A reprodução/impressão deste documento torna a CÓPIA NÃO CONTROLADA Impresso por: WTB GUOXING | 05/09/202508:32:318

POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS E TRATAMENTO DE INFORMAÇÕES CONFIDENCIAIS E SENSÍVEIS

SETEMBRO DE 2025

Elaborador: Daniel Lima

Aprovador: Eduardo Pires

1. Índice

A reprodução/impressão deste documento torna a CÓPIA NÃO CONTROLADA Impresso por: WTB GUOXING | 05/09/202508:32:318

A reprodução/impressão deste documento torna a CÓPIA NÃO CONTROLADA Impresso por: WTB GUOXING | 05/09/202508:32:318

2. Definições

Membros da organização: Os integrantes de compliance, diretores, gerentes, funcionários, colaboradores temporários e voluntários, bem como o restante de subordinados dos cargos acima.

Parceiros de Negócios: Toda pessoa física ou jurídica que não for colaborador da empresa ou que não integre a organização, mas que seja contratada para auxiliar no desempenho de suas atividades, tais como os parceiros, representantes, subcontratadas, fornecedores, consultores, prestadores de serviços em geral, entre outros.

Responsável pelo Compliance (RC): Profissional especializado em compliance, conhecido como "Compliance Officer" (CO), dotado de poderes autônomos de iniciativa e controles, a quem é confiado, entre outras tarefas, a responsabilidade de fiscalizar a operação, o devido cumprimento e a sustentabilidade do programa de compliance e privacidade e proteção de dados pessoais da organização.

Terceiro: pessoa física ou jurídica ou órgão independente da organização.

3. Objetivo

A presente política tem como objetivo implementar diretrizes e procedimentos para proteger as informações classificadas como confidenciais na organização a fim de garantir o cumprimento da **Política de Compliance Código de Conduta Anticorrupção (AC03-GX-0012-BRA-I)** relativas à troca de informações comerciais estratégicas e sensíveis.

Dessa forma, as informações confidenciais são consideradas importantes ativos para a empresa e, em razão disso, devem estar sujeitas à proteção especial para impedir o uso inadequado e que terceiros não autorizados tenham acesso, bem como utilizem de forma indevida tais informações confidenciais.

4. Âmbito de Aplicação

Esta política se aplica a todos os membros da organização, independentemente de sua posição, qualificação profissional e/ou cargo hierárquico na empresa.

Todos os membros da organização devem exercer os seus melhores esforços para garantir que todos, sem exceção, incluindo terceiros e Parceiros de Negócios, respeitem as diretrizes desta Política.

A reprodução/impressão deste documento torna a CÓPIA NÃO CONTROLADA Impresso por: WTB GUOXING | 05/09/202508:32:318

Esta Política segue as orientações e recomendações das melhores práticas de segurança da informação contidas na Norma Internacional ISO/IEC 27001, bem como as demais legislações vigentes de privacidade, proteção de dados pessoais e segurança da informação.

5. Classificação das Informações

O gestor de área deve definir um modelo de classificação da informação que permita conhecer e implementar as medidas técnicas e organizacionais necessárias para manter a sua disponibilidade, confidencialidade e integridade. O modelo de classificação deve integrar os requisitos e condições estabelecidos nesta seção da política.

Igualmente, o gestor acima mencionado terá a responsabilidade de atualizar o modelo de classificação quando julgar conveniente e compartilhar com a sua equipe.

5.1 Tipos de Informações

A organização deve classificar a informação de acordo com o meio em que está sendo utilizada:

a) Software: informação que está sendo utilizada por meio de automação de escritório, e- mail ou sistemas de informação desenvolvidos para medição ou adquiridos de terceiros; e

b) Mídia física: informações que estão em papel, mídia magnética como USBs, DVDs, etc..

5.2 Níveis de Classificação

Dependendo da sensibilidade das informações, a organização deverá classificá-las em cinco níveis, a observar no **Anexo I** “Níveis de classificação”:

- Uso público;
- Difusão limitada;
- Informações confidenciais;
- Informações reservadas; e
- Informações secretas.

5.3 Classificação das Informações

A organização deve classificar as informações utilizando métodos manuais e/ou, caso necessário, métodos automatizados para facilitar o processamento adequado das medidas de segurança aplicáveis para as informações.

Todos os documentos e materiais devem ser classificados, assim como os anexos, cópias, traduções ou extratos destes, de acordo com os níveis de classificação da informação definidos no item anterior, exceto para as informações classificadas para “Uso Público”.

