



MANUAL DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

| Governança, Proteção de Dados, Segurança Digital e Continuidade dos Negócios |

Versão: 01/2026 — Minuta para aprovação
Classificação: Documento Corporativo Interno

Responsável pela aprovação: Diretoria Executiva

Aplicabilidade: Todas as unidades, departamentos, colaboradores, administradores, prestadores de serviços e parceiros autorizados da WORDCOM.

APRESENTAÇÃO

A WORDCOM reconhece que a informação constitui um dos seus principais ativos estratégicos, sendo fundamental para a continuidade de suas operações, a preservação de sua credibilidade institucional, a proteção dos interesses de seus clientes e o desenvolvimento sustentável de seus negócios.

O presente Manual da Política de Segurança da Informação estabelece princípios, responsabilidades, normas, procedimentos e controles destinados a proteger as informações corporativas contra acessos não autorizados, perdas, vazamentos, alterações indevidas, destruição, fraudes, ataques cibernéticos e demais ameaças à segurança digital e documental.

Esta política integra o sistema de governança e o Programa de Integridade Corporativa da WORDCOM, abrangendo suas atividades de publicidade, comunicação, produção de conteúdo, jornalismo, eventos empresariais, inteligência de mercado e relacionamento institucional.

O Manual considera as boas práticas de segurança da informação das normas ISO/IEC 27001 e ISO/IEC 27002, a Lei Geral de Proteção de Dados Pessoais — LGPD (Lei nº 13.709/2018), o Marco Civil da Internet (Lei nº 12.965/2014) e demais disposições legais aplicáveis.

CAPÍTULO I — OBJETIVOS E PRINCÍPIOS

Artigo 1º — Objetivos

A Política de Segurança da Informação tem como objetivos:

- I. Proteger informações institucionais, comerciais, financeiras, operacionais e pessoais sob responsabilidade da WORDCOM.
- II. Prevenir incidentes de segurança, acessos indevidos, fraudes digitais, vazamentos e perdas de informações.
- III. Estabelecer responsabilidades para colaboradores, gestores, administradores e prestadores de serviços.
- IV. Garantir a utilização segura de sistemas, computadores, dispositivos móveis, redes e plataformas digitais.
- V. Assegurar o tratamento adequado dos dados pessoais de clientes, colaboradores, fornecedores, parceiros e participantes de eventos.
- VI. Preservar a continuidade das atividades empresariais diante de incidentes tecnológicos e operacionais.
- VII. Estabelecer mecanismos de identificação, comunicação, investigação e resposta a incidentes de segurança.
- VIII. Promover a cultura de segurança da informação em toda a organização.

Artigo 2º — Princípios fundamentais

A segurança da informação da WORDCOM observará os seguintes princípios:

- **Confidencialidade:** acesso às informações exclusivamente por pessoas autorizadas.
- **Integridade:** preservação da exatidão, consistência e confiabilidade das informações.
- **Disponibilidade:** garantia de acesso às informações e sistemas quando necessários às atividades autorizadas.
- **Autenticidade:** verificação da identidade de usuários e da origem das informações.
- **Rastreabilidade:** possibilidade de identificar e verificar operações relevantes realizadas nos sistemas.
- **Privacidade:** proteção dos dados pessoais e respeito aos direitos dos titulares.
- **Responsabilização:** definição clara das obrigações relacionadas à proteção da informação.

CAPÍTULO II — ABRANGÊNCIA E RESPONSABILIDADES

Artigo 3º — Abrangência

Esta política aplica-se a todos que tenham acesso a informações, documentos, equipamentos, sistemas ou ambientes tecnológicos da WORDCOM, independentemente de vínculo empregatício ou contratual.

Abrange informações armazenadas ou transmitidas em meios físicos, eletrônicos, digitais, audiovisuais e plataformas de terceiros.

Artigo 4º — Responsabilidade da Diretoria Executiva

Compete à Diretoria Executiva:

- I. Aprovar e promover a implementação da Política de Segurança da Informação.
- II. Assegurar recursos compatíveis com os riscos identificados.
- III. Designar formalmente o responsável pela Segurança da Informação.
- IV. Supervisionar a conformidade com as políticas internas e legislação aplicável.
- V. Deliberar sobre situações críticas que possam comprometer a continuidade dos negócios.

