política de segurança da informação

CONTROLE DO DOCUMENTOS	
Código do Documento	007-19-PSI
Data de Criação da Política	09/02/2019
Versão atual	Versão 3
Data da Versão Atual	25/06/2026
Diretoria Responsável (Aprovação)	Recursos Humanos
Periodicidade de Revisão	Anual

índice

1. objetivo

Esta Política de Segurança da Informação tem por objetivo estabelecer as diretrizes para a promoção, implementação, manutenção e melhoria contínua do Sistema de Segurança da Informação da Weplace Consultoria em Recursos Humanos Ltda. (“Weplace”), assegurando a confidencialidade, a integridade e a disponibilidade das informações sob sua responsabilidade.

A segurança da informação não se restringe a sistemas computacionais, informações eletrônicas ou meios de armazenamento digital. O conceito aplica-se a todos os formatos de tratamento de informações e de dados pessoais, inclusive em meios físicos, desde os estudos e projetos iniciais até a efetiva execução das operações.

2. abrangência

As disposições desta Política aplicam-se a todos os sócios, administradores e colaboradores da Weplace (empregados CLT, estagiários, aprendizes e prestadores de serviço), bem como a terceiros que tenham contato com informações produzidas ou custodiadas pela empresa.

Equiparam-se aos colaboradores, para os fins desta Política, os parceiros de negócios (Business Feeders, Conselheiros, Empresas Parceiras e Advisors) e os assessores externos (advogados, auditores e consultores), os quais deverão firmar compromisso de confidencialidade ao serem contratados. Onde se lê “sócio” e/ou “colaborador”, incluem-se todos os parceiros mencionados.

3. base legal e normativa

Esta Política fundamenta-se na legislação e nas normas técnicas aplicáveis, em especial:

a) Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD) e orientações da Autoridade Nacional de Proteção de Dados (ANPD);

b) Normas ABNT NBR ISO/IEC 27001 e ISO/IEC 27002 — sistemas de gestão e controles de segurança da informação;

c) Código Penal — art. 154 (violação de segredo profissional) e art. 307 (falsa identidade);

d) Lei nº 9.279/1996 — art. 195 (crime de concorrência desleal);

e) Medida Provisória nº 2.200-2/2001 — validade jurídica das assinaturas eletrônicas; e

f) demais legislações e normas internas correlatas, incluindo a Política de Resposta a Incidentes da Weplace.

4. definições

Para os fins desta Política, aplicam-se as seguintes definições:

a) Ativo: todo elemento que agregue valor ao negócio — informação digital ou física, hardware, software, pessoa ou ambiente físico — cuja quebra de confidencialidade, integridade ou disponibilidade traga prejuízo financeiro ou reputacional.

b) Informação: conteúdo que possua valor (financeiro, tecnológico, reputacional, arquivístico, entre outros) para a empresa, independentemente do meio de armazenamento (físico, impresso, digital, áudio, vídeo etc.).

c) Dados Pessoais: qualquer informação relacionada a pessoa natural identificada ou identificável, isolada ou em combinação com outras informações tratadas.

d) Segurança da Informação (SI): proteção da informação contra ameaças, com a finalidade de garantir a continuidade do negócio, reduzir riscos e maximizar o retorno dos investimentos e as oportunidades.

e) Confidencialidade: limitação do acesso à informação às pessoas autorizadas pelo seu proprietário.

f) Integridade: garantia de que a informação mantenha as características originais estabelecidas pelo seu proprietário, com controle de mudanças ao longo de seu ciclo de vida.

g) Disponibilidade: garantia de que a informação esteja disponível para uso legítimo pelos usuários autorizados sempre que necessário.

h) Incidente de Segurança da Informação: qualquer destruição, perda, modificação, divulgação não autorizada ou acesso indevido, acidental ou ilícito, que envolva dados ou informações — por exemplo, perda ou roubo de dados ou hardware, acesso não autorizado e tentativas fraudulentas de obtenção de informações (phishing).

i) Informações Confidenciais: todas as informações verbais e/ou escritas, não públicas, referentes aos negócios, operações, atividades e planos da Weplace, conforme detalhado na Seção 7.

5. princípios da segurança da informação

A gestão da segurança da informação na Weplace orienta-se pelos seguintes princípios:

a) Confidencialidade — restrição do acesso à informação às pessoas autorizadas;

b) Integridade — manutenção das características originais da informação e controle de seu ciclo de vida;

c) Disponibilidade — garantia de acesso à informação pelos usuários legítimos sempre que necessário;

d) Mínimo Privilégio (Least Privilege) e Necessidade de Conhecer (Need to Know) — concessão do menor nível de acesso necessário ao desempenho da função;

e) Legalidade, responsabilidade e transparência no tratamento das informações; e

f) Melhoria contínua dos processos e controles de segurança.

