POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

MONTREAL

O FUTURO PRESENTE

SUMÁRIO

1. Objetivo..... 2
2. Aplicabilidade..... 2
3. Papeis e Responsabilidades..... 2
4. Diretrizes..... 3
5. Estrutura de Governança..... 3
6. Classificação da Informação..... 4
7. Controles de acesso..... 4
8. Direitos de propriedade intelectual..... 4
9. Proteção e privacidade de informações pessoais..... 5
10. Diretrizes quanto ao uso do e-mail corporativo..... 5
11. Diretrizes quanto ao uso da Internet e Download de Arquivos..... 5
12. Diretrizes quanto ao uso de Software de Mensageria..... 5
13. Diretrizes quanto ao uso de senhas corporativas..... 6
14. Diretrizes quanto ao uso de Mídias Removíveis..... 6
15. Diretrizes quanto a utilização de equipamentos de terceiros nas instalações da Montreal... 6
16. Uso de Dispositivos Móveis e Trabalho Remoto..... 6
17. Instalação e Uso de Softwares..... 7
18. Violações da Política de SI e Medidas administrativas disciplinares..... 7
19. Disposições Finais..... 7
20. Controle de alterações..... 8
21. Validação..... 8

© Este documento é de propriedade da Montreal

1. Objetivo

A Política de Segurança da Informação e Privacidade (PSIP), é o documento que orienta e estabelece diretrizes para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os envolvidos, e deverá ser cumprida e aplicada em todas as áreas da empresa.

A Política visa garantir a confidencialidade, integridade e disponibilidade das informações, assegurando o seu uso adequado e a mitigação de riscos à segurança da informação, bem como o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e de outras normas vigentes.

O documento norteia aos colaboradores e terceiros a seguirem padrões de comportamento relacionados à segurança da informação e privacidade adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo. Está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27001:2022 e ABNT NBR ISO/IEC 27701:2019.

2. Aplicabilidade

A PSIP é de caráter corporativo, aplicando-se a M.I. MONTREAL INFORMÁTICA S/A e empresas do Grupo. Cada regional deve observar integralmente as diretrizes aqui estabelecidas e, quando necessário, complementá-las com procedimentos locais específicos, respeitando suas particularidades operacionais, legais e tecnológicas, desde que não conflitem com as diretrizes corporativas.

Quaisquer alterações, adaptações ou complementações propostas pelas regionais deverão ser submetidas previamente ao Comitê de Segurança da Informação para análise, validação e aprovação formal, antes de sua implementação.

A Política se aplica a todos os ativos de informação da MONTREAL, incluindo dados, sistemas, aplicativos, dispositivos e redes. Seu escopo abrange todos os colaboradores, funcionários, contratados, parceiros e terceiros que acessam, utilizam ou processam informações da organização.

Esta política se aplica em todas as instalações físicas administradas ou utilizadas pela Montreal.

3. Papeis e Responsabilidades

- **Colaborador:** seja no regime CLT, Prestador de Serviço ou temporário, ao assinar o contrato declara estar ciente e comprometido com a política da segurança e privacidade da informação da MONTREAL, e deverá cumprir a Política e demais normas específicas de segurança da informação, e torna-se inteiramente responsável por todo prejuízo ou dano que vier sofrer ou causar à MONTREAL e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

© Este documento é de propriedade da Montreal

- **DAP e RH:** Exigir dos colaboradores a assinatura dos Termos, referente a segurança e privacidade da informação, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações sob responsabilidade da Montreal.

- **Gestor:** Ter postura exemplar em relação à segurança e privacidade da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão. Antes de conceder acesso às informações, deve-se avaliar a real necessidade de acesso com base nas funções exercidas ou perfil de acesso, conforme as responsabilidades atribuídas a cada colaborador. Analisar periódica e criticamente, conforme norma específica, os direitos de acesso dos usuários aos ativos sob sua responsabilidade. Propor adequação dos procedimentos, dos processos e sistemas sob sua responsabilidade para atender a esta PSIP.

- **Comitê de Segurança da Informação (CSI):** O Comitê de Segurança da Informação, se compromete com uma abordagem integrada e alinhada às necessidades específicas de cada localidade. É responsabilidade do comitê estabelecer e manter a Política de Segurança da Informação atualizada. Assim como, avaliar e aprovar os planos de continuidade e recuperação de desastres, relatórios de auditorias internas e externas, apoiar nas campanhas de conscientização e treinamentos em segurança e propor investimentos estratégicos em segurança.

- **Encarregado pelo Tratamento dos Dados Pessoais:** Conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis.

4. Diretrizes

- A segurança da informação é responsabilidade de todos os colaboradores.
- As informações devem ser classificadas conforme seu grau de criticidade e sensibilidade.
- O acesso às informações deve seguir o princípio do **menor privilégio** e da **necessidade de saber.**
- Todos os sistemas e ativos de informação devem ser protegidos contra uso não autorizado, perda, alteração ou destruição.
- É proibido o uso de recursos corporativos para fins pessoais, ilícitos ou que comprometam a imagem da empresa.