A reprodução/impressão deste documento torna a CÓPIA NÃO CONTROLADA Impresso por: WTB GUOXING | 05/09/202508:32:318

Assim, deve-se definir um procedimento para a classificação das informações de acordo com os seguintes requisitos:

- Certificar que o rótulo das informações siga as diretrizes de classificação das informações adotado.
- Garantir que as etiquetas sejam facilmente reconhecíveis entre todos os colaboradores.
- Orientar os colaboradores sobre onde e como as etiquetas serão colocadas ou utilizadas, de acordo com o processo de acesso à informação, bem como dos ativos que a suportam.
- Indicar as exceções para casos em que não há necessidade de classificação das informações.

Para os casos de itens e bens físicos com informações sensíveis e secretas, é necessária uma atenção especial a fim de evitar e mitigar riscos de acessos indevidos e roubo.

Ainda, também é necessária a implementação de medidas técnicas, quando necessário, para a classificação automática de informações suportadas em mídia digital.

A organização deve garantir a capacitação e treinamento sobre classificação das informações de todos os seus colaboradores, bem como ministrar um treinamento especial para os colaboradores que lidam nas suas atividades com informações confidenciais ou sigilosas.

6. Funções e Obrigações

6.1 Testes com Dados Reais

- Os testes prévios à implementação ou modificação dos sistemas de informação que processam arquivos com dados pessoais devem ser comunicados ao Departamento de Sistemas de Informação da organização.

6.2 Uso do E-mail

O email deve conter o seguinte rodapé:

ADVERTENCIA LEGAL

Esta mensagem é destinada exclusivamente ao seu destinatário e contém informações confidenciais sujeitas a sigilo profissional, cuja divulgação não é permitido por lei. Se você recebeu esta mensagem por engano, por favor, imediatamente, avise-nos através deste e-mail e proceda com a sua eliminação, bem como a de quaisquer documentos a este ligado. Da mesma forma, informamos que a distribuição, cópia ou uso desta mensagem ou qualquer de seus anexos, qualquer que seja a sua finalidade, é proibido por lei.

O correio eletrônico não garante a confidencialidade das mensagens, nem a sua integridade ou a correta recepção. A WTB GUOXING não assume qualquer responsabilidade por essas circunstâncias. Caso o destinatário desta mensagem não concorde com a utilização deste correio eletrônico e a gravação destas mensagens, leve a nosso conhecimento imediatamente.

Em conformidade com os regulamentos de proteção de dados, o informamos que os seus dados pessoais são parte de um arquivo de propriedade da WTB GUOXING Ltda., e que são tratados com o propósito de desenvolver a relação com você. Você pode exercer seus direitos de acesso, retificação, cancelamento e oposição por escrito para o endereço acima.

A reprodução/impressão deste documento torna a CÓPIA NÃO CONTROLADA Impresso por: WTB GUOXING | 05/09/202508:32:318

6.3 Encarregado de Privacidade e Proteção de Dados Pessoais

No caso de um caso previsto na legislação aplicável, a organização designará a figura do encarregado de privacidade, proteção de dados pessoais e sistemas de informação, podendo contatá-lo através do seguinte e-mail: conformidade@wtbguoxing.com.br.

6.4 Medidas de Controle

O conselho de administração da organização, de acordo com os seus poderes de gestão, reconhecidos no estatuto do trabalhador, poderá realizar, através da direção de sistemas de informação da empresa, as auditorias internas necessárias para verificar a correta utilização dos recursos tecnológicos, hardware e software da organização. Igualmente, poderá verificar que o correio eletrônico e a Internet somente serão utilizados para fins profissionais, especialmente durante a jornada de trabalho.

7. Diretrizes para Tratamento de Dados Pessoais

A organização estabeleceu uma série de diretrizes e procedimentos a serem seguidos pelos colaboradores no tratamento de dados pessoais.

Todos os colaboradores devem conhecer e aceitar as suas funções e obrigações em matéria de privacidade e proteção de dados pessoais. Dessa forma, para facilitar o cumprimento deste documento, uma série de procedimentos são disponibilizados aos colaboradores que respondem eventuais dúvidas que surgem no trabalho diário e que podem ser solicitadas ao departamento de privacidade e proteção de dados pessoais da organização.

Os colaboradores só terão que seguir os procedimentos que possam afetar o desempenho de suas funções.

8. Direitos dos Titulares de Dados Pessoais

Toda e qualquer pessoa natural tem a garantia da titularidade dos seus dados pessoais, bem como os direitos essenciais da liberdade, intimidade e privacidade, amparado pelo artigo 17º da LGPD.

