jurídico para confirmar si este requiere ser informado a los titulares, y será quien tome la decisión de notificar o no al Titular sobre la presencia de una vulneración de seguridad. Dicha notificación únicamente se realizará en caso de que el equipo lo considere estrictamente necesario.

El Departamento de Cumplimiento y legal local también podrá solicitarle a otro funcionario o empleado de Emergent Cold MX su apoyo para realizar la notificación correspondiente. Los empleados, directivos y/o funcionarios de Emergent Cold MX en ningún momento podrán notificar al Titular la presencia de una vulneración de seguridad, sin que dicha notificación haya sido previamente autorizada e instruida.

5.10. CONFIDENCIALIDAD

Emergent Cold MX ha adoptado convenios de confidencialidad para evitar la divulgación no autorizada de Datos Personales con sus empleados, proveedores o terceros

relacionados y ha establecido que estas obligaciones subsisten aun después de la relación contractual.

El Tratamiento conlleva implícita la obligación de guardar como confidencial la información recibida o que en virtud de su trabajo puedan conocer, obligación que subsistirá incluso al terminar la relación existente con el Titular o con Emergent Cold MX. Todas las áreas de Emergent Cold MX, incluyendo empleados, personal y funcionarios deberán guardar estricta confidencialidad de los Datos Personales a los que tengan acceso en virtud de su labor diaria, por lo que queda estrictamente prohibido revelar dicha información a terceros no autorizados.

5.11. BLOQUEO, CONSERVACIÓN Y SUPRESIÓN

5.11.1. Bloqueo:

De resultar procedente la Cancelación el Departamento de Cumplimiento y legal deberá:

- I. Establecer un periodo de Bloqueo con el único propósito de determinar posibles responsabilidades en relación con su Tratamiento hasta el plazo de prescripción legal o contractual y notificarlo al Titular o a su representante en la respuesta a la Solicitud ARCO;
- II. Atender las Medidas de Seguridad adecuadas para el Bloqueo;
- III. Llevar a cabo el bloqueo en el plazo de 15 días hábiles;
- IV. Transcurrido el periodo de Bloqueo, llevar a cabo la supresión correspondiente.

La entrega de los Datos Personales será gratuita y el Titular sólo debe cubrir los gastos justificados de envío o el costo de reproducción en copias u otros formatos. Si la misma persona reitera su Solicitud ARCO en un periodo menor a 1 año, deberá cubrir los costos correspondientes, que no deben ser mayores a 3 días de Salario Mínimo General Vigente en la Ciudad de México, salvo que hayan existido cambios sustanciales al Aviso de Privacidad.

5.11.2. Conservación:

Períodos de conservación: Los líderes de áreas en conjunto con el Equipo Legal Local deben identificar los periodos de bloqueo que son aplicables para cada categoría de titular de datos personales de los que se realiza el tratamiento de datos personales, de conformidad con la normatividad que rige el tratamiento de que se trate y conforme al

cuadro de plazos de Conservación que se inserta para fines ejemplificativos y no limitativos.

Regulación aplicable	Periodo de Retención (Legal)	Tipo de Registro	Tipo de documentos	Ejemplo
Código de Comercio	Mínimo 120 meses (10 años)	Todo tipo de registro que refleje la operación de la compañía	Expediente físico, electrónico, datos en los sistemas.	Información de siniestros, objetivos de los empleados, actas de Comités, contratos con proveedores
Ley Federal de Protección al Consumidor	Mínimo 1 año	Registros que contengan información con identificación de clientes. Grabaciones de operaciones voz a voz o atención al cliente.	Expediente físico, electrónico, datos en los sistemas. Grabaciones	Información y documentación relativas a la identificación de clientes. Grabaciones de llamadas al <i>Call Center</i>
NOM-004-SSA3-2012 (Expediente Clínico)	Mínimo 5 años, contados a partir de la fecha del último acto médico registrado en el expediente	Todo tipo de registro que Refleje información de pacientes	Expediente físico, electrónico, datos en los sistemas.	Expediente de pacientes.
Ley Federal de Protección de Datos Personales en Posesión de los Particulares	72 meses (6 años, contados a partir del incumplimiento o de la obligación contractual)	Obligaciones contractuales incumplidas	Expediente físico, electrónico, datos en los sistemas relativos a incumplimientos de Obligaciones contractuales.	Contratos con obligaciones incumplidas
Ley Federal del Trabajo	Mínimo 1 año para la mayoría de las acciones; 2 meses si deriva de despido.	Todo tipo de registro que Refleje información de empleados	Expediente físico, electrónico, datos en los sistemas.	Expediente del empleado.

