POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO

Emergent Cold LatAm, en adelante **"Emergent Cold", "ECLA"** o la **"Compañía"**, es la mayor organización de soluciones logísticas a temperatura controlada para alimentos en América Latina. En el desarrollo de sus actividades operativas, comerciales, financieras y administrativas, la Compañía trata información estratégica, operativa y, en determinados casos, datos personales de colaboradores, clientes, proveedores y otros grupos de interés.

Establecer los principios, lineamientos y medidas generales que orientan la protección de la información administrada por **Emergent Cold LatAm**, asegurando su **confidencialidad, integridad, disponibilidad y trazabilidad**, así como la gestión adecuada de los riesgos asociados al acceso, uso, divulgación o modificación no autorizada de la información, ya sea tratada en sistemas propios o a través de terceros.

Esta Política constituye un componente esencial del **marco regional de cumplimiento y gestión de riesgos**, y se integra con lineamientos corporativos en materia de protección de datos personales, seguridad de la información, continuidad operativa, gestión de incidentes y ciberseguridad. Su finalidad es promover un enfoque uniforme y consistente en todas las operaciones de la región, fortaleciendo la cultura organizacional orientada a la protección de los activos de información y al cumplimiento de las obligaciones legales aplicables en cada país.

Asimismo, esta Política sirve como guía para el diseño, implementación y mejora continua de los controles de seguridad, procedimientos internos y prácticas tecnológicas que permitan resguardar los activos de información de la Compañía durante todo su ciclo de vida y garantizar el funcionamiento seguro, confiable y eficiente de sus operaciones en los países donde opera.

2. ALCANCE

Estos lineamientos tienen una aplicabilidad para:

a. Toda la información tratada por **ECLA**, con independencia de su soporte (físico, digital o mixto), su localización o el medio a través del cual se procese o comunique.

b. Todos los sistemas, aplicaciones, redes, infraestructuras y servicios tecnológicos utilizados por la Compañía, propios o de terceros (incluyendo servicios en la nube y soluciones SaaS).
c. Todos los directores, gerentes, trabajadores, colaboradores, consultores y terceros que, por cualquier título, accedan o traten información de **Emergent Cold LatAm**.
d. Todos los proveedores de servicios que, directa o indirectamente, traten información de la Compañía.

3. MARCO NORMATIVO

Esta Política de Seguridad de la Información se dicta en coherencia con la legislación vigente en cada uno de los países donde **ECLA** desarrolla sus operaciones, y con los principios corporativos que rigen la protección de activos de información, la gestión de riesgos y el cumplimiento normativo a nivel regional. Su propósito es establecer un marco común que permita resguardar la confidencialidad, integridad y disponibilidad de la información, asegurando prácticas homogéneas y consistentes en toda la organización.

Asimismo, la Compañía adopta **estándares y buenas prácticas internacionalmente reconocidas en materia de seguridad de la información**, ajustándolas a las características operativas de sus instalaciones, sistemas y procesos. Estos estándares guían el diseño e implementación de controles técnicos y organizativos, así como los procesos de gestión de incidentes, monitoreo, capacitación, concientización y mejora continua.

La presente Política constituye un pilar fundamental del **Programa Corporativo de Cumplimiento y Gestión de Riesgos,** integrándose con las políticas, procedimientos y lineamientos regionales que rigen la protección de datos personales, la ciberseguridad, el gobierno de TI y el resguardo de activos críticos de la Compañía

Esta Política se sustenta, entre otros, en:

a. La legislación vigente en materia de seguridad de la información, ciberseguridad y protección de datos personales aplicable en cada uno de los países donde opera Emergent Cold LatAm, incluyendo normas generales, sectoriales y regulatorias relacionadas con la gestión y resguardo de activos de información.

b. Las obligaciones regulatorias específicas que resulten aplicables a la Compañía según su actividad comercial y operativa, en áreas como seguridad de la información, continuidad operativa, servicios tecnológicos, trazabilidad logística, prevención de fraudes, seguridad física y digital, así como cualquier regulación emitida por autoridades competentes en los países donde Emergent Cold LATAM desarrolla sus operaciones.
c. Las buenas prácticas, lineamientos y estándares internacionales reconocidos en materia de seguridad de la información y ciberseguridad.
d. Procesos, procedimientos y lineamientos corporativos de Emergent Cold LATAM, que conforman el marco regional de cumplimiento, gestión de riesgos y protección de la información, así como los documentos internos que regulan la seguridad tecnológica, el tratamiento de datos personales, la gestión de incidentes, la continuidad del negocio y cualquier otro instrumento normativo que complemente esta Política.

4. PRINCIPIOS RECTORES

La seguridad de la información en **Emergent Cold LatAm** se rige, al menos, por los siguientes principios:

a. **Confidencialidad**: la información se accede y comunica únicamente por personas autorizadas y para finalidades específicas y legítimas.
b. **Integridad**: la información debe ser exacta, completa y estar protegida contra alteraciones no autorizadas.
c. **Disponibilidad**: la información y los sistemas deben estar disponibles cuando sean necesarios para la operación, prestación de servicios y ejercicio de derechos por parte de los titulares.
d. **Proporcionalidad**: las medidas de seguridad se ajustarán a la naturaleza de la información, al contexto del tratamiento y al nivel de riesgo.
e. **Prevención y enfoque basado en riesgos**: se prioriza la adopción de medidas que permitan prevenir incidentes.
f. **Responsabilidad proactiva**: la Compañía velará por tener los medios que permitan acreditar, mediante documentación y evidencias, la implementación efectiva de controles de seguridad.
g. **Seguridad por diseño y por defecto**: los sistemas, procesos y proyectos que involucren datos personales o información crítica deberán considerar la seguridad desde su diseño, configuración inicial y parámetros por defecto.

5. MEDIDAS DE SEGURIDAD INTERNAS

Emergent Cold LatAm implementa medidas de seguridad internas que combinan controles organizativos, técnicos y físicos, acordes con la naturaleza de la información tratada y con el nivel de riesgo identificado. A nivel general, estas medidas incluyen, al menos, los siguientes ámbitos:

a. **Controles de red y perímetro**: Mecanismos de protección perimetral y segmentación de redes para prevenir accesos no autorizados, detectar actividades anómalas y limitar el alcance de eventuales incidentes.
b. **Protección de equipos y comunicaciones, propios y de terceros**: Soluciones y procedimientos orientados a proteger los dispositivos corporativos, el correo electrónico y otros canales de comunicación frente a malware, phishing y amenazas similares.
c. **Gestión de identidades y accesos**: Procedimientos y herramientas de gestión de usuarios, roles y permisos, bajo el principio de privilegios mínimos necesarios, incluyendo autenticación robusta (por ejemplo, multifactor) para el acceso a sistemas y aplicaciones críticas, políticas de contraseñas y registro de actividades de cuentas con privilegios elevados.
d. **Monitoreo, detección y respuesta ante incidentes**: Servicios y capacidades de monitoreo continuo de los eventos de seguridad relevantes, con correlación de logs, detección de patrones de riesgo y procedimientos de respuesta y escalamiento frente a incidentes de seguridad de la información.
e. **Pruebas, y mejora continua**: Ejecución periódica de pruebas de seguridad (incluyendo, cuando corresponda, pruebas de penetración y análisis de vulnerabilidades), así como auditorías internas o externas sobre los controles implementados, con registro de hallazgos, planes de acción y seguimiento de su cumplimiento.
f. **Respaldo, continuidad y recuperación**: Mecanismos de copia de seguridad periódica de la información y planes de continuidad y recuperación ante desastres, destinados a asegurar la restauración oportuna de los sistemas y datos críticos frente a incidentes que afecten la disponibilidad.

Estas medidas se revisarán y actualizarán en función de la evolución tecnológica, de los resultados de las evaluaciones de riesgo y de los cambios regulatorios o de negocio que resulten aplicables, pudiendo complementarse con procedimientos y anexos técnicos específicos de carácter restringido.

6. MEDIDAS DE SEGURIDAD APLICABLES A PROVEEDORES

Emergent Cold exigirá a sus proveedores de software, servicios tecnológicos, soluciones en la nube y, en general, a cualquier tercero que trate información de la Compañía, estándares de seguridad coherentes con el nivel de riesgo y con la sensibilidad de los datos involucrados. A nivel general, se considerarán, entre otros, los siguientes ámbitos:

a. **Gestión de la confidencialidad e integridad de la información**: Adopción de medidas técnicas y organizativas adecuadas para proteger la información frente a accesos, usos, alteraciones o divulgaciones no autorizadas, incluyendo por ejemplo el uso de mecanismos de cifrado y controles de acceso acordes a buenas prácticas de la industria.
b. **Controles de seguridad sobre infraestructuras y servicios críticos**: Implementación de controles de protección en redes, servidores, aplicaciones y dispositivos utilizados para la prestación de los servicios, en línea con estándares de referencia y con el nivel de criticidad de las operaciones que soportan.
c. **Continuidad del servicio y recuperación ante desastres**: Existencia de procedimientos documentados de continuidad operativa y recuperación ante incidentes graves, que permitan restablecer los servicios dentro de plazos razonables y acordes con los compromisos contractuales asumidos.
d. **Compromisos contractuales de seguridad y protección de datos personales**: Inclusión en los contratos de cláusulas específicas en materia de seguridad de la información, protección de datos personales, confidencialidad, notificación oportuna de incidentes y facultades de auditoría o verificación por parte de **Emergent Cold LatAm**, cuando corresponda.
e. **Integraciones y accesos seguros entre sistemas**: Implantación de mecanismos de autenticación, autorización y registro de accesos adecuados para las interconexiones entre sistemas de los terceros relacionados y de **Emergent Cold LatAm**, así como para el acceso remoto a la infraestructura o a los datos de la Compañía.

La selección, contratación y evaluación periódica de proveedores tecnológicos considerará desde el inicio criterios de seguridad de la información y protección de datos personales, de acuerdo con el enfoque de seguridad por diseño y por defecto y con la política de gestión de proveedores de **Emergent Cold LatAm**.

7. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La detección, reporte, análisis, contención, notificación y remediación de incidentes de seguridad de la información se regirá por la Política de Gestión de Incidentes de

Vulneración de Datos Personales, los Lineamientos locales de Seguridad de la información y los procedimientos que la desarrollan, sin perjuicio de las obligaciones sectoriales o contractuales que resulten aplicables.

Todo trabajador, colaborador o proveedor que detecte o sospeche una vulneración de seguridad deberá reportarla de inmediato a través de los canales definidos, absteniéndose de borrar evidencias salvo que su conservación comprometa aún más la seguridad.

8. FORMACIÓN Y CONCIENTIZACIÓN

Emergent Cold LatAm promoverá programas periódicos de formación y concientización en materia de **seguridad de la información** y **protección de datos personales**, dirigidos a todos los colaboradores, que hagan uso de los sistemas o manejen información de la Compañía. Estos programas tendrán como objetivo fortalecer la cultura organizacional de seguridad a nivel regional y en cada uno de los países donde ECLA tiene operaciones. Los contenidos formativos se enfocarán, entre otros, en:

a. **Identificación y prevención de amenazas comunes**, incluidas prácticas de phishing, ingeniería social, malware y otros riesgos habituales.
b. **Buenas prácticas en el uso seguro de contraseñas**, dispositivos, plataformas digitales, canales de comunicación y herramientas tecnológicas.
c. **Procedimientos internos para la notificación y gestión de incidentes**, así como el rol de cada persona dentro del proceso.
d. **Obligaciones de confidencialidad y protección de datos personales**, y el uso adecuado de la información durante todo su ciclo de vida.

La participación en estas actividades podrá ser obligatoria según la función, nivel de acceso a la información o requerimientos normativos aplicables en cada país de la región.

9. INTEGRACIÓN CON EL PROGRAMA DE CUMPLIMIENTO CORPORATIVO.

Esta Política forma parte del **Marco Regional de Cumplimiento y Gestión de Riesgos de Emergent Cold LatAm**, y se integra con las políticas, lineamientos y procedimientos corporativos relacionados con la protección de datos personales, la ciberseguridad, la continuidad del negocio, la gestión de incidentes y otros componentes del sistema de control interno de la Compañía.

El cumplimiento de esta Política será considerado en los procesos de **identificación, evaluación y mitigación de riesgos**, así como en los mecanismos internos de seguimiento y auditoría que la Compañía implemente a nivel regional y local. El incumplimiento de las disposiciones aquí establecidas podrá dar lugar a la aplicación de medidas correctivas, contractuales o disciplinarias conforme a la normativa interna y a la legislación vigente en cada jurisdicción.

Cualquier actualización de esta Política será comunicada oportunamente a las áreas responsables y se reflejará en los procedimientos y lineamientos complementarios que integran el sistema regional de seguridad de la información.

10. VIGENCIA Y REVISIÓN

La presente política entra en vigor desde su aprobación por el Directorio de **Emergent Cold LatAm,** y será revisada, al menos, cada dos años o cuando se produzcan cambios normativos, tecnológicos u organizacionales que lo justifiquen. Las actualizaciones deberán comunicarse a las áreas responsables.