A organização tem o compromisso de facilitar e garantir o exercício dos direitos dos titulares de dados - amparados pelo artigo 18º da LGPD (Lei n.º 13.709/2018):

- Confirmação de existência de tratamento;
- Acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com os requisitos da LGPD;

A reprodução/impressão deste documento torna a CÓPIA NÃO CONTROLADA Impresso por: WTB GUOXING | 05/09/202508:32:318

- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da Autoridade Nacional (ANPD), observados os segredos comercial e industrial;
- Eliminação dos dados pessoais tratados (com o consentimento do titular), com exceções previstas no art. 16º da LGPD;
- Informação das entidades públicas e privadas com as quais o controlador realizou a utilização compartilhada de dados;
- Informação sobre a possibilidade da negativa do consentimento do fornecimento dos dados pessoais, bem como suas consequências;
- Revogação do consentimento, de acordo com os requisitos do § 5º do art. 8º da LGPD.

Dessa forma, todos os colaboradores e parceiros da organização devem respeitar as diretrizes e regras estabelecidas nas políticas internas que regem o exercício dos direitos dos titulares de dados.

Para qualquer tipo de consulta relacionada ao tratamento de dados pessoais, os colaboradores podem entrar em contato com: dpo@carmoenergy.com.

9. Transferência Internacional de Dados Pessoais

A organização deve sempre garantir que em casos de transferência de dados pessoais para países que não tenham um nível adequado de conformidade de privacidade e proteção de dados pessoais, prevaleça os requisitos estabelecidos pela legislação aplicável.

10. Implementação do Sistema de Gestão de Proteção de Dados Pessoais

De acordo com os princípios e normas presentes nesta política, a organização deverá desenvolver procedimentos internos que permitam a implementação da Lei Geral de Proteção de Dados Pessoais, possibilitando um efetivo sistema de gestão de proteção de dados, em caráter obrigatório para todos os colaboradores e parceiros da organização.

O departamento de privacidade e proteção de dados pessoais da organização é responsável pelo acompanhamento do cumprimento e implementação do sistema de gestão de proteção de dados pessoais. Ainda, é importante a criação de um comitê de privacidade e proteção de dados para se responsabilizar e monitorar a conformidade e a implementação do sistema de gestão de proteção de dados.

11. Segurança nas Tratativas com o Fornecedor

O departamento de privacidade e proteção de dados pessoais deve avaliar com atenção todos os serviços que poderão ser terceirizados para que sejam identificados aqueles que são relevantes do ponto a nível de

A reprodução/impressão deste documento torna a CÓPIA NÃO CONTROLADA Impresso por: WTB GUOXING | 05/09/202508:32:318

segurança da informação - seja pela sua natureza, pela sensibilidade dos dados que precisam ser endereçados, bem como pela dependência de continuidade de negócios.

Em relação aos prestadores desses serviços, devem ser atendidos os processos de seleção, requisitos contratuais, monitoramento dos níveis de serviço, retorno de dados e as medidas de segurança implementadas pelo referido prestador, que devem ser, no mínimo, equivalentes às estabelecidas nos regulamentos internos da organização.

12. Informações Confidenciais Internas e Comerciais

As informações confidenciais devem ser definidas como informações relativas à organização ou a qualquer membro da organização que, caso divulgadas, possam causar danos à situação financeira, ao planejamento estratégico ou à reputação da organização, bem como à privacidade de seus membros. As informações confidenciais são propriedade da organização.

Como regra geral, todas as informações geradas no desenvolvimento da atividade da organização pelos seus membros são confidenciais, incluindo as informações divulgadas aos membros da organização devido ao desenvolvimento do seu trabalho profissional - geralmente não conhecidas fora da organização ou protegidas por lei.

São consideradas informações confidenciais:

- A estratégia da organização;
- Informações – pessoais e profissionais - sobre os membros da organização;
- Informações não públicas sobre o organograma, estrutura de acionistas, finanças, auditoria, seguro ou processos judiciais (em andamento ou concluídos) dos quais a organização ou seus membros fazem parte;
- Licitações públicas ou privadas, em fase de oferta; e
- Informações – pessoais e profissionais - sobre os clientes, terceiros e parceiros de negócios da organização.

Consideram-se “informações comerciais sensíveis” as informações que uma empresa normalmente não compartilharia com terceiros fora da organização e, em particular, informações que possam permitir ao destinatário conhecer ou antecipar a conduta da empresa no mercado.