Artigo 5º — Responsável pela Segurança da Informação

A WORDCOM deverá designar um responsável pela coordenação dos controles de segurança da informação, com apoio técnico especializado, interno ou externo.

Suas atribuições compreenderão:

- I. Identificar e avaliar riscos tecnológicos e informacionais.
- II. Coordenar políticas de acesso e proteção dos sistemas.
- III. Supervisionar medidas de prevenção e resposta a incidentes.
- IV. Orientar os colaboradores sobre práticas seguras.
- V. Acompanhar rotinas de backup e recuperação de dados.
- VI. Manter inventário dos principais ativos tecnológicos.
- VII. Apresentar relatórios periódicos à Diretoria Executiva.

Artigo 6º — Responsabilidades dos colaboradores

Todos os colaboradores deverão:

- I. Utilizar os recursos tecnológicos exclusivamente para finalidades profissionais autorizadas, admitidas exceções expressamente previstas nas normas internas.
- II. Preservar o sigilo de informações corporativas e de terceiros.
- III. Proteger suas credenciais de acesso.
- IV. Comunicar imediatamente suspeitas de incidentes.
- V. Respeitar as orientações de segurança e privacidade.
- VI. Não compartilhar arquivos, senhas ou dados confidenciais sem autorização.
- VII. Participar dos treinamentos obrigatórios.

CAPÍTULO III — CLASSIFICAÇÃO E PROTEÇÃO DAS INFORMAÇÕES

Artigo 7º — Classificação

As informações da WORDCOM deverão ser classificadas conforme seu grau de sensibilidade.

Classificação	Exemplos	Regra de acesso
Pública	Comunicados oficiais, notícias publicadas e materiais institucionais autorizados	Divulgação permitida
Interna	Procedimentos, rotinas operacionais e comunicados internos	Pessoas autorizadas da organização
Confidencial	Contratos, propostas comerciais, informações financeiras e cadastros de clientes	Acesso restrito por necessidade profissional
Restrita	Senhas administrativas, dados pessoais sensíveis, estratégias críticas e informações sob sigilo especial	Acesso individualizado e rigorosamente controlado

Artigo 8º — Tratamento das informações

As informações classificadas como confidenciais ou restritas deverão ser armazenadas em ambientes autorizados, protegidas contra acesso indevido e compartilhadas somente com pessoas que necessitem delas para executar atividades legítimas.

A transmissão externa deverá utilizar meios aprovados pela organização, com medidas de proteção compatíveis com o risco.

Artigo 9º — Descarte seguro

Documentos físicos contendo informações protegidas deverão ser fragmentados ou descartados por procedimento seguro.

Arquivos eletrônicos, dispositivos e mídias deverão ser eliminados ou sanitizados por métodos adequados, observados os prazos legais de conservação e eventuais obrigações de preservação.

CAPÍTULO IV — CONTROLE DE ACESSO E SENHAS

Artigo 10º — Acesso aos sistemas

O acesso aos sistemas corporativos será concedido de acordo com as atribuições profissionais, observando o princípio do menor privilégio.

Cada usuário deverá possuir identificação individual, sendo proibido o compartilhamento de contas pessoais de acesso.

Artigo 11º — Política de senhas

Os usuários deverão adotar senhas fortes e exclusivas para os serviços corporativos.

A WORDCOM estabelecerá os seguintes requisitos mínimos:

I. Utilização preferencial de senhas longas, com pelo menos 12 caracteres, quando suportado pelo sistema.

II. Proibição de senhas previsíveis ou reutilizadas em contas pessoais.

III. Utilização obrigatória de autenticação multifator nos serviços que a suportem, prioritariamente em e-mails, plataformas financeiras, contas administrativas e redes sociais.

