

INTRODUÇÃO

O uso de dispositivos móveis, como telefone celular e chip corporativo, é essencial para garantir agilidade, conectividade e comunicação eficiente nas operações da empresa. Esta política estabelece as melhores práticas, medidas de segurança e condutas profissionais para o uso adequado desses recursos tecnológicos.

DEFINIÇÕES E ABRANGÊNCIA

1. Fins Profissionais:

1.1. O uso do telefone celular e chip corporativo deve ser restrito a fins estritamente profissionais, o que inclui atividades diretamente relacionadas às funções do colaborador e aos negócios da empresa, tais como:

- a) Comunicação com colegas, clientes e fornecedores;
- b) Acesso a e-mails corporativos e sistemas da empresa;
- c) Participação em videoconferências e reuniões online;
- d) Uso de aplicativos de produtividade e gerenciamento de tarefas autorizados pela empresa;
- e) Consulta a informações e pesquisas relacionadas ao trabalho.

1.2. São expressamente proibidas as seguintes atividades:

- a) Uso de redes sociais para fins pessoais;
- b) Acesso a sites de entretenimento e jogos online;
- c) Download e uso de aplicativos não autorizados pela empresa;
- d) Compartilhamento de informações confidenciais da empresa em redes sociais ou aplicativos de mensagens instantâneas;
- e) Realização de atividades que não estejam relacionadas ao trabalho durante o horário de expediente.

2. Aplicativos Não Autorizados

2.1. A instalação de aplicativos em dispositivos corporativos deve ser restrita àqueles autorizados pela empresa e diretamente relacionados às funções do colaborador.

2.2. Aplicações de jogos, redes sociais, streaming de vídeo e áudio, e outros aplicativos que não se enquadrem nessa categoria são expressamente proibidos.

- 2.3. O colaborador que necessitar de um aplicativo para fins profissionais deverá solicitar a autorização do seu gestor e do departamento de TI, justificando a necessidade e o uso que será feito do aplicativo.

3. Uso Durante a Condução de Veículos

- 3.1. É estritamente proibido o uso do telefone celular durante a condução de veículos, exceto quando utilizado com dispositivos de viva-voz que permitam a comunicação sem o uso das mãos. O colaborador deve respeitar a legislação de trânsito em vigor e garantir a segurança de si mesmo e de terceiros.

MONITORAMENTO E FISCALIZAÇÃO

4. Monitoramento do Uso

- 4.1. A empresa se reserva o direito de monitorar o uso dos telefones celulares e chips corporativos, incluindo registros de chamadas, histórico de navegação, uso de aplicativos e dados armazenados nos dispositivos, com o objetivo de garantir a conformidade com esta política e a segurança da informação.
- 4.2. O monitoramento será realizado em conformidade com a legislação aplicável e com respeito à privacidade dos colaboradores.
- 4.3. O monitoramento será **limitado ao mínimo necessário**, com registros controlados e finalidade específica, garantindo transparência e respeito à privacidade.

5. Investigação de Violações

- 5.1. Em caso de suspeita ou confirmação de violação desta política, a empresa poderá realizar investigações internas, incluindo o acesso aos dispositivos e dados armazenados, com o objetivo de apurar os fatos e tomar as medidas cabíveis.
- 5.2. As investigações serão conduzidas de forma confidencial e respeitando os direitos dos colaboradores.

PROTEÇÃO DE DADOS

6. Medidas de Segurança da Informação

- 6.1. Os colaboradores devem adotar as seguintes medidas de segurança da informação:
- a) Utilizar senhas complexas e únicas para acesso aos dispositivos e aplicativos;
 - b) Ativar a criptografia dos dispositivos para proteger os dados em caso de perda ou roubo;
 - c) Utilizar VPN para acesso à rede da empresa e garantir a segurança da conexão;
 - d) Manter os softwares de segurança atualizados e realizar varreduras regulares para prevenir malware e phishing¹;
 - e) Não compartilhar senhas ou códigos de acesso com terceiros;
 - f) Reportar imediatamente qualquer incidente de segurança, como perda, roubo ou acesso não autorizado aos dispositivos.
- 6.2. Em caso de perda ou roubo do dispositivo, o colaborador deve comunicar imediatamente o gestor para que sejam tomadas as medidas de segurança necessárias.
- 6.3. Falhas ou danos no equipamento devem ser reportados ao gestor imediatamente, para que providências de reparo ou substituição possam ser tomadas.

7. Armazenamento e Compartilhamento de Informações Confidenciais

- 7.1. Informações confidenciais da empresa devem ser armazenadas e compartilhadas com o máximo cuidado, utilizando-se de aplicativos de armazenamento seguros e autorizados pela empresa.