6. a segurança da informação na weplace

O sucesso da Weplace fundamenta-se em seus valores, na qualidade dos serviços prestados e nas informações e conhecimentos que gera e mantém. Todas as informações existentes em seus sistemas e processos de trabalho, bem como aquelas geradas em decorrência de suas operações, são confidenciais e essenciais à manutenção da excelência dos serviços.

O fluxo e o compartilhamento de informações entre sócios, colaboradores e parceiros de negócios são vitais para a evolução da Weplace; contudo, é imprescindível preservar sua confidencialidade, de modo a evitar que o uso indevido ou não autorizado por terceiros e concorrentes coloque a empresa em desvantagem competitiva, afete sua imagem ou gere prejuízos.

As informações confidenciais constituem diferencial competitivo, possuem alto valor econômico e integram o patrimônio intelectual da Weplace, estando sujeitas a constantes ameaças internas e externas. Por isso, devem ser manuseadas, protegidas e armazenadas de forma segura.

A segurança da informação deve ser parte do cotidiano, da cultura de trabalho e do relacionamento da Weplace com todos ao seu redor — sócios, colaboradores, parceiros, clientes, candidatos, fornecedores e autoridades, consolidando sua imagem de qualidade, inovação, eficiência e profissionalismo. A Política observa a Lei nº 13.709/2018 (LGPD) e busca seguir normas rigorosas de proteção de dados pessoais.

7. informações confidenciais

São consideradas Informações Confidenciais (“Informações Confidenciais”, “Informações” ou “Informação”) todas as informações verbais e/ou escritas que não sejam de conhecimento público, referentes aos negócios, operações, atividades e planos da Weplace. Incluem-se, sem limitação: dados e relações de clientes; dados pessoais de executivos e candidatos; relatórios de candidatos e registros de entrevistas; relatórios de projetos, apresentações, manuais, guias, esboços, modelos, amostras, materiais e estudos; contratos e atas internas; programas e documentação de computador; informações financeiras, operacionais, econômicas, técnicas e jurídicas; planos comerciais, estratégicos, de marketing e de tecnologia; bem como know-how e quaisquer cópias ou registros contidos em qualquer meio físico ou eletrônico.

Todos os sócios e colaboradores devem observar os procedimentos internos de coleta de dados pessoais, em conformidade com a LGPD.

Estão isentas da obrigação de confidencialidade as determinações decorrentes de lei ou emanadas do Poder Judiciário. O sócio ou colaborador instado a revelar informação a autoridade legalmente investida deverá notificar prontamente a Diretoria Administrativa Financeira, para a adoção das medidas legais e administrativas cabíveis à limitação da revelação.

8. proteção da informação

Toda informação é um ativo importante, valioso e essencial à condução das operações e à continuidade da Weplace, devendo ser adequadamente protegida e manuseada, independentemente da forma como é apresentada ou compartilhada.

A informação deve ser utilizada exclusivamente para a finalidade autorizada e em benefício da Weplace. A modificação, a divulgação pública ou a terceiros não autorizados e a destruição não autorizada — decorrentes de erro, fraude, vandalismo, espionagem ou sabotagem — podem causar danos aos negócios e à imagem da empresa.

É diretriz da administração que toda informação seja protegida contra riscos e ameaças que possam comprometer sua confidencialidade, integridade ou disponibilidade.

9. definição de responsabilidades

Todas as pessoas vinculadas à Weplace estão comprometidas com a aplicação, a manutenção e a melhoria dos protocolos estabelecidos nesta Política. As responsabilidades específicas, conforme o papel desempenhado, são as seguintes:

a) Gerente do Programa de Segurança da Informação (Gerente de SI): planeja e implementa, em conjunto com as demais áreas, os requisitos desta Política, coordenando as tarefas necessárias à sua efetividade. O Gerente de SI é designado pela Diretoria.

b) Gestores das áreas: responsáveis por (i) implementar as diretrizes desta Política nos processos e projetos sob sua responsabilidade; (ii) orientar e acompanhar a aplicação dos procedimentos recomendados pelo Gerente de SI; (iii) preencher, com os colaboradores, os relatórios e questionários solicitados; e (iv) comunicar ao Gerente de SI as questões relevantes trazidas pelos colaboradores.

c) Colaboradores: devem seguir os termos desta Política e colaborar com sua aplicação, notificar quaisquer fragilidades ou eventos que comprometam a segurança das informações e consultar o gestor da área sempre que houver dúvida em matéria de segurança da informação.