IV. Alteração imediata de senhas quando houver suspeita de comprometimento.

V. Proibição de compartilhamento de senhas por mensagens, e-mails ou documentos não protegidos.

VI. Utilização preferencial de gerenciador de senhas aprovado pela organização.

Artigo 12º — Desligamento e alteração de funções

No desligamento de colaboradores ou encerramento de contratos, os acessos deverão ser revogados imediatamente após o término da autorização, conforme procedimento coordenado entre a gestão responsável e a área de tecnologia.

Mudanças de função deverão resultar na revisão dos privilégios de acesso.

CAPÍTULO V — EQUIPAMENTOS, REDES E DISPOSITIVOS

Artigo 13º — Equipamentos corporativos

Computadores, notebooks, celulares e outros dispositivos utilizados nas atividades empresariais deverão possuir, conforme aplicável:

- I. Sistema operacional e programas atualizados.
- II. Proteção contra softwares maliciosos.
- III. Bloqueio automático de tela.
- IV. Criptografia de armazenamento, especialmente em equipamentos portáteis.
- V. Controle de instalação de programas.
- VI. Configuração segura de acesso às redes.

Artigo 14º — Dispositivos pessoais

A utilização de equipamentos pessoais para atividades profissionais dependerá de autorização e cumprimento dos requisitos mínimos de segurança definidos pela WORDCOM.

Deverão ser adotadas medidas que permitam separar informações corporativas de informações particulares, respeitada a privacidade dos usuários.

Artigo 15º — Redes e conexões

É proibida a utilização de redes inseguras para transmissão de informações confidenciais sem proteção adequada.

O acesso remoto a sistemas críticos deverá utilizar conexões protegidas, autenticação multifator e outros controles proporcionais ao risco.

CAPÍTULO VI — E-MAILS, INTERNET E COMUNICAÇÃO DIGITAL

Artigo 16º — E-mail corporativo

O e-mail corporativo constitui ferramenta institucional e deverá ser utilizado com responsabilidade.

É proibido:

- I. Encaminhar documentos confidenciais a pessoas não autorizadas.
- II. Abrir arquivos ou links suspeitos sem verificação adequada.
- III. Utilizar contas pessoais para armazenar informações corporativas sem autorização.
- IV. Transmitir mensagens fraudulentas, ofensivas ou contrárias às normas internas.
- V. Compartilhar listas de contatos, bases de clientes ou informações pessoais sem fundamento legítimo.

Artigo 17º — Aplicativos de mensagens

O uso de WhatsApp, plataformas de mensagens e ferramentas colaborativas para fins profissionais deverá respeitar a confidencialidade e a proteção de dados.

Informações restritas não deverão ser compartilhadas em grupos não autorizados.

As decisões contratuais e autorizações relevantes deverão ser registradas nos sistemas ou repositórios corporativos definidos pela organização.

CAPÍTULO VII — PROTEÇÃO DE DADOS PESSOAIS E LGPD

Artigo 18º — Tratamento de dados pessoais

A WORDCOM deverá tratar dados pessoais exclusivamente para finalidades legítimas, específicas e informadas, observando as bases legais aplicáveis e os princípios previstos na LGPD.

A coleta deverá limitar-se às informações necessárias à finalidade pretendida.

Artigo 19º — Direitos dos titulares

A organização deverá estabelecer procedimentos para atender solicitações legalmente cabíveis de titulares de dados, incluindo acesso, correção, eliminação, informação sobre compartilhamento e demais direitos previstos na legislação.

Artigo 20º — Dados de eventos e relacionamento comercial

As bases de dados de participantes de eventos, patrocinadores, palestrantes, clientes e contatos comerciais deverão ser utilizadas exclusivamente para finalidades compatíveis com as bases legais aplicáveis e as informações prestadas aos titulares.

A transferência de listas de participantes a patrocinadores ou terceiros dependerá de fundamento legal adequado, transparência e controles contratuais pertinentes.

Artigo 21º — Encarregado de Dados

A WORDCOM deverá avaliar suas obrigações legais quanto à designação de encarregado pelo tratamento de dados pessoais e manter canal apropriado para atendimento dos titulares, conforme a regulamentação aplicável.