Ley del Seguro Social	Mínimo 5 años para el cumplimiento de obligaciones de seguridad social	Todo tipo de registro que refleje información de seguridad social de los empleados	Expediente físico, electrónico, datos en los sistemas.	Expediente del empleado.
Código Fiscal de la Federación	Mínimo 5 años para el cumplimiento de obligaciones fiscales.	Todo tipo de registro que refleje el cumplimiento de obligaciones fiscales.	Expediente físico, electrónico, datos en los sistemas.	Facturas, Constancias Fiscales

Una vez identificada la normatividad aplicable deberá definirse el período de bloqueo atendiendo a dichas disposiciones normativas y las siguientes variables: (i) Período(s) de bloqueo aplicable(s), considerando en primer lugar el más amplio; (ii) Tipo de información sometida a tratamiento, y (iii) Tiempo que puede ser almacenada la información por la regla técnica de almacenamiento, solo cuándo esta es menor a la establecida por la norma.

- Ejemplo:

Período: 5 años contados a partir de que el titular deja de ser empleado y se han ejecutado todas las obligaciones obrero-patronales pendientes.

Una vez que se concluye el tratamiento de los datos personales conforme al Aviso de Privacidad que lo sustente, o bien, una vez que se declare la procedencia de un ejercicio del Derecho de Cancelación, los datos serán bloqueados por lo que no podrá realizarse ningún otro tratamiento, más que su almacenamiento.

En caso de que los activos de almacenamiento sean físicos, cada líder de área definirá si el almacenamiento se realiza en las áreas físicas que le han sido asignadas, o bien, si los envía al área de Archivo Muerto.

En caso de enviarlo a Archivo Muerto, seguirá siendo responsabilidad del líder del área de que se trate la de controlar su almacenamiento, por lo que deberá identificar los activos en esta situación, a efecto de que, al concluir el período de bloqueo, será dicho líder el que debe iniciar las acciones de supresión correspondientes.

En caso de que los datos personales consten en activos digitales, será el equipo de Sistemas o TI la que defina las acciones para el bloqueo y supresión de datos personales que constan en activos de almacenamiento físicos o técnicos.

5.11.3. Supresión:

Los Registros que contenga datos personales que han llegado al final del período de conservación aplicable y no están sujetos a un plazo de conservación/retención legal, se eliminan de acuerdo con el Cuadro de plazos de conservación.

Para la eliminación de registros deberá consultarse al área Legal a través de una solicitud formal llenando el "Acta de Destrucción de Registros e Información" en la que se detallará la información general del área responsable, el tipo o medio de destrucción, la clasificación de la información, el proveedor contratado para la destrucción de la información, el tipo de registro, la fecha de generación y periodo de retención, la justificación de la información así como la firma del personal autorizado.

La eliminación de los registros debe considerar los siguientes aspectos:

- Irreversibilidad. Se debe garantizar que no existe un proceso que permita recuperar la información.
- Seguridad y confidencialidad. Los medios de almacenamiento se deben tratar durante el borrado con la misma seguridad con que se han mantenido durante su existencia.
- Favorable al medio ambiente. El método reduce el impacto ecológico.

5.12. SANCIONES INTERNAS

El incumplimiento a esta Política se considerará como un incumplimiento a las obligaciones de la relación contractual celebrada con algún proveedor o de la relación laboral que corresponda y el empleado se hará acreedor de las medidas de apercibimiento y disciplinarias que correspondan.

Aunado a lo anteriormente señalado, aquellos que incumplan con lo establecido en esta Política serán acreedores a las sanciones que establezcan las leyes y demás disposiciones legales aplicables, incluyendo el pago de los daños y perjuicios que se causen a Emergent Cold LatAm y a las empresas pertenecientes al Grupo en México, derivado de su incumplimiento.

5.13. VIGENCIA Y CAMBIOS EN LA POLITICA

Esta Política entrará en vigor en la fecha de su aprobación por el Consejo de Administración y tendrá una vigencia indefinida, pero deberá revisarse, cuando menos, cada 3 (tres) años.

La Compañía puede cambiar esta Política en cualquier momento, sin comunicación previa al Titular. Por otro lado, Emergent Cold MX no podrá cambiar esta política sin notificar al Titular:

- Las finalidades del Tratamiento de sus Datos Personales;
- La forma y la duración del tratamiento de los Datos Personales;
- La identidad del Responsable;
- Las condiciones para la Transferencia de los Datos Personales.

En caso de duda, quejas o sugerencia relacionadas con la protección de datos personales o que involucren esta Política, por favor póngase en contacto con el Equipo Legal Local o el equipo de Cumplimiento Regional o puede contactarnos por el siguiente correo electrónico: datospersonales@emergentcold.com