10. programa de segurança da informação

O Programa de Segurança da Informação da Weplace foi concebido de acordo com as melhores práticas e normas de reconhecimento internacional, elegendo como prioridades a integridade das informações disponibilizadas a seus clientes e a disponibilidade de seus sistemas.

As disposições deste Programa orientam o planejamento, o tratamento e a análise das rotinas de segurança da informação, a fim de elevar seu grau de maturidade por meio de controles específicos sobre os ativos de dados.

Para mitigar os riscos a que estão expostos os ativos de segurança da informação, a Weplace aplica os controles descritos nas seções seguintes. Os comprovantes das rotinas podem ser obtidos junto ao Gerente de SI.

11. controles relativos aos colaboradores

A Weplace adota os seguintes controles relacionados aos colaboradores:

- Treinamento periódico de todos os colaboradores quanto aos protocolos de segurança da informação e de proteção de dados.
- Conscientização dos colaboradores, especialmente os diretamente envolvidos no tratamento de dados, sobre as obrigações da LGPD e as orientações da ANPD.
- Manutenção de ambiente organizacional que incentive usuários, clientes e colaboradores a reportar incidentes e vulnerabilidades detectados.
- Garantia de que os colaboradores conheçam os controles de segurança dos sistemas de TI do trabalho diário, os incidentes corriqueiros (vírus e phishing), a guarda de documentos físicos com dados pessoais em gavetas preferencialmente trancadas (se necessário), pois atualmente trabalhamos com arquivos em 100% formato digital, a proibição de compartilhamento de logins e senhas e a importância do bloqueio dos computadores ao se afastarem da estação de trabalho.

12. gerenciamento de acesso e identificação

Cada Sistema de Informação, diretório de rede e banco de dados da Weplace possui um gestor responsável por definir sua correta utilização e por autorizar os acessos, observada esta Política. A concessão de acessos cabe ao gestor responsável e à Diretoria Administrativa, segundo a regra do mínimo acesso necessário ao desempenho da função; acessos desnecessários ou com poder excessivo devem ser imediatamente revogados.

O usuário é integralmente responsável pela posse e correta utilização de suas senhas e autorizações de acesso, que são pessoais e intransferíveis, bem como pelas ações delas decorrentes. A Weplace adota os seguintes controles de acesso e identificação:

- Gestão de perfis de acesso a softwares e bancos de dados, com níveis de permissão definidos por usuário.
- Protocolo de segurança da informação para admissão e desligamento de colaboradores.
- Padrão mínimo de complexidade de senhas e gerenciamento de senhas, vedados o uso de senhas padrão de fornecedores e a reutilização de senhas antigas.
- Proibição do compartilhamento de contas e senhas entre colaboradores.
- Adoção dos princípios Least Privilege e Need to Know na autorização de qualquer acesso a sistemas e informações.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos acessíveis, baseadas em informações pessoais ou compostas por combinações óbvias. Após três tentativas de acesso incorretas, a conta é bloqueada, cabendo o desbloqueio à área Administrativa. A periodicidade máxima para troca de senhas é de 60 dias — reduzida a 45 dias para sistemas críticos —, vedada a repetição das três últimas senhas. Os dispositivos de identificação devem estar associados a uma pessoa física e não podem ser compartilhados, sendo o uso de identificação de terceiro crime de falsa identidade (art. 307 do Código Penal).

13. uso dos meios eletrônicos, monitoramento e auditoria

A utilização dos meios eletrônicos de propriedade da Weplace — acesso à internet, telefonia fixa e móvel, correio eletrônico, dispositivos móveis, softwares, hardwares, computadores, tablets, smartphones, pen drives, discos externos, armazenamento em nuvem, mídias e demais dispositivos — deve destinar-se exclusivamente ao exercício das atividades profissionais.

Para garantir a integridade e o sigilo das informações, a Weplace pode monitorar qualquer dado transmitido ou residente em seus meios eletrônicos. O correio eletrônico, o acesso à internet e quaisquer equipamentos ou dispositivos pessoais conectados aos meios eletrônicos da empresa poderão ser monitorados e auditados, não havendo expectativa de privacidade em seu uso.