CAPÍTULO VIII — SEGURANÇA DAS PLATAFORMAS DIGITAIS E REDES SOCIAIS

Artigo 22º — Contas institucionais

As contas oficiais de redes sociais, sites, plataformas de publicação, serviços de anúncios e sistemas de gestão de conteúdo deverão permanecer sob controle institucional da WORDCOM.

Deverão ser observados:

- I. Identificação dos administradores autorizados.
- II. Autenticação multifator.
- III. Controle de permissões.
- IV. Revisão periódica dos usuários com acesso.
- V. Recuperação segura de contas.
- VI. Revogação de acessos de ex-colaboradores e fornecedores.

Artigo 23º — Proteção de conteúdo e arquivos

Arquivos de criação, projetos audiovisuais, bancos de imagens, documentos editoriais, propostas e conteúdos não publicados deverão ser protegidos contra divulgação não autorizada, perda ou alteração indevida.

Os materiais produzidos para clientes deverão respeitar os compromissos de confidencialidade e propriedade intelectual assumidos contratualmente.

CAPÍTULO IX — CÓPIAS DE SEGURANÇA E CONTINUIDADE

Artigo 24º — Backup

A WORDCOM deverá implementar rotinas documentadas de cópias de segurança dos sistemas e informações considerados essenciais às suas atividades.

Os backups deverão observar:

- I. Frequência compatível com a criticidade das informações.
- II. Armazenamento em ambiente protegido.
- III. Controle de acesso às cópias.
- IV. Proteção contra exclusão ou alteração maliciosa.
- V. Testes periódicos de restauração.
- VI. Registro dos resultados e correção de falhas identificadas.

Artigo 25º — Continuidade dos negócios

Deverá ser elaborado Plano de Continuidade de Negócios para orientar a recuperação das atividades diante de ataques cibernéticos, falhas tecnológicas, indisponibilidade de serviços, desastres e outros eventos relevantes.

O plano deverá identificar sistemas críticos, responsáveis, prioridades de recuperação e alternativas operacionais.

CAPÍTULO X — INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Artigo 26º — Definição de incidente

Considera-se incidente de segurança qualquer evento confirmado ou suspeito que comprometa, ou possa comprometer, a confidencialidade, integridade, disponibilidade ou autenticidade das informações e sistemas da WORDCOM.

Incluem-se, entre outros, ataques cibernéticos, invasões de contas, perda de equipamentos, vazamento de dados, fraudes eletrônicas, instalação de programas maliciosos e divulgação não autorizada de informações.

Artigo 27º — Comunicação de incidentes

Todo colaborador deverá comunicar imediatamente ao responsável pela Segurança da Informação qualquer incidente ou suspeita identificada.

A comunicação deverá conter, sempre que possível, descrição do ocorrido, data e horário, sistemas envolvidos e informações potencialmente afetadas.

É proibido ocultar deliberadamente incidentes ou destruir evidências relacionadas à ocorrência.

Artigo 28º — Resposta a incidentes

O tratamento dos incidentes observará as seguintes etapas:

1. Identificação: registro do incidente e avaliação preliminar da gravidade.
2. Contenção: adoção de medidas para impedir a continuidade ou ampliação dos danos.
3. Investigação: identificação das causas, dos sistemas atingidos e das informações comprometidas.
4. Recuperação: restauração segura dos sistemas e das operações afetadas.
5. Comunicação: avaliação das obrigações de notificação aos titulares, clientes, autoridades e demais envolvidos.
6. Remediação: correção das vulnerabilidades e implementação de medidas para prevenir recorrências.

Artigo 29º — Comunicação à Autoridade Nacional de Proteção de Dados

Nos casos de incidentes de segurança envolvendo dados pessoais que possam acarretar risco ou dano relevante aos titulares, a WORDCOM, quando atuar como controladora, deverá observar as obrigações de comunicação à ANPD e aos titulares, conforme a LGPD e a regulamentação vigente.

O prazo regulamentar geral é de três dias úteis, ressalvadas as disposições específicas aplicáveis. A avaliação deverá ser realizada com prioridade pelo responsável competente, com apoio jurídico quando necessário.