¹ “Phishing” é um tipo de ciberataque que tem como objetivo roubar informações pessoais, como senhas, números de cartão de crédito e informações bancárias. Os criminosos cibernéticos se disfarçam de empresas confiáveis, amigos ou pessoas conhecidas para enviar mensagens de e-mail falsas que contêm links para sites de phishing

- 7.2. É proibido o compartilhamento de informações confidenciais em redes sociais, aplicativos de mensagens instantâneas ou por qualquer outro meio que possa comprometer a segurança da informação.

TREINAMENTO E CONSCIENTIZAÇÃO

8. Programa de Treinamento

- 8.1. A empresa divulgará através de seu site essa política e levará a conhecimento de todos os colaboradores as melhores práticas para o uso responsável e as diretrizes desta política.

9. Atualização da Política

- 9.1. Esta política será revisada e atualizada periodicamente, ou sempre que necessário, para garantir a sua adequação às necessidades da empresa, às mudanças na legislação e às evoluções tecnológicas.

COMUNICAÇÃO E TRANSPARÊNCIA

10. Divulgação da Política

- 10.1. Esta política será divulgada de forma clara e acessível a todos os colaboradores através da intranet, e-mail ou outros meios de comunicação interna.

11. Canal de Comunicação

- 11.1. A empresa disponibilizará um canal de comunicação confidencial para que os colaboradores possam esclarecer dúvidas sobre esta política e denunciar violações de forma segura e anônima.

12. Responsabilidade e Uso Exclusivo

- 12.1. O colaborador é responsável pelo uso adequado do telefone e do chip corporativo, bem como pela segurança das informações contidas nesses dispositivos.

- 12.2. O chip corporativo deve ser utilizado exclusivamente no aparelho fornecido pela empresa e apenas para fins profissionais.
- 12.3. É proibido o uso de chips pessoais em celulares corporativos e o uso do chip corporativo em dispositivos pessoais.
- 12.4. Além das normas descritas nesta política, os Motoristas da empresa devem seguir rigorosamente a legislação de trânsito brasileira, bem como a Política de Frota da empresa OBDI.

POLÍTICAS GERAIS

13. Instalação de Aplicativos

- 13.1. É estritamente proibida a instalação de aplicativos não autorizados pela empresa em dispositivos corporativos.
- 13.2. O dispositivo deve ser mantido atualizado com as últimas atualizações de segurança notificadas pelo sistema do celular e protegido com senha ou biometria para evitar acesso não autorizado.

14. Término do Contrato de Trabalho

- 14.1. No término do contrato de trabalho, o colaborador deve devolver o telefone e o chip corporativo ao departamento responsável;
- a) Colaboradores administrativos: Departamento de Pessoal.
 - b) Colaboradores operacionais: Gestor da filial (Preposto).
- 14.2. Os gestores das filiais devem enviar os dispositivos devolvidos para o Departamento de Pessoal na Matriz da empresa.
- 14.3. Todos os dados pessoais e informações confidenciais devem ser apagados antes da devolução do dispositivo.

15. Atualização de Contatos

- 15.1. O colaborador deve manter sua lista de contatos atualizada, incluindo números de emergência e de colegas de trabalho.

16. Uso do WhatsApp:

16.1. O uso do aplicativo WhatsApp no celular corporativo deve seguir estritamente a Política de Uso do WhatsApp da empresa OBDI.

17. Carregamento e Conectividade do Equipamento

17.1. O colaborador deve garantir que o dispositivo corporativo esteja sempre carregado durante o horário de trabalho, evitando desconexões que possam prejudicar a comunicação.

18. Uso Adequado do Telefone Corporativo

18.1. O telefone corporativo deve ser utilizado exclusivamente para atividades profissionais.

18.2. Ligações pessoais devem ser evitadas, exceto em casos de emergência ou quando autorizadas pelo gestor.

18.3. O colaborador é responsável por controlar o uso de dados móveis do chip corporativo, utilizando-os de forma eficiente e alinhada às necessidades profissionais.

18.4. Qualquer uso indevido ou abusivo do telefone e do chip corporativo poderá resultar em advertências, sanções disciplinares e até mesmo o reembolso dos custos gerados, conforme avaliação da empresa.

19. Disposições Gerais

19.1. A presente versão da Política de Uso de Telefone Celular e Chip Corporativo, foi aprovada pela Diretoria da OBDI e entra em vigor na data de 26/11/2024.

REVISÃO	DATA	DESCRIÇÃO	ITEM REVISADO	AUTOR
1	03/12/2025	Divulgação Política	8.1	Rodrigo C.de Souza
1	03/12/2025	Monitoramento	4.3	Rodrigo C.de Souza