Planning

TI · V2.0



POLÍTICA CORPORATIVA · VERSÃO 2.0

Política de Tecnologia da Informação

Diretrizes corporativas para a proteção dos ativos de informação, a conformidade com a LGPD e a prevenção de responsabilidade legal para todos os usuários.

Planning Engenharia · A Engenharia do Resultado
www.planningengenharia.com.br

TECNOLOGIA · SEGURANÇA DA INFORMAÇÃO · V2.0

Política de Tecnologia da Informação

1 Resumo

A Política de Tecnologia da Informação é o documento que orienta e estabelece as diretrizes corporativas da Planning para a proteção dos ativos de informação, a conformidade com a legislação de proteção de dados pessoais e a prevenção de responsabilidade legal para todos os usuários. Os itens contidos neste documento devem, portanto, ser cumpridos e aplicados em todas as áreas da empresa.

2 Abrangência

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como pelos prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte, inclusive aos dados pessoais e às informações confidenciais de clientes da Planning tratados no âmbito da prestação de serviços.

3 Objetivos

São objetivos desta Política de TI:

- Estabelecer diretrizes que permitam aos colaboradores seguirem padrões de comportamento relacionados à segurança da informação, adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo;
- Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento;
- Assegurar a conformidade da Planning com a Lei Geral de Proteção de Dados Pessoais (LGPD) e demais normas aplicáveis ao tratamento de dados pessoais, próprios e de clientes.

Preservar as informações da Planning e de seus clientes quanto à:

> **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;

> **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário e conforme termos contratuais;

Sigilo: garantia de que a informação fique exclusivamente com quem de direito, não tecendo comentários ou demonstração de documentos de caráter sigiloso.

4 Proteção de Dados Pessoais (LGPD)

A Planning trata dados pessoais de colaboradores, clientes, fornecedores e terceiros em conformidade com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais — LGPD) e as regulamentações da Autoridade Nacional de Proteção de Dados (ANPD).

- Todo tratamento de dados pessoais deve estar fundamentado em uma base legal prevista no art. 7º da LGPD (execução de contrato, cumprimento de obrigação legal, legítimo interesse, consentimento, entre outras);
- A coleta e o uso de dados pessoais devem observar os princípios de finalidade, adequação, necessidade, transparência e segurança previstos no art. 6º da LGPD;
- A Planning mantém um Encarregado pelo Tratamento de Dados Pessoais (Encarregado de Dados/DPO), responsável por orientar colaboradores, atender solicitações de titulares e ser o canal de comunicação com a ANPD;
- Qualquer incidente de segurança que possa acarretar risco ou dano relevante a titulares de dados pessoais deve ser comunicado imediatamente ao Encarregado de Dados, que avaliará a necessidade de comunicação à ANPD e aos titulares, observado o prazo regulamentar de até 3 (três) dias úteis a contar da ciência do incidente, nos termos do Regulamento de Comunicação de Incidente de Segurança (Resolução CD/ANPD nº 15/2024);
- Nenhuma informação, dado pessoal ou registro de monitoramento poderá ser tornado público ou compartilhado com terceiros sem prévia avaliação jurídica e do Encarregado de Dados, exceto por determinação judicial ou obrigação legal expressa;
- Solicitações de titulares de dados (acesso, correção, eliminação, portabilidade, entre outras previstas no art. 18 da LGPD) devem ser encaminhadas ao Encarregado de Dados e respondidas nos prazos legais.

5 Das Responsabilidades

Dos Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição. Será de inteira responsabilidade de cada colaborador todo prejuízo ou dano que vier a sofrer ou cau-

sar à Planning e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Dos Gestores de Pessoas e/ou Processos

São responsabilidades dos gestores Planning:

- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão;
- Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade pelo cumprimento da política;
- Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligados, sobre todos os ativos de informação da Planning e de seus clientes;
- Antes de conceder acesso às informações da instituição ou de seus clientes, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Do Encarregado de Dados (DPO)

- Atuar como canal de comunicação entre a Planning, os titulares de dados e a ANPD;
- Orientar colaboradores quanto às práticas de tratamento de dados pessoais;
- Avaliar e coordenar a comunicação de incidentes de segurança envolvendo dados pessoais, nos prazos legais;
- Aprovar, previamente, qualquer divulgação, compartilhamento ou publicização de informações obtidas por meio de sistemas de monitoramento e auditoria.

Da Área de Tecnologia da Informação

- Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais;
- Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta a incidentes;
- Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requisitos de segurança estabelecidos por esta política, incluindo autenticação multifator (MFA) obrigatória;
- Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando necessário para a execução de atividades operacionais sob sua

responsabilidade, como manutenção de computadores, realização de cópias de segurança, auditorias ou testes no ambiente;

- Administrar, proteger e testar periodicamente as cópias de segurança (backup) dos e-mails, dos drives/OneDrive dos colaboradores e dos demais programas e dados relacionados aos processos críticos e relevantes para a Planning, conforme detalhado na seção Backup, Continuidade e Recuperação;
- Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela;
- Informar previamente o gestor da informação sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes do descarte definitivo pelo custodiante;
- Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não sejam removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário;
- Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e demais ativos de informação a um responsável identificável como pessoa física, sendo que os logins individuais de funcionários são de responsabilidade do próprio funcionário e os logins de terceiros são de responsabilidade do gestor da área contratante;
- Proteger continuamente todos os ativos de informação da empresa contra código malicioso, garantindo que novos ativos só entrem em produção livres de código malicioso e/ou indesejado;
- Garantir que não sejam introduzidas vulnerabilidades no ambiente de produção em processos de mudança, sendo recomendável a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros;
- Definir regras formais para instalação de software e hardware em ambiente corporativo e educacional, exigindo seu cumprimento dentro da empresa;
- Realizar auditorias periódicas de configurações técnicas e análise de riscos, incluindo os ambientes de nuvem (Microsoft 365, Power Platform e demais plataformas contratadas);
- Responsabilizar-se pelo uso, manuseio e guarda de assinaturas e certificados digitais;
- Garantir, da forma mais rápida possível e mediante solicitação formal do RH ou do gestor, o bloqueio de acesso de usuários por desligamento, incidente, investigação ou outra situação que exija medida restritiva para salvaguardar os ativos da empresa;
- Monitorar o ambiente de TI, gerando indicadores e históricos de incidentes de segurança (vírus, acessos indevidos e afins) e de atividade dos colaboradores em redes externas e internet, observados os prazos de retenção definidos nesta política e a legislação aplicável;
- Comunicar imediatamente ao Encarregado de Dados qualquer incidente que envolva dados pessoais, para fins de avaliação quanto à comunicação à ANPD e aos titulares.

6 Do Monitoramento e da Auditoria do Ambiente

Os equipamentos, sistemas, ferramentas de comunicação (incluindo e-mail corporativo, aplicativos de mensageria de uso profissional e demais recursos de TI) fornecidos pela Planning são ferramentas de trabalho, de propriedade da instituição, destinadas exclusivamente ao uso profissional. O colaborador não possui expectativa de privacidade quanto ao conteúdo armazenado, transmitido ou recebido por meio desses recursos.

Para garantir as regras mencionadas nesta política, a Planning poderá:

- Auditar e acessar, a qualquer momento e sem aviso prévio, o conteúdo das caixas postais corporativas e demais ferramentas de trabalho, para fins de segurança, auditoria e cumprimento desta política;
- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede — a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso;
- Manter os registros de conexão e de acesso a aplicações pelos prazos mínimos previstos na Lei nº 12.965/2014 (Marco Civil da Internet) — um ano para registros de conexão e seis meses para registros de acesso a aplicações — podendo estendê-los quando necessário para fins de auditoria, segurança ou obrigação legal.

As informações obtidas pelos sistemas de monitoramento e auditoria somente poderão ser tornadas públicas ou compartilhadas com terceiros mediante exigência judicial, solicitação da diretoria, ou após prévia avaliação e aprovação conjunta da área de TI, do Jurídico e do Encarregado de Dados, de modo a assegurar o cumprimento da LGPD.

7 Correio Eletrônico

É proibido aos colaboradores o uso do correio eletrônico da Planning para:

- Enviar mensagens pelo endereço de outro departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem que torne seu remetente e/ou a Planning vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal do proprietário desse ativo de informação;

- Falsificar informações de endereçamento ou adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando a Planning estiver sujeita a algum tipo de investigação;
- Produzir, transmitir ou divulgar mensagem que vise vigiar secretamente ou assediar outro usuário, acessar informações confidenciais sem autorização explícita do proprietário, causar prejuízo a qualquer pessoa, incluir imagens criptografadas ou mascaradas, ou que tenha conteúdo impróprio, obsceno ou ilegal.

Todas as caixas de e-mail corporativas e os drives (OneDrive/SharePoint) dos colaboradores estão incluídos na rotina de backup mantida pela Planning, conforme descrito na seção Backup, Continuidade e Recuperação.

8 Internet

Todas as regras atuais da Planning visam basicamente o desenvolvimento de um comportamento ético, profissional e seguro no uso da internet. Qualquer informação acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet ou em serviços de nuvem contratados pela empresa, visando assegurar o cumprimento desta política. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e autorização, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor.

O uso de qualquer recurso para atividades ilícitas poderá acarretar ações administrativas e as penalidades decorrentes de processos civil e criminal, inclusive nos termos da Lei nº 12.737/2012, sendo que, nesses casos, a instituição cooperará ativamente com as autoridades competentes.

9 Nuvem, Ferramentas Colaborativas e Inteligência Artificial

A operação de TI da Planning é baseada, majoritariamente, em ambiente de nuvem (Microsoft 365, Power Platform e Dataverse) e em plataformas complementares de BI. Esta seção estabelece as regras específicas para esses ambientes.

- O acesso aos ambientes de nuvem corporativos é protegido por autenticação multifator (MFA) obrigatória, fornecida pela Microsoft, para todos os colaboradores, sem exceção;
- O compartilhamento externo de arquivos, pastas e relatórios (SharePoint, OneDrive, Power BI) deve seguir o princípio do menor privilégio, restringindo o acesso apenas às pessoas e organizações autorizadas para a finalidade específica;

- Para clientes que não possuem licença de Power BI, o acesso a relatórios deve ser disponibilizado exclusivamente por meio de plataforma de controle de acesso homologada pela Planning, vedado o compartilhamento de relatórios por links públicos ou métodos não controlados;
- É vedado o uso de ferramentas de inteligência artificial generativa não homologadas pela Planning (ex.: assistentes de IA públicos e gratuitos) para processar, resumir, traduzir ou de qualquer forma tratar dados pessoais, dados confidenciais ou informações de clientes;
- Ferramentas de IA homologadas pela Planning e integradas ao ambiente corporativo (ex.: Copilot no Microsoft 365) podem ser utilizadas para atividades de trabalho, observados os mesmos princípios de confidencialidade, minimização de dados e finalidade aplicáveis aos demais sistemas corporativos;
- Qualquer novo serviço de nuvem, integração ou aplicação que venha a tratar dados pessoais ou informações de clientes deve ser previamente avaliado pela área de TI e pelo Encarregado de Dados.

10 Identificação

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra. O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 — falsa identidade) e pode configurar, ainda, invasão de dispositivo informático nos termos da Lei nº 12.737/2012. Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Todos os dispositivos de identificação utilizados na Planning, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos, têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

Ainda sobre a identificação, segue:

- O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal);
- Todo e qualquer dispositivo de identificação pessoal não poderá ser compartilhado com outras pessoas em nenhuma hipótese;
- O acesso aos sistemas e ambientes corporativos é protegido por autenticação multifator (MFA) obrigatória, fornecida pela Microsoft, aplicável a todos os colaboradores e prestadores de serviço com acesso a ambientes corporativos;
- A Planning não exige a troca periódica obrigatória de senha. A alteração de senha ocorre a pedido do próprio colaborador ou em caso de esquecimento, mediante requisição formal ou comparecimento à área técnica responsável para cadastro de uma nova senha;

- Os usuários devem alterar a própria senha sempre que suspeitarem que terceiros obtiveram acesso indevido ao seu login/senha;
- Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Assim que um usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá comunicar imediatamente o fato ao Departamento de Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica a usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como a usuários de testes e situações similares.

Nota de revisão: a exigência de troca de senha a cada 180 dias, prevista na versão anterior desta política, foi removida. A prática de rotação forçada de senha sem indício de comprometimento é hoje desaconselhada por referências técnicas como o NIST SP 800-63B, que recomenda priorizar autenticação multifator e monitoramento de comprometimento em vez de expiração periódica — controle já adotado pela Planning por meio do MFA obrigatório da Microsoft.

11 Classificação da Informação

Toda informação produzida, recebida ou custodiada pela Planning deve ser classificada por seu proprietário/gestor em uma das categorias abaixo, de forma a orientar as regras de acesso, armazenamento e compartilhamento aplicáveis:

A tabela a seguir resume as categorias adotadas:

Classificação	Descrição	Exemplo
Pública	Pode ser divulgada livremente, sem restrição.	Materiais institucionais, site, propostas de marketing.
Interna	Restrita aos colaboradores da Planning.	Procedimentos internos, comunicados corporativos.
Confidencial	Restrita a colaboradores e terceiros autorizados por necessidade de acesso.	Contratos, dados de RH, informações financeiras.
Restrita	Acesso limitado a pessoas nominalmente autorizadas; inclui dados pessoais sensíveis e informações operacionais de clientes.	Dados de sistemas de clientes, dados pessoais sensíveis, credenciais de acesso.

12 Dados de Clientes e Confidencialidade Contratual

Considerando que a Planning presta serviços a clientes de grande porte, com acesso frequente a sistemas, dados e informações operacionais de terceiros, aplicam-se as seguintes diretrizes adicionais:

- O acesso a sistemas, bases de dados e ambientes de clientes deve ser individual, nominal e limitado à finalidade contratada, sendo vedado o uso de credenciais compartilhadas;

- Informações e dados de um cliente não podem, em nenhuma hipótese, ser acessados, comparados, replicados ou utilizados em benefício de outro cliente, ainda que atuantes no mesmo setor;
- Colaboradores e prestadores de serviço alocados em projetos de clientes devem observar as cláusulas de confidencialidade específicas de cada contrato, que prevalecem sobre esta política sempre que estabelecerem obrigação mais restritiva;
- O encerramento de um contrato ou a saída de um colaborador/prestador de um projeto implica o bloqueio imediato de todos os acessos aos sistemas do respectivo cliente, cabendo ao gestor do projeto comunicar formalmente a TI;
- A entrega de relatórios e dashboards a clientes deve ocorrer exclusivamente por meio de canais controlados e homologados (Power BI com licenciamento adequado, ou plataforma de controle de acesso Dashpress para clientes sem licença de Power BI), vedada a distribuição de extratos de dados por e-mail, planilhas soltas ou links não controlados, salvo autorização expressa do cliente.

13 Backup, Continuidade e Recuperação

A Planning mantém rotina de cópias de segurança (backup) para os principais ativos de informação corporativos, com o objetivo de assegurar a disponibilidade e a recuperação de dados em caso de incidente, falha ou perda acidental.

- Os e-mails corporativos e os arquivos armazenados nos drives dos colaboradores (OneDrive/SharePoint) estão incluídos na rotina de backup mantida pela Planning;
- A área de TI é responsável por testar periodicamente a integridade e a restaurabilidade das cópias de segurança;
- Sistemas e bases de dados críticos para a operação de clientes, quando hospedados ou geridos pela Planning, devem ter rotina de backup específica, definida em conjunto com o gestor do contrato;
- Em caso de incidente que resulte em perda ou indisponibilidade de dados, a TI deve acionar o processo de restauração a partir do backup mais recente disponível e comunicar o gestor da informação e, quando aplicável, o Encarregado de Dados.

14 Disposições Gerais

Assim como a ética e os valores da Planning, a segurança no meio digital e a proteção de dados pessoais devem ser entendidas como parte fundamental da cultura interna da empresa. Todos devem colaborar e seguir os itens listados neste documento para o correto e seguro uso dos dados.

Referências normativas

- Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD);
- Resolução CD/ANPD nº 15/2024 — Regulamento de Comunicação de Incidente de Segurança;
- Resolução CD/ANPD nº 2/2022 — Regulamento da LGPD para agentes de tratamento de pequeno porte;
- Lei nº 12.965/2014 — Marco Civil da Internet, e Decreto nº 8.771/2016;
- Lei nº 12.737/2012 — Tipificação de delitos informáticos (Lei Carolina Dieckmann);
- Código Penal Brasileiro, art. 307 — Falsa identidade;
- Consolidação das Leis do Trabalho (CLT), art. 482 — Justa causa;
- Constituição Federal, art. 5º, incisos X e XII — Direito à intimidade e ao sigilo das comunicações;
- ISO/IEC 27001:2022 e ISO/IEC 27002:2022 — referências internacionais de boas práticas de gestão de segurança da informação, adotadas como orientação (não certificação) pela Planning.

Controle de Versão

Versão	Data	Alteração	Responsável
1.0	—	Emissão original	Douglas Rodrigues
2.0	12/08/2026	Revisão geral: inclusão de seções de LGPD, nuvem/IA, classificação da informação, dados de clientes, backup/continuidade e atualização da política de senhas/MFA	Douglas Rodrigues

15 Aprovação

ELABORADO POR
Douglas Rodrigues
Diretor de Tecnologia da Informação

APROVADO POR
Felipe Resende
Diretor de Engenharia

VALIDADO POR
Rodrigo Barbosa
Diretor Executivo