CAPÍTULO XI — INTELIGÊNCIA ARTIFICIAL E SERVIÇOS EM NUVEM

Artigo 30º — Utilização de inteligência artificial

A utilização de ferramentas de inteligência artificial nas atividades da WORDCOM deverá respeitar a confidencialidade, a proteção de dados pessoais, os direitos autorais e os compromissos contratuais.

É proibida a inserção de informações confidenciais, dados pessoais sensíveis, documentos estratégicos ou segredos comerciais em plataformas de inteligência artificial não autorizadas.

Conteúdos produzidos com auxílio de inteligência artificial deverão passar por revisão humana antes de sua utilização ou publicação, conforme sua finalidade e os riscos envolvidos.

Artigo 31º — Armazenamento em nuvem

O armazenamento e compartilhamento de arquivos em serviços de nuvem deverão ocorrer exclusivamente por plataformas autorizadas.

Os serviços deverão oferecer controles adequados de acesso, proteção das informações, recuperação de dados e gerenciamento de usuários.

A contratação de fornecedores de tecnologia deverá considerar os requisitos de segurança, privacidade e continuidade dos serviços.

CAPÍTULO XII — SEGURANÇA FÍSICA E DOCUMENTAL

Artigo 32º — Proteção dos ambientes

O acesso a salas técnicas, servidores, equipamentos de rede, arquivos confidenciais e demais áreas sensíveis deverá ser limitado a pessoas autorizadas.

Visitantes e prestadores de serviços deverão observar as regras de identificação e acompanhamento estabelecidas pela WORDCOM.

Artigo 33º — Documentos impressos

Documentos contendo informações confidenciais não deverão permanecer expostos em mesas, impressoras, salas de reunião ou ambientes acessíveis a pessoas não autorizadas.

Ao término das atividades, os colaboradores deverão guardar adequadamente documentos, equipamentos e mídias que contenham informações protegidas.

CAPÍTULO XIII — AUDITORIA, MONITORAMENTO E CONTROLES

Artigo 34º — Verificações periódicas

A WORDCOM deverá promover verificações periódicas dos controles de segurança, contemplando, entre outros:

- I. Revisão das permissões de acesso.
- II. Verificação das atualizações dos sistemas.
- III. Avaliação dos procedimentos de backup.
- IV. Análise dos incidentes registrados.
- V. Verificação da conformidade dos fornecedores críticos.
- VI. Avaliação dos riscos de segurança da informação.
- VII. Verificação da eficácia das ações corretivas.

Artigo 35º — Monitoramento dos recursos corporativos

A WORDCOM poderá realizar monitoramento proporcional e legítimo de seus recursos tecnológicos corporativos para fins de segurança, continuidade operacional, prevenção a fraudes e cumprimento de obrigações legais.

O monitoramento deverá respeitar a legislação, a privacidade, a transparência e os limites das finalidades informadas.

CAPÍTULO XIV — TREINAMENTO E CONSCIENTIZAÇÃO

Artigo 36º — Capacitação

Todos os colaboradores deverão receber treinamento inicial e participar de ações periódicas de conscientização sobre segurança da informação.

Os treinamentos deverão contemplar proteção de senhas, identificação de mensagens fraudulentas, uso seguro da internet, prevenção de vazamentos, proteção de dados pessoais e comunicação de incidentes.

Artigo 37º — Campanhas internas

A WORDCOM deverá promover orientações e comunicados internos para reforçar as práticas de segurança, especialmente diante da identificação de novas ameaças ou alterações relevantes nos procedimentos.

CAPÍTULO XV — DESCUMPRIMENTO E PENALIDADES

Artigo 38º — Infrações

O descumprimento desta Política poderá constituir infração às normas internas e ao Programa de Integridade Corporativa da WORDCOM.

Artigo 39º — Medidas disciplinares

As infrações serão apuradas mediante procedimento adequado, observadas a gravidade, as circunstâncias e a legislação aplicável.

Poderão ser adotadas medidas educativas, advertências, suspensão disciplinar quando cabível, desligamento, rescisão contratual e providências judiciais, conforme a natureza da infração.