O monitoramento e a auditoria poderão ocorrer por meio de análises físicas, rastreamentos e registros de auditoria, sem aviso prévio, para investigações internas ou cumprimento de medidas judiciais. Para tanto, a Weplace poderá implantar sistemas de rastreamento e monitoramento, realizar inspeções físicas nos meios eletrônicos de sua propriedade e instalar sistemas de proteção preventivos e detectáveis.

14. correio eletrônico corporativo (e-mail)

O correio eletrônico da Weplace destina-se a fins corporativos e às atividades profissionais. O uso para fins pessoais é permitido com parcimônia e bom senso, desde que não prejudique a empresa nem impacte o tráfego da rede. É vedado aos sócios e colaboradores:

- enviar informações confidenciais para endereços eletrônicos pessoais, sob qualquer pretexto;
- enviar mensagens não solicitadas a múltiplos destinatários, salvo para atender a interesse legítimo da empresa;
- utilizar o endereço eletrônico ou o nome de usuário de terceiro sem autorização;
- enviar mensagens que exponham a Weplace a ações civis ou criminais;
- divulgar informações sem autorização expressa da empresa;
- falsificar dados de endereçamento ou adulterar cabeçalhos para ocultar a identidade de remetentes ou destinatários;
- apagar mensagens relevantes quando a empresa estiver sujeita a auditoria ou investigação; e
- produzir, transmitir ou divulgar mensagens com ameaças eletrônicas, arquivos perigosos ou tentativas de acesso não autorizado a sistemas.

As mensagens devem conter a assinatura padrão da empresa, elaborada pela área Administrativa, com nome do colaborador, função ou área, telefone(s), correio eletrônico e aviso de confidencialidade. Os endereços eletrônicos de colaboradores desligados poderão permanecer ativos pelo tempo necessário ao redirecionamento de mensagens, a critério da Diretoria Administrativa.

15. acesso à internet

A Weplace espera de seus sócios e colaboradores comportamento ético e profissional no uso da internet. Embora a conexão ofereça benefícios, também expõe a empresa a riscos significativos à integridade e ao sigilo das informações.

Toda informação acessada, transmitida, recebida ou produzida via internet conectada aos meios eletrônicos da Weplace está sujeita a monitoramento e auditoria. A empresa reserva-se o direito de analisar e bloquear qualquer arquivo, site, e-mail, domínio ou aplicação para assegurar a conformidade com esta Política.

É vedado o uso da internet para atividades ilícitas e o download ou a distribuição de softwares ou dados pirateados. O descumprimento poderá ensejar medidas administrativas, trabalhistas, cíveis e criminais, com a cooperação da Weplace com as autoridades competentes.

16. dispositivos móveis, portáteis e acesso remoto

A Weplace permite a utilização de dispositivos portáteis — notebooks, smartphones e tablets — para facilitar a mobilidade e o fluxo de informações, reservando-se o direito de inspecioná-los, monitorá-los e auditá-los a qualquer tempo, sem aviso prévio.

Os colaboradores são responsáveis por não instalar ou utilizar programas não autorizados nesses dispositivos e, em caso de furto ou roubo, devem notificar imediatamente a Diretoria Administrativa e registrar boletim de ocorrência. Documentos essenciais devem ser salvos nas pastas de rede da Weplace, pois arquivos armazenados localmente não têm garantia de backup.

As normas desta Política aplicam-se também aos acessos remotos realizados por meio dos meios eletrônicos da Weplace. Em caso de desligamento, o colaborador deve entregar os dispositivos móveis à Diretoria Administrativa para a remoção das informações e dos aplicativos relacionados à empresa.

17. segurança dos dados pessoais e lgpd

A Weplace coleta, processa e armazena apenas os dados pessoais necessários à finalidade pretendida, adotando o princípio da minimização. Os colaboradores são orientados a não desativar as configurações de segurança dos dispositivos de trabalho e a evitar a transferência de dados pessoais de dispositivos corporativos para dispositivos pessoais de armazenamento externo.

A Weplace mantém o Registro das Operações de Tratamento de Dados Pessoais (RoPA) e adota medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou tratamento inadequado ou ilícito.

As informações e os dados pessoais tratados são armazenados em ambientes reconhecidos pelo alto nível de segurança — como Microsoft SharePoint, Clockwork e Acronis Cyber Cloud — e em servidores internos, observados os padrões de segurança de mercado, com criptografia de senha do usuário, rotação de senhas de acesso ao banco de dados, realização periódica de backups e acesso controlado.