5. Estrutura de Governança

- **Comitê de Segurança da Informação:** órgão colegiado responsável por definir, revisar e aprovar políticas e diretrizes de SI.

© Este documento é de propriedade da Montreal

- **Equipe de Segurança da Informação:** responsável pela implementação dos controles, acompanhamento de incidentes e conscientização.
- **Representantes Regionais de SI:** cada regional deve designar um representante para atuar como ponto focal local, reportando incidentes e disseminando boas práticas.

6. Classificação da Informação

A MONTREAL adota um conjunto de diretrizes que tem por finalidade determinar como informações são classificadas, rotuladas e tratadas em todo o seu ciclo de vida e assegurar que a informação receba um nível adequado de proteção de acordo com a sua relevância para a organização e seus negócios, requisitos legais e outros aplicáveis.

A informação será classificada de acordo com sua sensibilidade, impacto e necessidade de restrição de acesso, utilizando as seguintes categorias:

- **Pública:** Informações que podem ser livremente divulgadas ao público externo, sem causar qualquer prejuízo à empresa.
- **Interna:** Informações de uso exclusivo dos colaboradores e parceiros autorizados. Embora não críticas, sua divulgação externa não autorizada pode gerar impactos operacionais ou reputacionais.
- **Restrita:** Informações cujo acesso deve ser limitado a grupos específicos dentro da empresa. Sua exposição pode causar impactos significativos aos negócios.
- **Confidencial:** Informações altamente sensíveis, cujo acesso deve ser rigorosamente controlado. O vazamento pode gerar graves consequências legais, financeiras ou estratégicas.

7. Controles de acesso

A MONTREAL regula o controle de acessos a sistemas e informações, garantindo que cada usuário tenha apenas os privilégios necessários às suas funções, prevenindo acessos indevidos, ou seja, o controle de acessos a recursos e informações da Montreal, são assegurados através de procedimentos de solicitação, identidade e autentificação para que apenas usuários autorizados possam acessar dados e sistemas de acordo com suas funções e responsabilidades. Todo esse processo está em conformidade com a Política de Gestão do Controle de Acesso da organização.

8. Direitos de propriedade intelectual

Toda a informação produzida, acessada ou manuseada pelos colaboradores durante o período de trabalho pertence integralmente à MONTREAL e é de uso exclusivo da empresa. Todos os ativos tangíveis e intangíveis, bem como marcas, conhecimentos e recursos tecnológicos, devem ser utilizados apenas para fins profissionais e dentro das funções atribuídas. O uso da marca, identidade visual e materiais de comunicação — inclusive em redes sociais — requer

© Este documento é de propriedade da Montreal

autorização prévia do departamento de marketing. Colaboradores podem mencionar a empresa apenas para indicar vínculo profissional, sem criar perfis ou representá-la oficialmente.

9. Proteção e privacidade de informações pessoais

A Política de Privacidade e Proteção de Dados Pessoais tem como objetivo estabelecer as diretrizes e responsabilidades da MONTREAL que assegurem e reforcem o compromisso da Organização com o cumprimento das legislações de proteção de dados pessoais. Este documento está em consonância com a legislação nacional em vigor, especialmente, a Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD).

10. Diretrizes quanto ao uso do e-mail corporativo

O e-mail corporativo é uma ferramenta de trabalho e propriedade da MONTREAL. Seu uso deve ser exclusivo para assuntos profissionais, com mensagens claras, objetivas e redigidas de forma respeitosa.

É proibido utilizar o e-mail para fins pessoais, cadastro em sites, envio de spam, correntes, piadas ou compartilhamento de informações confidenciais sem autorização.

A MONTREAL poderá monitorar os e-mails sempre que necessário para garantir a segurança da informação e o cumprimento desta política.

11. Diretrizes quanto ao uso da Internet e Download de Arquivos

A internet corporativa deve ser utilizada exclusivamente para fins profissionais. É proibido acessar sites com conteúdo impróprio, realizar atividades pessoais, participar de redes sociais ou baixar arquivos de fontes não confiáveis.

Downloads só devem ser feitos quando necessários ao trabalho, a partir de fontes seguras e com autorização, quando exigido. É proibido instalar programas ou armazenar arquivos pessoais nos dispositivos da empresa.

A MONTREAL poderá monitorar o uso da internet e os downloads realizados, visando à segurança da informação e ao cumprimento desta política.

12. Diretrizes quanto ao uso de Software de Mensageria

A internet corporativa deve ser utilizada exclusivamente para fins profissionais. É proibido acessar sites com conteúdo impróprio, realizar atividades pessoais, participar de redes sociais ou baixar arquivos de fontes não confiáveis.

© Este documento é de propriedade da Montreal

É proibido utilizar softwares de mensageria não autorizados (como WhatsApp, Telegram, entre outros) para tratar assuntos corporativos, exceto mediante aprovação prévia da área responsável.

As conversas no Teams devem manter linguagem profissional, objetiva e respeitosa. O uso da ferramenta está sujeito a monitoramento, visando garantir a segurança da informação e o bom uso dos recursos corporativos.

13. Diretrizes quanto ao uso de senhas corporativas

As senhas de acesso aos sistemas, e-mails e recursos corporativos são de uso pessoal e intransferível, sendo responsabilidade do colaborador mantê-las em sigilo.

14. Diretrizes quanto ao uso de Mídias Removíveis

O uso de mídias removíveis (como cartões de memória, pen drives ou HDs externos) não é permitido, exceto mediante autorização expressa e formal, emitida por escrito pelo Setor de Infraestrutura de TI da Montreal.

Caso o uso seja autorizado para transporte de arquivos, os dados deverão ser apagados imediatamente após o uso, a fim de prevenir eventuais vazamentos de informação.

15. Diretrizes quanto a utilização de equipamentos de terceiros nas instalações da Montreal

Computadores particulares não podem ser utilizados nas instalações da MONTREAL bem como para acesso à rede corporativa da organização.

Essa medida visa garantir a segurança das informações, a conformidade com as diretrizes internas de tecnologia e a mitigação de riscos relacionados ao uso de dispositivos não autorizados.

16. Uso de Dispositivos Móveis e Trabalho Remoto

A Montreal adota medidas para garantir a segurança da informação no uso de dispositivos móveis e na realização de atividades em regime de trabalho remoto.

Usuários autorizados devem utilizar esses recursos de forma segura, seguindo as diretrizes estabelecidas para proteger os dados e os sistemas da empresa.

A conexão remota ocorre por meios seguros e controlados, e o uso de dispositivos móveis respeitam as políticas internas quanto a proteção de acesso, armazenamento e transmissão de informações.

© Este documento é de propriedade da Montreal

17. Instalação e Uso de Softwares

A instalação e o uso de softwares nos ativos da organização são realizados de forma controlada, segura e em conformidade com as diretrizes internas.

Somente softwares previamente autorizados e licenciados podem ser utilizados em dispositivos corporativos, sendo expressamente proibida a instalação de programas não homologados ou adquiridos de fontes não confiáveis.

18. Violações da Política de SI e Medidas administrativas disciplinares

O não cumprimento dos requisitos previstos na PSIP e das Normas de Segurança da Informação e privacidade no caso do infrator ser um colaborador, acarretará violação às regras internas da empresa e sujeitará o colaborador às medidas administrativas e legais cabíveis. O Comitê Gestor de Segurança da Informação reportará o assunto para a Gerência de Recursos Humanos, podendo aplicar-se as seguintes penalidades:

- Advertência Verbal;
- Advertência escrita;
- Suspensão;
- Demissão por justa causa.

Nota: *As medidas disciplinares são proporcionais ao ato cometido, não podendo ser excessivas ou abusivas. São aplicadas após a apuração da ocorrência e ser única, ou seja, não devem ser aplicadas diversas medidas para uma mesma violação. São aplicadas em ordem gradativa onde as advertências verbal e escrita podem ser aplicadas às faltas mais leves e enquanto a suspensão e a demissão por justa causa pode ser aplicada para as faltas mais graves.*

19. Disposições Finais

A PSIP da MONTREAL será completada por Políticas Complementares de Segurança da Informação que tratem assuntos relacionados ao uso de controle de acesso, Proteção de Dados Pessoais, entre outros, serão consideradas partes integrantes desta PSIP.

As Políticas Complementares de Segurança da Informação estarão disponíveis em documentos internos, em local de fácil localização e acesso restrito. Já a PSIP deverá ficar disponível ao público.

Esta política entra em vigor a partir da data de sua publicação e pode ser revisada e alterada a qualquer momento, sempre que necessário, visando garantir sua efetividade diante das mudanças tecnológicas, organizacionais e legais. Deve, obrigatoriamente, ser revisada a cada dois anos para assegurar sua atualização contínua.

© Este documento é de propriedade da Montreal

20. Controle de alterações

Versão	Data	Elaborador	Aprovador	Descrição da Alteração
01	04/11/2025			Elaboração Inicial
02	18/11/2025	Sandro	Denise	Ajustes de formatação e nome da empresa

21. Validação

Data	Verificador
29/09/26	Revisão periódica realizada, sem alteração de conteúdo. Denise Castro.

Esta política se aplica a todas as empresas Montreal.
São elas PC Service Tecnologia, Mcare e Montreal Ventures.

Acesse nossos canais e saiba mais sobre este e outros temas.

© Este documento é de propriedade da Montreal