A aplicação de penalidades deverá respeitar os direitos das pessoas envolvidas e as normas legais pertinentes.

CAPÍTULO XVI — DISPOSIÇÕES FINAIS

Artigo 40º — Integração com as políticas corporativas

Esta Política integra o conjunto de instrumentos de governança da WORDCOM, devendo ser aplicada de forma complementar ao Código de Ética, ao Programa de Integridade, aos procedimentos de Compliance e às demais normas internas.

Artigo 41º — Revisão e atualização

O presente Manual deverá ser revisado, no mínimo, anualmente, ou sempre que ocorrerem mudanças significativas nos sistemas, nas atividades empresariais, na legislação ou nos riscos de segurança.

Artigo 42º — Vigência

Esta Política entrará em vigor após aprovação formal pela Diretoria competente, devendo ser divulgada a todos os colaboradores e demais pessoas abrangidas.

ANEXO I — MATRIZ DE CONTROLES OPERACIONAIS

A seguinte matriz estabelece os controles mínimos propostos para implementação da Política.

Área de controle	Procedimento obrigatório	Frequência proposta
Contas e acessos	Revisão de usuários e permissões	Trimestral
Senhas e autenticação	Verificação da adoção de MFA	Trimestral
Backups	Verificação de execução e falhas	Diária, nos sistemas críticos
Restauração de dados	Testes de recuperação	Trimestral
Equipamentos	Verificação de atualizações e proteção	Mensal
Fornecedores de tecnologia	Avaliação de riscos e conformidade	Anual
Dados pessoais	Revisão das atividades de tratamento	Anual e quando houver alterações relevantes
Incidentes	Registro e tratamento de ocorrências	Imediatamente após identificação
Treinamentos	Capacitação e conscientização	Anual e na admissão
Política de Segurança	Revisão geral e aprovação	Anual

ANEXO II — PLANO DE IMPLANTAÇÃO EM 90 DIAS

Todos os colaboradores aderem ao plano

1. Primeiros 15 dias — Governança

Aprovação do Manual, designação dos responsáveis, definição do canal para incidentes e comunicação interna da Política.

2. Até 30 dias — Diagnóstico

Inventário dos equipamentos, sistemas, contas corporativas, bases de dados e identificação das vulnerabilidades prioritárias.

3. Até 45 dias — Proteção

Revisão das senhas e acessos, implementação de autenticação multifator e verificação dos mecanismos de backup.

4. Até 60 dias — Padronização

Formalização dos procedimentos de armazenamento, compartilhamento, uso de dispositivos e resposta a incidentes.

5. Até 75 dias — Capacitação

Treinamento dos colaboradores, assinatura dos Termos de Ciência e orientação dos gestores.

6. Até 90 dias — Verificação

Testes de recuperação, avaliação dos controles implantados e apresentação do primeiro relatório de segurança à Diretoria.

ANEXO III — TERMO DE CIÊNCIA E COMPROMISSO

Todos os colaboradores aderem ao programa

TERMO DE CIÊNCIA E COMPROMISSO

Política de Segurança da Informação — WORDCOM

Declaro que recebi, li e compreendi o Manual da Política de Segurança da Informação da WORDCOM, comprometendo-me a cumprir integralmente suas normas, procedimentos e orientações.

Comprometo-me a preservar a confidencialidade das informações às quais tiver acesso em razão das minhas atividades profissionais, utilizar adequadamente os recursos tecnológicos disponibilizados e comunicar imediatamente qualquer suspeita de incidente de segurança.

Reconheço que o acesso a informações corporativas deverá ocorrer exclusivamente para finalidades profissionais autorizadas e que o descumprimento das normas poderá resultar nas medidas previstas na legislação, nos contratos e nas políticas internas aplicáveis.

O dever de confidencialidade permanecerá após o encerramento do meu vínculo com a WORDCOM, nos limites legais e contratuais pertinentes.

Nome: _____

Cargo/Função: _____

Departamento: _____

Data: ____ / ____ / ____

Assinatura: _____