1. Introdução

A Columbia Integração reconhece que a informação é um de seus ativos mais valiosos. A forma como a empresa coleta, utiliza, armazena, compartilha e protege dados está diretamente ligada à confiança dos clientes, parceiros e da sociedade. Esta Política de Segurança da Informação estabelece os princípios e diretrizes que regem o tratamento da informação em todos os seus formatos e suportes, com o objetivo de garantir sua **confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade**.

A política está alinhada com as melhores práticas internacionais, especialmente os requisitos das normas ISO/IEC 27001:2022 (Sistema de Gestão de Segurança da Informação), ISO/IEC 27002:2022 (Controles de Segurança), e ISO/IEC 27701:2019 (Privacidade da Informação), além de atender às exigências da Lei Geral de Proteção de Dados (LGPD) e demais normas aplicáveis.

2. Histórico de versões

Versão	Data	Responsável	Alteração Realizada
1.0	08/06/2020	Gestor de Segurança da Informação	Versão inicial da política
2.0	10/06/2021	Gestor de Segurança da Informação	Inclusão de diretrizes sobre controle de acesso
3.0	06/06/2022	Gestor de Segurança da Informação	Atualização com base na ISO/IEC 27002:2022
4.0	18/06/2023	Gestor de Segurança da Informação	Revisão geral com foco em privacidade e riscos
5.0	01/06/2025	Gestor de Segurança da Informação	Revisão geral com foco em privacidade e riscos

3. Requisitos Regulatórios e Normativos

- **3.1. Base Normativa:** A PSI da Columbia é desenvolvida e mantida em conformidade com as melhores práticas internacionais e nacionais, incluindo, mas não se limitando a:
    - ISO/IEC 27001:2022 (Sistema de Gestão de Segurança da Informação - SGSI)
    - ISO/IEC 27002:2022 (Controles de Segurança da Informação)
    - ISO/IEC 27701:2019 (Gestão de Privacidade da Informação - Extensão à ISO 27001/27002)
    - Normas ABNT NBR ISO/IEC 27002 (versões aplicáveis e atualizadas)

- **3.2. Base Legal:** A PSI atende integralmente às exigências da Lei Geral de Proteção de Dados (Lei nº 13.709/2018 - LGPD) e demais leis e regulamentos aplicáveis às atividades da Columbia no Brasil, especialmente no que tange ao tratamento de dados pessoais e dados pessoais sensíveis.

4. Componentes Essenciais da PSI

- **4.1. Objetivos Estratégicos:** A PSI visa alcançar os seguintes objetivos, alinhados à missão da Columbia:
    - Proteger os ativos de informação da Columbia e de seus clientes contra ameaças, perdas, acessos não autorizados, uso indevido, alteração, destruição ou divulgação.
    - Minimizar os riscos de danos técnicos, jurídicos, financeiros, operacionais e reputacionais decorrentes de incidentes de segurança.
    - Garantir a continuidade e a resiliência das operações e serviços críticos, mesmo diante de falhas ou desastres significativos.
    - Promover e preservar a confiança dos clientes, parceiros, fornecedores e demais stakeholders na capacidade da Columbia em proteger suas informações.
    - Garantir o atendimento aos requisitos legais, regulamentares e contratuais aplicáveis.
    - Estabelecer uma cultura organizacional de segurança da informação e proteção de dados.
- **4.2. Aspectos de Governança:**
    - **4.2.1. Comitê de Segurança da Informação e Privacidade:** Criação ou formalização de um comitê multidisciplinar com representantes da alta gestão, TI/Serviços, Jurídico/Compliance, RH e áreas de negócio. Este comitê será responsável por supervisionar a implementação da PSI, aprovar revisões, tomar decisões estratégicas relacionadas à segurança e privacidade e avaliar riscos em alto nível.
    - **4.2.2. Papéis e Responsabilidades:** Detalhamento das responsabilidades conforme já apontado na PSI existente, expandindo para outros papéis essenciais (Ex: DPO, Gestor de Riscos, Responsáveis pelos Ativos).
    - **4.2.3. Níveis de Aprovação:** Definir quem aprova a PSI principal, as normas complementares e os procedimentos operacionais, garantindo o envolvimento da alta gestão.
    - **4.2.4. Mecanismos de Atualização e Revisão:** Estabelecer a periodicidade mínima de revisão da PSI e os gatilhos para revisões extraordinárias (mudanças regulatórias, incidentes graves, mudanças no ambiente de risco, novas tecnologias/serviços).
- **4.3. Gestão de Riscos:**
    - **4.3.1. Metodologia:** Adotar uma metodologia formal para identificação, análise e avaliação de riscos de segurança da informação e privacidade. O processo deve considerar ameaças (naturais, acidentais, intencionais) e vulnerabilidades aos ativos de informação.
    - **4.3.2. Processos de Mitigação:** Definir como os riscos identificados serão tratados (mitigar, transferir, aceitar, evitar), priorizando aqueles com maior impacto e probabilidade. Detalhar a implementação dos controles de segurança como forma de mitigação.

- **4.3.3. Tratamento de Vulnerabilidades:** Estabelecer processos para a identificação (scans, pentests), avaliação e correção de vulnerabilidades técnicas nos sistemas e infraestruturas.

