Código LGPSC001	Assunto	Data de Emissão 29/10/2025	Revisão 29/10/2025

1-Introdução

Este é um resumo contendo as linhas gerais da Política de Segurança Cibernética da Menegalli Administradora de Consórcio Ltda, em cumprimento à Resolução nº 85 do Banco Central do Brasil , de 08 de abril de 2021, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil em especial o artigo 5º. que trata da divulgação ao público das linhas gerais da política de segurança cibernética.

2- Objetivos e Princípios

A Política de Segurança da Informação e Cibernética da Menegalli Administradora de Consórcios Ltda. tem como objetivo assegurar a proteção integral dos ativos de informação, garantindo a confidencialidade, integridade, disponibilidade e autenticidade dos dados sob sua gestão, incluindo informações corporativas, de clientes, colaboradores, parceiros e terceiros.

Inspirada nas boas práticas internacionais de governança e gestão da segurança da informação (especialmente na norma ABNT NBR ISO/IEC 27002:2013) e em conformidade com as legislações vigentes — como a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e as normas do Banco Central do Brasil — a política orienta a condução ética, segura e responsável das atividades digitais e operacionais da administradora.

Os princípios que norteiam a política são:

- Confidencialidade: assegurar que informações e dados pessoais sejam acessados apenas por pessoas autorizadas.
- Integridade: garantir que os dados permaneçam completos, exatos e protegidos contra alterações indevidas.
- Disponibilidade: assegurar que as informações e sistemas estejam acessíveis quando necessários.
- Autenticidade e rastreabilidade: permitir a identificação segura de usuários, origens e operações realizadas.
- Conformidade: atuar em alinhamento às normas legais e regulatórias aplicáveis ao setor de consórcios.

Esses princípios orientam a gestão segura de informações e o compromisso da Menegalli com a confiança, transparência e continuidade das operações.

3- Abrangência e Responsabilidades

A Política de Segurança da Informação se aplica a todas as unidades, departamentos, colaboradores, estagiários, prestadores de serviços, parceiros comerciais e visitantes que tenham acesso, direto ou indireto, a informações, sistemas, redes ou ativos tecnológicos da Menegalli.

A aplicação da política abrange todas as formas de informação, sejam impressas, digitais, orais ou audiovisuais, e todos os meios utilizados para o seu armazenamento e transmissão, incluindo servidores, estações de trabalho, dispositivos móveis, redes corporativas e sistemas de comunicação eletrônica.

Cada usuário é responsável pelo uso ético, lícito e diligente dos recursos tecnológicos disponibilizados. As credenciais de acesso (usuário e senha) são pessoais e intransferíveis, e o titular responde pelas ações realizadas sob sua identificação.

Cabe aos gestores e à área de Tecnologia da Informação (TI) supervisionar o cumprimento das diretrizes, garantir que controles de segurança estejam implementados e promover ações de conscientização entre os colaboradores.

A Diretoria da Menegalli mantém a responsabilidade final sobre a governança da política e o apoio institucional às práticas de segurança e privacidade.

4- Governança e Gestão de Riscos Cibernéticos

A governança de segurança da informação da Menegalli está estruturada com base em gestão de riscos contínua, alinhada aos objetivos estratégicos do negócio e às exigências do Banco Central do Brasil.

O processo de gestão de riscos cibernéticos envolve as etapas de identificação, análise, avaliação e tratamento de riscos, considerando a probabilidade e o impacto de incidentes que possam comprometer a continuidade operacional, a integridade dos dados e a imagem institucional.

As principais medidas de governança incluem:

- Classificação e inventário dos ativos de informação, com identificação de responsáveis.
- Avaliação periódica de vulnerabilidades e ameaças, por meio de controles técnicos e administrativos.
- Adoção de medidas preventivas e corretivas compatíveis com o nível de risco identificado.
- Controle formal de acesso, garantindo o princípio do menor privilégio.
- Gestão de contratos e fornecedores, exigindo o cumprimento de padrões mínimos de segurança e confidencialidade.
- Capacitação e conscientização contínua dos colaboradores em temas de segurança da informação, proteção de dados e uso ético de recursos tecnológicos.

A gestão de riscos cibernéticos visa preservar a resiliência operacional da Menegalli, evitando interrupções de serviço e protegendo os dados pessoais e corporativos tratados sob sua responsabilidade.

5- Controles e Medidas de Proteção Adotadas

A Menegalli implementa um conjunto de controles técnicos, físicos e administrativos para prevenir, detectar e responder a incidentes de segurança, abrangendo:

a) Acesso e Senhas

- Utilização de senhas individuais, complexas e intransferíveis, com renovação periódica e bloqueio após tentativas malsucedidas.
- Controle de privilégios de acesso, assegurando que cada usuário possua apenas as permissões necessárias à sua função.
- Bloqueio de contas inativas e rastreabilidade das ações de usuários.

b) Uso da Internet e E-mail

- Acesso à Internet restrito aos sites autorizados pela área de TI, mediante autenticação de usuário.
- Proibição de instalação de softwares não homologados e de compartilhamento de informações sigilosas por canais externos.
- Monitoramento de tráfego e controle de mensagens para evitar vazamento de dados, fraudes e malwares.
- Política de uso ético e profissional do e-mail corporativo, vedado o envio de mensagens pessoais, spam ou conteúdo ilícito.

c) Segurança Física

- Controle de acesso às instalações críticas, como o departamento de TI, RH e arquivo geral.
- Identificação obrigatória de funcionários e visitantes.
- Restrição ao uso de câmeras, celulares e dispositivos externos sem autorização.

d) Dispositivos Móveis

- Aplicação de regras específicas para uso de notebooks, smartphones e tablets corporativos ou pessoais (BYOD).
- Obrigatoriedade de antivírus atualizado, duplo fator de autenticação e backups regulares.
- Proibição de armazenar dados sigilosos em mídias removíveis (pendrives, HDs externos).
- Acesso de visitantes apenas mediante rede isolada e credenciais temporárias.

Esses controles integram uma arquitetura de segurança que combina tecnologia, processos e comportamento humano, assegurando a conformidade e a proteção do ambiente digital da administradora.

6- Procedimentos de Monitoramento, Comunicação e Resposta a Incidentes

A Menegalli realiza monitoramento contínuo de suas redes e sistemas, com registro e análise de eventos relevantes à segurança da informação. O objetivo é detectar rapidamente anomalias, prevenir fraudes, conter ameaças e mitigar impactos sobre a operação e os dados.

Todos os usuários devem reportar imediatamente qualquer suspeita de incidente, falha ou ameaça à segurança da informação ao canal institucional — preferencialmente via e-mail consorcio@menegalli.com.br.

São considerados incidentes, entre outros:

- Acesso não autorizado a sistemas, redes ou dados.
- Vazamento, modificação ou destruição indevida de informações.
- Infecção por vírus, malwares ou softwares maliciosos.

- Violações às normas internas ou legais sobre o uso de recursos tecnológicos.

A equipe responsável pela gestão de segurança realiza a investigação, registro e tratamento dos incidentes, adotando medidas corretivas e comunicando, quando necessário, às autoridades competentes e às partes afetadas, conforme previsto em lei.

O monitoramento automatizado do tráfego de rede, uso de internet e e-mails corporativos visa garantir a conformidade com esta política e prevenir a ocorrência de condutas ilícitas ou lesivas à instituição.

7- Processo de Atualização e Revisão da Política

A Política de Segurança da Informação e Cibernética é revista e atualizada periodicamente, de forma a acompanhar a evolução tecnológica, as novas ameaças cibernéticas e as exigências legais e regulatórias aplicáveis ao sistema financeiro.

Projetos, aquisições e implementações tecnológicas futuras devem estar alinhados aos padrões de segurança estabelecidos nesta política. Caso alguma adequação técnica não seja possível, a justificativa será formalmente documentada para fins de auditoria e controle.

Esta política é um documento dinâmico, sujeito a revisões e atualizações periódicas para se adequar às novas tecnologias, regulamentações e cenários de ameaças.

A Menegalli Consórcios reafirma seu compromisso com a proteção contínua das informações, tratando a segurança cibernética como um pilar estratégico de suas operações.

A colaboração e o engajamento de todos os usuários são fundamentais para a construção de uma cultura de segurança robusta e para garantir a eficácia das medidas aqui descritas, assegurando a confiança de nossos clientes e a integridade de nossos serviços.