Exemplos de informações que, via de regra, são consideradas confidenciais em matéria de defesa da concorrência “antitruste”:

- Preços atuais ou futuros, incluindo descontos, abatimentos e promoções;
- Números de vendas, dados de custos ou margens;
- Quotas de mercado, dados sobre capacidade e sistemas de produção;
- Identidade de clientes ou fornecedores (reais ou potenciais);

A reprodução/impressão deste documento torna a CÓPIA NÃO CONTROLADA Impresso por: WTB GUOXING | 05/09/202508:32:318

- Informações sobre tecnologias de fabricação, direitos de propriedade intelectual ou industrial ou conhecimento técnico;
- Estratégias futuras de negócios, incluindo a intenção de participação de licitação, bem como apresentação ofertas em relação a um determinado contrato;
- Estratégias, orçamentos, planos ou políticas comerciais e/ou de marketing;
- Planos de expansão ou contratação de negócios, bem como planos de acesso à novos mercados ou saída de um mercado no qual a organização ou seus concorrentes operam atualmente;
- Previsões de ofertas futuras, condições de demanda, oferta ou indicadores financeiros.

13. Armazenamento das Informações Confidenciais

As informações confidenciais podem ser tanto físicas quanto eletrônicas. A organização terá que determinar qual o local específico para o armazenamento dessas informações confidenciais, bem como quais as medidas de segurança que impedem o acesso irregular e não autorizado.

Assim, essas informações não podem ser armazenadas em dispositivos pessoais dos Colaboradores ou em qualquer outro meio que não seja expressamente autorizado pela Empresa (por exemplo, Dropbox, redes sociais e/ou e-mails privados).

14. Divulgação de Informações Confidenciais

As informações confidenciais devem ser tratadas de forma ética e sigilosa e de acordo com as leis e normas vigentes, evitando-se o mau uso e exposição indevida.

Igualmente, todos os colaboradores tem o dever de respeitar o princípio da necessidade de informação e divulgar as informações confidenciais somente nas seguintes circunstâncias: (i) quando houver tratativa de informações comerciais negociadas com os clientes, sujeitas à aprovação do responsável pelo departamento correspondente; (ii) quando for necessário para a realização de determinadas atividades profissionais; (iii) quando os profissionais externos necessitarem, justificadamente, de determinada informação (por exemplo, auditores, advogados, consultores, etc.); (iv) quando for necessário o compartilhamento de informações confidenciais com os parceiros de negócios da organização; e (vi) quando for necessária a divulgação das informações confidenciais para viabilizar o desenvolvimento das atividades empresariais.

Portanto, caso a divulgação de informações confidenciais da empresa seja realizada em conformidade com as diretrizes da empresa, o colaborador responsável pelo compartilhamento de tais informações deverá garantir que ela cumpra com os seguintes requisitos:

- Transmitir informações confidenciais ao destinatário através de meios que garantam a manutenção da confidencialidade.

A reprodução/impressão deste documento torna a CÓPIA NÃO CONTROLADA Impresso por: WTB GUOXING | 05/09/202508:32:318

- Informar ao destinatário sobre a natureza estritamente confidencial das informações e suas obrigações relacionadas a ela.

Não se caracterizará descumprimento desta política a divulgação de informações confidenciais quando em atendimento a determinações decorrentes do poder judiciário ou legislativo, bem como de órgãos fiscalizadores e reguladores. E quando a divulgação se justificar, por força da natureza do negócio, a advogados, auditores e contrapartes.

15. Divulgação de Informações Comerciais Confidenciais

Os regulamentos de defesa da concorrência “Antitruste” proíbem a troca de informações comerciais sensíveis entre concorrentes, abarcando todos os contextos sujeitos a riscos de troca de informações comerciais sensíveis, por exemplo: associações de indústria, criação de joint venture com empresa concorrente, subcontratação em licitações públicas, negociação de operações de concentração ou colaboração, bem como elaboração de estudos de mercado ou outros projetos de interesse do setor.

Dessa forma, a troca de informações será considerada contrária à regulamentação na medida em que a informação trocada ultrapasse o necessário para realizar com sucesso a colaboração ou o projeto em questão, mesmo que não seja feito efetivamente o uso dela.

Todos os membros da organização devem sempre consultar o departamento jurídico sempre que tiverem dúvidas se a troca de informações é permitida ou não.

Assim, caso um concorrente envie ou sugira a troca de informações confidenciais, a recusa em receber ou trocar tais informações devem ser declarada de forma clara e expressa, gerando evidência, e o incidente relatado ao departamento de compliance da organização. Para os casos de recebimento das informações referidas (por exemplo, por e-mail ou durante uma reunião), o colaboradores deve entrar em contato com o responsável pelo compliance da organização.

Quaisquer informações comerciais trocadas com terceiros serão tratadas de acordo com os itens 14 (“Divulgação de Informações Confidenciais”) e 17 (“Terceiros, Informações Confidenciais e Informações Empresariais Confidenciais”).

16. Membros da Organização, Informações Confidenciais e Informações Comerciais Confidenciais

Os membros da organização têm o dever de não fazer uso indevido e não divulgar informações confidenciais internas e comerciais da organização. Esta obrigação deve ser expressamente incluída nos contratos de trabalho.

A reprodução/impressão deste documento torna a CÓPIA NÃO CONTROLADA Impresso por: WTB GUOXING | 05/09/202508:32:318

Durante o curso do contrato laboral, os membros da organização devem usar informações confidenciais internas e comerciais com absoluta responsabilidade e sigilo somente para o desenvolvimento de seu trabalho profissional.

Caso um membro da organização tiver quaisquer dúvidas sobre o uso e/ou divulgação de informações confidenciais, ele deve consultar o seu superior hierárquico e o departamento de compliance da organização.

Os membros da organização devem relatar qualquer ciência e/ou suspeita de violação desta Política, de acordo com as orientações no item 8 deste documento.

Dessa forma, recomenda-se que todos os membros da organização assinem a **Declaração de Confidencialidade (1001-FO-00012-BRA-I)**, de forma que declarem que todas as informações recebidas pela organização são estritamente confidenciais e que o signatário é obrigado a cumprir as diretrizes desta Política.

17. Terceiros, Informações Confidenciais e Informações Empresariais Confidenciais

Da mesma forma, a organização deve implementar as medidas necessárias para garantir que terceiros também sejam obrigados a manter a confidencialidade dos documentos recebidos pela organização.

Portanto, é necessário incluir as obrigações específicas de confidencialidade para as tratativas com quaisquer terceiros, através de cláusulas, termos ou avisos de confidencialidade. Tais obrigações devem ser claras e adequadas de acordo com a classificação da informação e suas obrigatoriedades.

Os membros da organização devem garantir que - antes da entrega de qualquer tipo de informação confidencial e informação comercial sensível - os destinatários tenham assumido efetivamente a sua obrigação de confidencialidade. A referida obrigação deverá estar prevista no acordo de confidencialidade entre as partes.

18. Auditoria e Monitoramento Contínuo

O sistema de gestão de proteção de dados deverá ser avaliado e monitorado periodicamente. Dessa forma, deverão ser realizadas auditorias periódicas para análise de cumprimento das diretrizes desta política, bem como análise da conformidade e adequação efetiva à Lei Geral de Proteção de Dados Pessoais, sob a direção e supervisão do comitê de privacidade e proteção de dados pessoais da organização

Todos os resultados obtidos em auditorias e controles de privacidade e proteção de dados pessoais deverão ser reportados ao Comitê de Privacidade e Proteção de Dados e à Alta Direção da organização.

A reprodução/impressão deste documento torna a CÓPIA NÃO CONTROLADA Impresso por: WTB GUOXING | 05/09/202508:32:318

A reprodução/impressão deste documento torna a CÓPIA NÃO CONTROLADA Impresso por: WTB GUOXING | 05/09/202508:32:318

Anexo I

Níveis de Classificação

Nível	Nível de detalhe	Exemplos
Uso público	Esta é uma informação que pode ser conhecida por qualquer tipo de pessoa e seu uso fraudulento não representa risco aosinteresses da organização.	Exemplos desse tipo de informação são os catálogos de produtos e as informações disponíveis no site corporativo.
Disseminação Limitada	São as informações utilizadas pelas áreas da organização e cujo uso fraudulento representa um risco insignificante aos interesses da organização.	Exemplos desse tipo de informação são os e-mails e documentos de trabalho das áreasda organização.
Informação Confidencial	É aquela informação que só pode ser conhecida por um pequeno número de pessoas e cuja utilização fraudulenta pode ter um impacto significativo nos interesses da organização.	Exemplos desse tipo de informação é a estratégia corporativa da organização, bem como os relatórios de auditoria.
Informação Reservada	É aquela informação que só o dono do mesmo deve saber, assim como, em casos específicos, um grupo muito pequeno de pessoas. A divulgação ou divulgação não autorizada deste tipo de informação pode prejudicar gravemente os interesses da organização.	Exemplos desse tipo de informação são as comunicações entre gerentes ou acionistas com decisões relevantes para as operações do negócio.
Informação Secreta	É aquela informação que somente o dono do mesmo devesaber e não deve ser revelada em hipótese alguma. A divulgação ou divulgação não autorizada deste tipo deinformação pode causar danos excepcionalmente graves aos interesses essenciais da organização.	Exemplos deste tipo de informação são os códigos de acesso dos colaboradores, credenciais de clientes ou chaves criptográficas para aceder aos sistemas.