

POLÍTICA DE GOVERNANÇA DE DADOS

1. OBJETIVO

A presente Política de Governança de Dados ("Política") tem por objetivo estabelecer o marco regional que orienta a gestão, uso, proteção, segurança, qualidade e disponibilidade dos dados tratados pela **Emergent Cold LatAm** ("Emergent Cold", "ECLA" ou "Companhia"), assegurando que sua administração seja realizada de maneira lícita, segura, responsável e alinhada aos objetivos estratégicos do negócio e à continuidade operacional.

Esta Política define as diretrizes corporativas para a governança de dados em todas as operações da região, promovendo práticas consistentes que possibilitem gerir os dados como um ativo estratégico, reduzir os riscos associados ao seu tratamento, fortalecer a confiabilidade das informações e garantir o cumprimento da legislação vigente em cada país no que diz respeito à privacidade, proteção de dados pessoais, segurança da informação e normas setoriais relacionadas.

Além disso, esta Política estabelece a estrutura regional e local para a supervisão, coordenação e escalonamento em matéria de governança de dados, incluindo os papéis e responsabilidades aplicáveis às funções de supervisão e controle, tais como as equipes de Compliance, Tecnologia, Segurança da Informação e outros atores relevantes. Seu propósito é assegurar uma adequada separação de funções, independência operacional nos papéis de supervisão e uma coordenação efetiva com os responsáveis locais pelo tratamento de dados.

A implementação desta Política permite à ECLA consolidar um modelo regional de governança integral, baseado em princípios de qualidade, rastreabilidade, transparência, minimização de riscos e melhoria contínua ao longo do ciclo de vida dos dados.

2. ESCOPO

Estas diretrizes aplicam-se ao seguinte:

- Todos os dados gerados, recebidos, administrados, armazenados ou utilizados pela Emergent Cold LatAm, independentemente do seu suporte (físico, digital ou misto) e de sua natureza. Isso inclui, sem limitação, dados operacionais, comerciais, contratuais, logísticos, administrativos, financeiros, de continuidade operacional, de segurança da informação e quaisquer outros dados necessários

para as atividades da Companhia. Incluem-se também todos os dados pessoais e, quando aplicável, dados sensíveis ou de categoria especial tratados no âmbito das operações da ECLA.

- Todos os tratamentos de dados realizados no contexto das atividades da Emergent Cold LatAm, incluindo — a título exemplificativo — dados de contato de clientes (B2B), destinatários, remetentes, fornecedores, transportadores, visitantes, colaboradores, candidatos e qualquer outro terceiro cujos dados sejam tratados pela Companhia.
- Todo o pessoal da Emergent Cold LatAm, independentemente do regime de vínculo contratual (empregados, contratados, consultores, temporários), bem como fornecedores, operadores e suboperadores que acessem, gerenciem ou tratem dados em nome da Companhia em qualquer dos países onde ela opera.

Este escopo inclui todas as instalações, sistemas, processos, unidades de negócio e operações tecnológicas que participem do ciclo de vida dos dados, tanto em ambientes próprios quanto naqueles gerenciados por terceiros.

3. MARCO NORMATIVO

Esta Política é emitida e interpretada em conformidade com o marco legal vigente em cada um dos países onde a Emergent Cold LATAM desenvolve suas operações, incluindo a regulamentação aplicável em matéria de governança de dados, proteção de dados pessoais, segurança da informação, cibersegurança e continuidade operacional, conforme corresponda à atividade da Companhia.

Além disso, baseia-se nas obrigações regulatórias setoriais e nas disposições emitidas por autoridades competentes em nível regional, quando estas impuserem requisitos específicos para o tratamento, resguardo, administração ou proteção de dados no contexto das atividades da Emergent Cold LatAm.

A ECLA também adota princípios, boas práticas e diretrizes internacionalmente reconhecidas em matéria de governança de dados, gestão de riscos, segurança da informação e cibersegurança, aplicando-os de maneira proporcional e coerente com seu modelo operacional e com a legislação aplicável em cada jurisdição.

Por fim, esta Política integra-se às políticas, procedimentos e diretrizes corporativas internas da ECLA relacionadas à proteção de dados pessoais, segurança da informação, gestão de incidentes, continuidade de negócios e outros componentes do sistema

regional de compliance e gestão de riscos, os quais devem ser observados de forma complementar.

4. DEFINIÇÕES

Para os efeitos desta Política, sem prejuízo das definições contidas na legislação aplicável em cada país, entende-se por:

- **Governança de dados:** Conjunto de estruturas, papéis, princípios, políticas, práticas e procedimentos que orientam a gestão, uso, qualidade, proteção e administração dos dados ao longo de todo o seu ciclo de vida, assegurando seu aproveitamento responsável e alinhado aos objetivos corporativos.
- **Comitê de Governança de Dados (CGD):** Órgão responsável por liderar, supervisionar e orientar estrategicamente as diretrizes, iniciativas e controles associados à governança de dados dentro da Emergent Cold LATAM.
- **Direitos dos titulares:** Faculdades reconhecidas pela regulamentação aplicável às pessoas cujos dados são tratados, podendo incluir acesso, retificação, atualização, cancelamento, oposição, bloqueio, portabilidade e quaisquer outros previstos na legislação vigente.
- **Procedimento de exercício de direitos:** Processos e canais internos disponibilizados pela Emergent Cold LATAM para receber, gerenciar e responder às solicitações dos titulares dentro dos prazos e condições estabelecidos pela legislação aplicável e pelas políticas corporativas.
- **Responsável local de proteção de dados:** Papel designado em cada operação local para coordenar a implementação de políticas de governança de dados e proteção de dados pessoais, gerenciar riscos, atender solicitações de titulares e atuar como ponto de ligação com a equipe regional.
- **Função Regional de Governança e Proteção de Dados:** Equipe ou função responsável por estabelecer diretrizes regionais, supervisionar a implementação em cada país, fornece suporte técnico e normativo, monitorar o cumprimento e escalar incidentes ou riscos relevantes.
- **Dado ou ativo de informação:** Qualquer informação gerada, recebida, administrada ou utilizada pela Emergent Cold LATAM, independentemente de seu formato ou suporte, que possua valor operacional, legal, comercial ou estratégico.
- **Qualidade de dados:** Grau em que os dados atendem atributos essenciais como exatidão, completude, consistência, atualidade e oportunidade, permitindo decisões e operações confiáveis.

- **Ciclo de vida do dado:** Conjunto de etapas pelas quais um dado passa desde sua criação ou coleta, armazenamento, uso, compartilhamento, atualização, arquivamento e, finalmente, sua eliminação segura ou anonimização.
- **Proprietário de dados (Data Owner):** Papel ou área responsável por definir a finalidade, os critérios de qualidade, os níveis de acesso e os requisitos de proteção para um conjunto específico de dados.
- **Custodiante ou administrador de dados (Data Steward / Data Custodian):** Responsável por aplicar, manter e monitorar os controles operacionais necessários para preservar a integridade, disponibilidade, qualidade e rastreabilidade dos dados nos sistemas sob sua administração.
- **Inventário de dados:** Registro estruturado que documenta os tipos de dados tratados pela Companhia, sua localização, responsáveis, finalidades, fluxos, níveis de criticidade e controles aplicáveis.
- **Classificação de dados:** Processo por meio do qual os dados são categorizados com base em seu nível de sensibilidade, criticidade ou confidencialidade, estabelecendo os requisitos de proteção associados.
- **Dados críticos:** Dados cuja perda, alteração, divulgação ou indisponibilidade pode afetar significativamente a operação, a continuidade do negócio, o cumprimento regulatório, a segurança ou as relações comerciais.
- **Fluxos de dados:** Movimentos ou transferências de dados entre sistemas, áreas, processos, países ou terceiros, incluindo intercâmbios internos e transmissões externas.
- **Acesso autorizado:** Permissão concedida a pessoas ou sistemas, baseada em princípios de necessidade e proporcionalidade, para consultar, modificar ou utilizar dados conforme as funções atribuídas.
- **Incidente de dados:** Qualquer evento que afete ou possa afetar a integridade, confidencialidade, disponibilidade, qualidade ou rastreabilidade dos dados, incluindo acessos não autorizados, perda, destruição, alteração ou divulgação indevida.
- **Rastreabilidade de dados:** Capacidade de conhecer e reconstruir a origem, uso, modificações, acessos e movimentações dos dados ao longo de seu ciclo de vida.
- **Anonimização:** Processo pelo qual os identificadores de um dado pessoal são removidos de forma irreversível, de modo que não seja possível associá-lo a uma pessoa.
- **Pseudonimização:** Técnica que substitui identificadores pessoais por códigos ou atributos indiretos, reduzindo o nível de exposição do dado sem impedir sua utilização para certos fins permitidos.