18. revisão e gestão de documentos

A Weplace mantém rotinas de revisão e gestão dos documentos relacionados à segurança da informação, entre as quais:

- Revisão periódica dos Termos de Uso e da Política de Privacidade da plataforma da Weplace.
- Disponibilização do Manual de Boas Práticas para o Tratamento de Dados Pessoais aos colaboradores.
- Gestão do recebimento de denúncias e da apuração de Incidentes de Segurança da Informação por meio do canal segurancadainformacao@weplace.com.br, conforme a Política de Resposta a Incidentes.
- Estudo das relações contratuais firmadas pela Weplace, com avaliação dos riscos à segurança da informação nelas contidos.
- Manutenção de contratos com cláusulas de proteção de dados pessoais, disciplinando o compartilhamento e o tratamento conforme a posição dos agentes de tratamento.
- Assinatura de Termos de Confidencialidade (Non-Disclosure Agreement – NDA) pelos colaboradores da Weplace.

19. monitoramento

A rotina de verificação da aplicação dos protocolos de segurança da informação ocorre semestralmente, envolvendo as pessoas e organizações vinculadas à Weplace, e pode incluir o envio de questionários a fornecedores, a disponibilização de manuais de orientação, a assinatura de termos vinculantes e/ou treinamentos, entre outras medidas consideradas eficazes. Para a verificação dos controles de Incidentes de Segurança da Informação, observa-se a Política de Resposta a Incidentes da Weplace.

20. melhoria contínua

A fim de proporcionar maior segurança no desenvolvimento de suas atividades de negócio, toda a organização está comprometida com a melhoria contínua de seus processos. A elaboração desta Política, bem como o projeto de conformidade à Lei Geral de Proteção de Dados, representam os melhores esforços da Weplace para entregar a seus clientes e parceiros informações precisas e seguras.

21. violações e gestão de consequências

As violações a esta Política devem ser comunicadas aos sócios e à Diretoria Administrativa Financeira da Weplace e serão investigadas para a definição das medidas punitivas e corretivas cabíveis. Constituem exemplos de violações sujeitas a sanção:

- divulgação de informações a terceiros não autorizados;
- uso de informações para benefício próprio;
- recusa em entregar informações ao deixar a empresa;
- uso de senha de outro sócio ou colaborador;
- compartilhamento de acesso à caixa de e-mail;
- uso ilegal de software; e
- introdução de vírus ou tentativa de acesso não autorizado a sistemas.

A não conformidade com esta Política poderá resultar em responsabilização civil e, quando aplicável, em denúncia criminal, bem como em exclusão por justa causa da sociedade, no caso de sócio, ou em demissão por justa causa, no caso de colaborador.

22. documentos de referência

Esta Política foi construída com base nos seguintes documentos de referência:

- Norma ABNT NBR ISO/IEC 27001 — Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos;
- Norma ABNT NBR ISO/IEC 27002 — Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação;
- Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD); e
- Política de Resposta a Incidentes da Weplace.

23. revisão da política

Esta Política será revisada anualmente ou sempre que houver alteração legal, regulatória ou organizacional relevante. Toda alteração deverá ser registrada em controle de versões, com indicação de data, responsável, revisor, aprovador e sumário das alterações, e submetida à revisão e à aprovação da Diretoria para sua validade.

24. disposições gerais

Os casos omissos e as dúvidas decorrentes desta Política serão dirimidos pela Diretoria da Weplace, com o apoio do Gerente de Segurança da Informação. Esta Política entra em vigor na data de sua aprovação e revoga as versões anteriores.

25. termo de ciência e conhecimento

Declaro que recebi e li a Política de Segurança da Informação da Weplace, compreendendo suas diretrizes, normas e procedimentos, bem como a importância da segurança da informação para a proteção dos dados da empresa, de seus clientes e parceiros.

Comprometo-me a cumprir rigorosamente as disposições desta Política e a respeitar a confidencialidade das informações a que tiver acesso no exercício de minhas funções. Reconheço que a violação das normas aqui estabelecidas poderá resultar em sanções administrativas, trabalhistas, cíveis e/ou criminais, conforme previsto nesta Política.

Estou ciente de que a Weplace se reserva o direito de monitorar e auditar o uso de seus meios eletrônicos e de comunicação, não havendo expectativa de privacidade em tal uso, e de que, ao deixar a empresa, devo devolver todos os dispositivos e informações pertencentes à Weplace.

São Paulo, 26 de junho de 2026.

Nome:

Cargo:

CPF:

Assinatura: