POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

Emergent Cold LATAM, doravante **"ECLA"** ou a **"Companhia"**, é a maior organização de soluções logísticas com temperatura controlada para alimentos na América Latina. No desenvolvimento de suas atividades operacionais, comerciais, financeiras e administrativas, a Companhia trata informações estratégicas, operacionais e, em determinados casos, dados pessoais de colaboradores, clientes, fornecedores e outros grupos de interesse

Estabelecer os princípios, diretrizes e medidas gerais que orientam a proteção das informações administradas pela **Emergent Cold LATAM**, assegurando sua **confidencialidade, integridade, disponibilidade e rastreabilidade,** bem como a adequada gestão dos riscos associados ao acesso, uso, divulgação ou modificação não autorizada das informações, seja em sistemas próprios ou por meio de terceiros.

Esta Política constitui um componente essencial do **marco regional de conformidade e gestão de riscos** e integra-se às diretrizes corporativas em matéria de proteção de dados pessoais, segurança da informação, continuidade operacional, gestão de incidentes e cibersegurança. Sua finalidade é promover uma abordagem uniforme e consistente em todas as operações da região, fortalecendo a cultura organizacional voltada à proteção dos ativos de informação e ao cumprimento das obrigações legais aplicáveis em cada país.

Da mesma forma, esta Política serve como guia para o desenho, implementação e melhoria contínua dos controles de segurança, procedimentos internos e práticas tecnológicas que permitam proteger os ativos de informação da Companhia durante todo o seu ciclo de vida e garantir o funcionamento seguro, confiável e eficiente de suas operações nos países onde atua.

I. ALCANCE

Estas diretrizes aplicam-se a:

a. Toda a informação tratada pela **Emergent Cold LatAm**, independentemente de seu suporte (físico, digital ou misto), sua localização ou o meio pelo qual seja processada ou comunicada.

b. Todos os sistemas, aplicações, redes, infraestruturas e serviços tecnológicos utilizados pela Companhia, próprios ou de terceiros (incluindo serviços em nuvem e soluções SaaS).
c. Todos os diretores, gerentes, trabalhadores, colaboradores, consultores e terceiros que, por qualquer título, acessem ou tratem informações.
d. Todos os fornecedores de serviços que, direta ou indiretamente, tratem informações da Companhia.

II. MARCO NORMATIVO

Esta Política de Segurança da Informação é estabelecida em conformidade com a legislação vigente em cada um dos países onde a **ECLA** desenvolve suas operações, bem como com os princípios corporativos que regem a proteção de ativos de informação, a gestão de riscos e a conformidade regulatória em nível regional. Seu propósito é estabelecer um marco comum que permita resguardar a confidencialidade, integridade e disponibilidade das informações, assegurando práticas homogêneas e consistentes em toda a organização.

Da mesma forma, a Companhia adota **padrões e boas práticas internacionalmente reconhecidas em matéria de segurança da informação**, ajustando-os às características operacionais de suas instalações, sistemas e processos. Esses padrões orientam o desenho e a implementação de controles técnicos e organizacionais, bem como os processos de gestão de incidentes, monitoramento, capacitação, conscientização e melhoria contínua.

A presente Política constitui um pilar fundamental do **Programa Corporativo de Conformidade e Gestão de Riscos**, integrando-se às políticas, procedimentos e diretrizes regionais que regem a proteção de dados pessoais, a cibersegurança, a governança de TI e a proteção de ativos críticos da Companhia.

Esta Política baseia-se, entre outros, em:

a. A legislação vigente em matéria de segurança da informação, cibersegurança e proteção de dados pessoais aplicável em cada um dos países onde opera a Emergent Cold LatAm, incluindo normas gerais, setoriais e regulatórias relacionadas à gestão e proteção de ativos de informação.
b. As obrigações regulatórias específicas aplicáveis à Companhia de acordo com sua atividade comercial e operacional, em áreas como segurança da informação, continuidade operacional, serviços tecnológicos, rastreabilidade logística,

prevenção de fraudes, segurança física e digital, bem como qualquer regulamentação emitida por autoridades competentes nos países onde a Emergent Cold LatAm desenvolve suas operações.

c. As boas práticas, diretrizes e padrões internacionais reconhecidos em matéria de segurança da informação e cibersegurança.
d. Processos, procedimentos e diretrizes corporativas da Emergent Cold LATAM, que compõem o marco regional de conformidade, gestão de riscos e proteção da informação, bem como os documentos internos que regulam a segurança tecnológica, o tratamento de dados pessoais, a gestão de incidentes, a continuidade do negócio e qualquer outro instrumento normativo que complemente esta Política.

III. PRINCÍPIOS NORTEADORES

A segurança da informação na Emergent Cold rege-se, no mínimo, pelos seguintes princípios:

a. **Confidencialidade:** a informação é acessada e comunicada apenas por pessoas autorizadas e para finalidades específicas e legítimas.
b. **Integridade:** a informação deve ser exata, completa e protegida contra alterações não autorizadas.
c. **Disponibilidade:** a informação e os sistemas devem estar disponíveis quando necessários para a operação, prestação de serviços e exercício de direitos por parte dos titulares.
d. **Proporcionalidade:** as medidas de segurança serão ajustadas à natureza da informação, ao contexto do tratamento e ao nível de risco.
e. **Prevenção e abordagem baseada em riscos:** prioriza-se a adoção de medidas que permitam prevenir incidentes.
f. **Responsabilidade proativa:** a Companhia garantirá possuir meios que permitam demonstrar, por meio de documentação e evidências, a implementação efetiva de controles de segurança.
g. **Segurança desde a concepção e por padrão:** os sistemas, processos e projetos que envolvam dados pessoais ou informações críticas deverão considerar a segurança desde seu desenho, configuração inicial e parâmetros padrão.

IV. MEDIDAS DE SEGURANÇA INTERNAS

A Emergent Cold implementa medidas de segurança internas que combinam controles organizacionais, técnicos e físicos, de acordo com a natureza das informações tratadas e

com o nível de risco identificado. De forma geral, essas medidas incluem, ao menos, os seguintes aspectos:

a. **Controles de rede e perímetro:** mecanismos de proteção perimetral e segmentação de redes para prevenir acessos não autorizados, detectar atividades anômalas e limitar o alcance de eventuais incidentes.
b. **Proteção de equipamentos e comunicações, próprios e de terceiros:** soluções e procedimentos destinados a proteger dispositivos corporativos, e-mail e outros canais de comunicação contra malware, phishing e ameaças semelhantes.
c. **Gestão de identidades e acessos:** procedimentos e ferramentas para gestão de usuários, funções e permissões, sob o princípio do menor privilégio necessário, incluindo autenticação robusta (por exemplo, multifator) para acesso a sistemas e aplicações críticas, políticas de senhas e registro de atividades de contas com privilégios elevados.
d. **Monitoramento, detecção e resposta a incidentes:** serviços e capacidades de monitoramento contínuo de eventos relevantes de segurança, com correlação de logs, detecção de padrões de risco e procedimentos de resposta e escalonamento diante de incidentes de segurança da informação.
e. **Testes, auditoria e melhoria contínua**: realização periódica de testes de segurança (incluindo, quando aplicável, testes de penetração e análises de vulnerabilidades), bem como auditorias internas ou externas sobre os controles implementados, com registro de achados, planos de ação e acompanhamento de sua execução.
f. **Backup, continuidade e recuperação**: mecanismos de cópia de segurança periódica das informações e planos de continuidade e recuperação de desastres, destinados a assegurar a restauração oportuna de sistemas e dados críticos diante de incidentes que afetem a disponibilidade.

Essas medidas serão revisadas e atualizadas conforme a evolução tecnológica, os resultados das avaliações de risco e mudanças regulatórias ou de negócios aplicáveis, podendo ser complementadas por procedimentos e anexos técnicos específicos de caráter restrito.

V. MEDIDAS DE SEGURANÇA APLICÁVEIS A FORNECEDORES

Emergent Cold LatAm exigirá de seus fornecedores de software, serviços tecnológicos, soluções em nuvem e, em geral, de qualquer terceiro que trate informações da Companhia, padrões de segurança coerentes com o nível de risco e com a sensibilidade dos dados envolvidos:

a. **Gestão da confidencialidade e integridade da informação**: Adoção de medidas técnicas e organizacionais adequadas para proteger a informação contra acessos, usos, alterações ou divulgações não autorizadas, incluindo, por exemplo, o uso de mecanismos de criptografia e controles de acesso alinhados às boas práticas da indústria.
b. **Testes e avaliações de segurança**: Realização periódica de testes e revisões de segurança sobre os sistemas e serviços oferecidos, bem como a disponibilização de evidências ou relatórios que permitam à **Emergent Cold** conhecer, quando aplicável, o estado geral da segurança do fornecedor.
c. **Controles de segurança sobre infraestruturas e serviços críticos**: Implementação de controles de proteção em redes, servidores, aplicações e dispositivos utilizados para a prestação dos serviços, em conformidade com padrões de referência e com o nível de criticidade das operações que suportam.
d. **Continuidade do serviço e recuperação de desastres**: Existência de procedimentos documentados de continuidade operacional e recuperação diante de incidentes graves, que permitam restabelecer os serviços dentro de prazos razoáveis e compatíveis com os compromissos contratuais assumidos.
e. **Compromissos contratuais de segurança e proteção de dados pessoais**: Inclusão, nos contratos, de cláusulas específicas relacionadas à segurança da informação, proteção de dados pessoais, confidencialidade, notificação oportuna de incidentes e facultando à **Emergent Cold** o direito de auditoria ou verificação, quando aplicável.
f. **Integrações e acessos seguros entre sistemas**: Implementação de mecanismos adequados de autenticação, autorização e registro de acessos para as interconexões entre os sistemas do fornecedor e os da **Emergent Cold LatAm**, bem como para o acesso remoto à infraestrutura ou aos dados da Companhia.

A seleção, contratação e avaliação periódica de fornecedores tecnológicos considerarão, desde o início, critérios de segurança da informação e proteção de dados pessoais, de acordo com a abordagem de segurança desde a concepção e por padrão, bem como com a política de gestão de fornecedores da **Emergent Cold LatAm**.

VI. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

A detecção, o reporte, a análise, a contenção, a notificação e a remediação de incidentes de segurança da informação serão regidos pela Política de Gestão de Incidentes de Violação de Dados Pessoais, pelas Diretrizes locais de Segurança da Informação e pelos

procedimentos que as desenvolvem, sem prejuízo das obrigações setoriais ou contratuais aplicáveis.
Todo trabalhador, colaborador ou fornecedor que detecte ou suspeite de uma violação de segurança deverá reportá-la imediatamente por meio dos canais definidos, abstendo-se de apagar evidências, salvo se sua preservação comprometer ainda mais a segurança.

VII. FORMAÇÃO E CONSCIENTIZAÇÃO

A ECLA promoverá programas periódicos de formação e conscientização em matéria de segurança da informação e proteção de dados pessoais, destinados a todos os colaboradores, contratados e terceiros que utilizem os sistemas ou manuseiem informações da Companhia. Esses programas terão como objetivo fortalecer a cultura organizacional de segurança em nível regional e em cada um dos países onde a ECLA possui operações. Os conteúdos formativos abordarão, entre outros, os seguintes temas:

a. **Identificação e prevenção de ameaças comuns** incluindo práticas de phishing, engenharia social, malware e outros riscos recorrentes.
b. **Boas práticas no uso seguro de senhas**, dispositivos, plataformas digitais, canais de comunicação e ferramentas tecnológicas.
c. **Procedimentos internos para notificação e gestão de incidentes**, bem como o papel de cada pessoa dentro desse processo.
d. **Obrigações de confidencialidade e proteção de dados pessoais**, além do uso adequado das informações ao longo de todo o seu ciclo de vida.

A participação nessas atividades poderá ser obrigatória de acordo com a função, o nível de acesso à informação ou requisitos normativos aplicáveis em cada país da região.

VIII. INTEGRAÇÃO COM O MARCO REGIONAL DE CONFORMIDADE.

Esta Política faz parte do **Marco Regional de Conformidade e Gestão de Riscos da Emergent Cold LatAm** e integra-se às políticas, diretrizes e procedimentos corporativos relacionados à proteção de dados pessoais, cibersegurança, continuidade de negócios, gestão de incidentes e a outros componentes do sistema de controle interno da Companhia.

O cumprimento desta Política será considerado nos processos de **identificação, avaliação e mitigação de riscos**, bem como nos mecanismos internos de acompanhamento e auditoria que a Companhia implemente em nível regional e local. O descumprimento das disposições aqui estabelecidas poderá resultar na aplicação de

medidas corretivas, contratuais ou disciplinares, conforme a normativa interna da **Emergent Cold LatAm** e a legislação vigente em cada jurisdição.
Qualquer atualização desta Política será comunicada oportunamente às áreas responsáveis e será refletida nos procedimentos e diretrizes complementares que integram o sistema regional de segurança da informação.

IX. VIGÊNCIA E REVISÃO

A presente política entra em vigor a partir de sua aprovação pelo Diretório (Diretoria/Conselho de Administração) da **Emergent Cold LatAm**, e será revisada, no mínimo, a cada dois anos ou sempre que ocorrerem mudanças normativas, tecnológicas ou organizacionais que o justifiquem. As atualizações deverão ser comunicadas às áreas responsáveis.