- **Ecossistema de dados:** Conjunto de processos, sistemas, plataformas, pessoas, tecnologias e regras que interagem para permitir a gestão, proteção e uso dos dados dentro da Emergent Cold LATAM.

5. PRINCÍPIOS NORTEADORES

A governança de dados da Emergent será regida, no mínimo, por:

- a. **Licitude:** todo tratamento deve possuir base legal definida.
- b. **Finalidade e compatibilidade:** uso para finalidades explícitas e legítimas, evitando usos incompatíveis.
- c. **Minimização e proporcionalidade:** apenas dados estritamente necessários.
- d. **Qualidade e integridade:** dados exatos, consistentes e atualizados.
- e. **Confidencialidade e segurança:** medidas técnicas e organizacionais adequadas.
- f. **Limitação temporal:** conservação apenas pelo tempo necessário; eliminação ou anonimização oportuna.
- g. **Transparência:** informação clara aos titulares quando aplicável.
- h. **Responsabilização proativa (accountability):** evidência documental de conformidade.
 - a. **Gestão baseada em riscos:** controles proporcionais ao risco do tratamento (tipo de dado, volume, exposição, criticidade operacional, terceiros, tecnologias).

6. PAPÉIS E RESPONSABILIDADES

A implementação efetiva da Governança de Dados na Emergent Cold LatAm requer a participação coordenada de diversos papéis e estruturas organizacionais, tanto em nível regional quanto local. Cada ator envolvido desempenha funções específicas destinadas a garantir que os dados sejam gerenciados, protegidos e utilizados de forma responsável, segura e alinhada aos objetivos estratégicos da Companhia.

Os seguintes papéis e responsabilidades estabelecem o marco base que deve ser aplicado de forma uniforme em todas as operações da região, sem prejuízo das obrigações adicionais que possam ser aplicáveis conforme a legislação vigente em cada país:

1. Comitê de Compliance:

Órgão colegiado responsável por liderar a governança de dados. Compete-lhe:

- Aprovar esta Política e suas atualizações.
- Definir diretrizes estratégicas, priorizar iniciativas e resolver conflitos de acesso/uso entre áreas.
- Assegurar coerência entre esta Política, o MPI e os procedimentos (bases legais, retenção/eliminação, incidentes, fornecedores).
- Revisar periodicamente riscos associados ao tratamento de dados e exigir planos de melhoria.
- Coordenar com Segurança da Informação, Compliance e o(s) DPO(s) a implementação de controles e evidências.

2. **Responsável Local de Proteção de Dados (função local aplicada a cada país):**

A Emergent Cold LatAm designará um responsável local em cada operação para coordenar a correta implementação desta Política e do programa de proteção de dados em nível país. Essa função atuará com independência operacional e terá acesso às informações, recursos e apoio necessários, cabendo-lhe:

- Informar e assessorar as áreas operacionais e a área de Compliance quanto à Legislação Vigente e às políticas internas aplicáveis ao tratamento de dados pessoais.
- Supervisionar o cumprimento desta Política, do MPI e dos procedimentos associados (bases legais, retenção, incidentes, gestão de terceiros), identificando lacunas e propondo medidas corretivas.
- Validar e manter a documentação de conformidade (registros, evidências, matrizes, instruções), e apoiar a elaboração de avaliações de impacto quando aplicável.
- Validar e manter a documentação de conformidade (registros, evidências, matrizes, instruções), e apoiar a elaboração de avaliações de impacto quando aplicável.
- Coordenar, juntamente com Segurança da Informação e Compliance, a gestão de incidentes e violações que afetem dados pessoais, assegurando rastreabilidade e evidências.
- Capacitar e promover treinamentos periódicos em proteção de dados para as equipes que participam de operações de tratamento.
- Atuar como ponto de contato operacional para consultas internas sobre tratamento de dados, mantendo o dever de reserva e confidencialidade.

Escalonamento obrigatório: quando ocorrerem (i) solicitações de titulares complexas ou sensíveis, (ii) procedimentos administrativos de fiscalização, requisições da

autoridade, ou (iii) controvérsias relevantes sobre bases legais, transferências, suboperadores, incidentes ou decisões de alto risco, o DPO Local deverá consultar e coordenar com o DPO Regional antes de adotar determinações finais ou emitir respostas definitivas, salvo quando a urgência impedir tal coordenação, caso em que informará imediatamente ao DPO Regional.

3. **Responsável Regional de Governança e Proteção de Dados:**

A ECLA designará um Responsável Regional encarregado da supervisão, direção e governança do cumprimento regional em matéria de governança de dados e proteção de dados pessoais. Este papel atuará com independência operacional para emitir critérios, recomendações e relatórios, e reportará diretamente ao Conselho de Administração ou órgão equivalente estabelecido pela Companhia. Em particular, compete-lhe:

- a. **Definir diretrizes regionais** em matéria de governança de dados, proteção de dados pessoais, gestão de riscos e integração com as políticas corporativas aplicáveis, assegurando uma abordagem homogênea em toda a região.
- b. **Solicitar e revisar relatórios periódicos do Responsável Local**, incluindo métricas de conformidade, riscos, incidentes, violações, auditorias, implementação de controles e quaisquer outras evidências relevantes.
- c. **Avaliar e se manifestar sobre matérias críticas** elevadas pelo Responsável Local, tais como fiscalizações, incidentes relevantes, avaliações de impacto quando aplicáveis, tratamento de riscos significativos, decisões sobre fornecedores e terceiros, ou eventos que exijam diretrizes regionais. Da mesma forma, coordenará com Segurança da Informação, Tecnologia e Compliance para assegurar respostas unificadas e coerentes com os requisitos regulatórios da região.
- d. **Apresentar relatórios periódicos ao Conselho de Administração** ou órgão equivalente, informando o estado regional da conformidade, os principais riscos, incidentes, métricas, violações, medidas de mitigação e planos de melhoria, sem prejuízo de relatórios extraordinários quando a criticidade do caso assim o exigir.

7. **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 com as diretrizes, políticas e procedimentos corporativos vigentes em matéria de governança de dados, proteção de dados pessoais,

segurança da informação, cibersegurança, continuidade operacional e outros instrumentos próprios do sistema de controle interno da Companhia.

O cumprimento desta Política será considerado dentro dos processos de identificação, avaliação e mitigação de riscos, bem como nas atividades de auditoria, monitoramento e controle que derivem do marco regional. Qualquer descumprimento de suas disposições poderá dar origem a medidas corretivas, contratuais ou disciplinares conforme a normativa interna da Emergent Cold LatAm e a legislação aplicável em cada jurisdição.

As modificações ou ajustes decorrentes de mudanças normativas, tecnológicas ou organizacionais deverão ser incorporados oportunamente, e as versões atualizadas serão comunicadas às áreas responsáveis e integradas aos documentos e procedimentos complementares correspondentes.

8. VIGÊNCIA E REVISÃO

A presente Política entrará em vigor a partir de sua aprovação pelo Comitê de Compliance da ECLA e permanecerá vigente até que tal Comitê determine sua atualização ou substituição.

O Comitê de Compliance realizará uma revisão periódica, pelo menos a cada dois anos, ou com maior frequência quando ocorrerem mudanças normativas, tecnológicas, estratégicas ou operacionais que a justifiquem. Essa revisão considerará a evolução do marco regulatório nos países onde a Companhia opera, as práticas corporativas emergentes, os riscos associados ao tratamento de dados e os resultados obtidos em auditorias ou atividades de monitoramento.

As atualizações desta Política serão comunicadas a todas as áreas envolvidas e deverão refletir-se nos procedimentos, diretrizes e documentos complementares aplicáveis.