5. Dimensões Técnicas

- **5.1. Arquitetura de Segurança:** Diretrizes para o desenho e implementação de arquiteturas de rede e sistemas seguras, incluindo segmentação de rede, uso de firewalls, sistemas de detecção/prevenção de intrusão, segurança em ambientes de nuvem e segurança de dispositivos móveis.
- **5.2. Controles de Acesso:** Implementação rigorosa do princípio do menor privilégio (Least Privilege) e da necessidade de saber (Need-to-Know). Processos formais para concessão, alteração e revogação de acessos. Utilização de autenticação forte (MFA - Autenticação Multifator) para sistemas e dados críticos. Revisão periódica de acessos e privilégios.
- **5.3. Gestão de Identidades:** Padronização e centralização da gestão de identidades e credenciais de usuários. Diretrizes para criação e uso de senhas seguras.
- **5.4. Proteção de Dados:** Diretrizes para a proteção da informação em repouso (armazenamento), em trânsito (transmissão) e em uso (processamento). Uso de criptografia onde aplicável. Tratamento diferenciado para dados pessoais e dados pessoais sensíveis.
- **5.5. Monitoramento de Sistemas:** Implementação de sistemas de monitoramento e registro de atividades (logs) em sistemas, redes e acessos, conforme já previsto na PSI existente. Definição dos tipos de eventos a serem monitorados, período de retenção de logs e responsabilidades pela análise.
- **5.6. Resposta a Incidentes:** Estabelecimento de um plano formal de resposta a incidentes de segurança da informação, incluindo a identificação, contenção, erradicação, recuperação e lições aprendidas. Definição clara dos canais de comunicação e responsabilidades. Procedimentos específicos para incidentes envolvendo dados pessoais, incluindo a avaliação da necessidade de notificação à ANPD e aos titulares.

6. Componentes Organizacionais

- **6.1. Treinamento e Conscientização:** Programa obrigatório e contínuo de treinamento em segurança da informação e proteção de dados para todos os stakeholders. O treinamento deve abordar a PSI, normas complementares, riscos relevantes e procedimentos de reporte de incidentes.
- **6.2. Segurança de Recursos Humanos:** Diretrizes de segurança desde a fase de recrutamento (verificação de antecedentes onde aplicável e permitido), inclusão de cláusulas de confidencialidade nos contratos, treinamento inicial, gestão de acessos durante o ciclo de vida do colaborador, e procedimentos rigorosos de desligamento (revogação de acessos, devolução de ativos).
- **6.3. Terceirização e Gestão de Fornecedores:** Processo formal para avaliação da segurança e conformidade de fornecedores e parceiros que terão acesso a informações da Columbia ou de seus clientes. Inclusão de cláusulas contratuais específicas de segurança da informação, confidencialidade e proteção de dados (Termos de Tratamento de Dados - DPA). Monitoramento periódico da conformidade de fornecedores críticos.
- **6.4. Comunicação de Políticas:** A PSI e as normas complementares devem ser comunicadas de forma eficaz e acessível a todos os stakeholders, garantindo que a ciência das regras seja formalizada (ex: assinatura do Termo de Responsabilidade).

7. Requisitos Específicos (Consolidando e Detalhando)

- **7.1. Gestão de Acessos:** (Detalhar o processo de concessão/revogação, uso de MFA, revisão periódica, acesso a sistemas e dados sensíveis).
- **7.2. Classificação da Informação:** Estabelecer os critérios de classificação (Confidencial, Restrita, Uso Interno, Pública - como já listado na versão DOCX) e as regras de manuseio, armazenamento, transmissão e descarte para cada nível de classificação. Responsabilidade pela classificação.
- **7.3. Backup e Recuperação:** Definir a política de backup (periodicidade, tipos de backup, locais de armazenamento - incluindo cópias externas criptografadas), procedimentos de recuperação e periodicidade de testes de restauração.
- **7.4. Segurança Física e Lógica:** Diretrizes para proteção das instalações físicas (data centers, escritórios, salas de servidores) e dos ativos lógicos (sistemas, dados, software). Inclui controle de acesso físico, monitoramento por CFTV (*Politica de Segurança da Informação 2023, Seção 8*), segurança de estações de trabalho e dispositivos móveis, proteção contra malware.
- **7.5. Conformidade com LGPD:** Detalhamento dos princípios da LGPD aplicados às operações da Columbia (finalidade, adequação, necessidade, transparência, segurança, prevenção, etc.). Diretrizes para o tratamento de dados pessoais ao longo de todo o seu ciclo de vida. Processos para atendimento aos direitos dos titulares. Diretrizes para transferência internacional de dados.

8. Estrutura de Governança

- Detalhar a composição, responsabilidades e periodicidade das reuniões do Comitê de Segurança da Informação e Privacidade.
- Estabelecer os fluxos de comunicação e reporte de segurança da informação, desde o usuário (reportando incidentes à Gerência de Serviços, por exemplo) até a alta gestão.

9. Disposições finais

As infrações a esta PSIC serão passíveis de processo disciplinar, podendo resultar de mera advertência até demissão por justa causa. A qualquer tempo, e em qualquer um dos casos previstos, prevalecendo o descumprimento das regras expostas, a Gerência de Serviços poderá bloquear temporariamente o acesso do usuário e comunicar os motivos ao profissional e ao gestor da área. O uso de qualquer recurso da Columbia para atividades ilegais é motivo de demissão por justa causa e a instituição vai cooperar ativamente com as autoridades.
Esta PSIC estarão disponíveis em documentos internos e em local de fácil acesso.

10. Vigência e Atualização

Esta política passa a ter vigência a partir da data de sua publicação. Devendo ser revisada e atualizada sempre que necessário.

DECLARAÇÃO DE CIÊNCIA

Nome completo:
Data:

_____
Assinatura