1 – OBJETIVOS

• Estabelecer diretrizes e normas que permitam aos colaboradores, prestadores de serviços, estagiários e demais stakeholders da Columbia, seguir padrões de comportamento desejáveis e aceitáveis, de acordo com a legalidade e as boas práticas globais de Segurança da Informação a fim de mitigar riscos técnicos e jurídicos;
• Nortear a definição de procedimentos específicos de Segurança da Informação e a implementação de controles e processos para o atendimento de seus requisitos;
• Preservar a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações da Columbia;
• Prevenir possíveis incidentes e responsabilidade legal da instituição e de seus colaboradores, prestadores de serviços, estagiários e afins;
• Garantir a normalidade e a continuidade das atividades da Columbia, protegendo os ativos, informações e processos críticos contra falhas ou desastressignificativos;
• Atender aos requisitos legais, regulamentares e contratuais pertinentes à atividade da Columbia;
• Minimizar riscos que possam causar danos aos ativos da companhia e, vazamento de informações, assim ocasioando perdas financeiras, participação no mercado, confiança de clientes e de parceiros ou qualquer outro impacto negativo nas atividades da Columbia resultante de uma falha de segurança;
• Assegurar o treinamento contínuo e atualizado das políticas e dos procedimentos de Segurança da Informação, enfatizando as obrigações das pessoas em relação à respectiva segurança;
• Garantir que todas as responsabilidades relacionadas da Segurança da Informação sejam amplamente divulgadas de forma clara e objetiva, por meio de campanhas de conscientização palestras, informes internos, dentro outros métodos de comunicação.
Deixar claro para todos os colaboradores, prestadores de serviços, estagiários e demais stakeholders da Columbia, quais implicações legais podem ser adotadas pela companhia no caso do não atendimento das diretrizes determinadas por esta Política de Segurança da Informação.

2 – ÁREA RESPONSÁVEL: Comitê de Segurança da Informação, composto por um representante das respectivas áreas: Segurança da Informação; Diretoria Financeira; Recursos Humanos e Gerência de Serviços.

3 – ÁREAS ENVOLVIDAS: Esta política se aplica a todas as áreas e unidades da Columbia Integração.

4 – CONTEXTUALIZAÇÃO

A Política de Segurança da Informação da Columbia (PSIC) é o documento que orienta e estabelece as diretrizes corporativas da Columbia para a proteção dos ativos de informação e a prevenção da responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da empresa.
A PSIC segue as leis vigentes no Brasil e foi elaborada com base nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2013, reconhecida mundialmente como um código de prática para a gestão da segurança da informação.

5. CONCEITOS E DEFINIÇÕES

Ativo: todo e qualquer bem da Columbia que possui valor econômico, incluindo a informação, e todo o recurso utilizado para o seu tratamento, tráfego e armazenamento.

Ativo Crítico e Sensível: todo ativo considerado essencial para a Columbia, cujo acesso por pessoas não autorizadas ou a falta de acesso por quem é permitido podem causar danos à instituição.

Autenticidade: tudo que garante a verdadeira autoria da informação, ou seja, que os dados são de fato provenientes de determinada fonte.

Cavalo de Troia (Trojan horse): programa malicioso que cria abertura para outros programas e invasões indesejadas.

Código Executável: arquivo interpretado pelo computador como um comando de execução para determinadas funções.

Código Malicioso: programa que possibilita ações danosas, como vírus, worms, trojans, spywares, malware, botnet, ransomware, entre outros.

Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Comunicadores Instantâneos: aplicativos que permitem interatividade, troca de conversas e conteúdos em tempo real. Ex. WhatsApp, Teams, entre outros.
Custodiante: quem detém a guarda da informação, mas não é necessariamente seu proprietário.

Cyberbullying: prática negativa de assédio moral que afeta o psicológico de outra pessoa por meio de recursos tecnológicos, como publicações na internet e o envio de fotos e vídeos com mensagens ofensivas pelo celular ou qualquer outro dispositivo móvel.

Dados Pessoais: informação relacionada a pessoa natural/física identificada ou identificável.

Dados Pessoais Sensíveis: dado pessoal sobre origem racial, ou étnica, convicção religiosa, opinião política, filiação à sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Disponibilidade: garantia de que os usuários autorizados obtenham, sempre que necessário, acesso à informação e aos ativos correspondentes.

Informação: todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para o uso restrito ou exposta ao público para consulta ou aquisição.

Informação Sensível: toda informação sigilosa que, se divulgada, pode resultar em danos e/ou, prejuízos de qualquer ordem, perda de vantagem, inclusive financeira, bem como impacto negativo para a Columbia.

Integridade: capacidade de garantir que a informação esteja mantida em seu estado original, conforme foi concebida, a fim de protegê-la contra alterações indevidas, intencionais ou acidentais na guarda ou transmissão.

Lei Geral de Proteção de Dados (LGPD): tem como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade, e a livre formação da personalidade de cada indivíduo. A Lei fala sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando um amplo conjunto de operações que podem ocorrer em meios manuais ou digitais.

Parceiros: Empresas, órgãos públicos e demais instituições que possuem contrato com a Columbia com objetivos em comum, unindo esforços em suas competências e expertises, sem que haja remuneração, mas apenas empenho de serviços por cada parte.

Peer to Peer: arquitetura de redes de computadores em que cada um dos pontos funciona como cliente e servidor possibilitando o compartilhamento de arquivos. Habitualmente são utilizadas para o compartilhamento de vídeos e músicas.

Segurança da Informação: preservação da confidencialidade, integridade e disponibilidade da informação.

Spam: e-mails não solicitados e normalmente enviados para um grande número de pessoas.

Usuário: todo colaborador, prestador de serviço, estagiário e afins que tenham acesso aos recursos tecnológicos oferecidos pela Columbia.

Vírus: programa malicioso que se propaga e infecta o computador.

Worm: programa semelhante ao vírus, que infecta o sistema, tendo como característica a auto replicação.

6 – PRINCÍPIOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Os equipamentos de informática, de comunicação, os sistemas e as informações devem ser utilizados para a realização de atividades profissionais, com senso de responsabilidade e preceitos éticos comuns à sociedade e dentro da legalidade.

Respeitar a privacidade dos usuários, agindo de forma ética e atendendo aos princípios da Lei Geral de Proteção de Dados Pessoais.
A Columbia reserva-se no direito de monitorar e registrar todo e qualquer uso das informações geradas, armazenadas ou veiculadas na empresa. Para tanto, são criados, implantados e utilizados controles apropriados, trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que a Columbia julgar necessário para reduzir os riscos, pautando-se na ética e na legalidade de forma a detalhar as ações na Norma de Monitoramento de Ativos.

7 – REQUISITOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A PSI deve ser comunicada a todos os colaboradores, prestadores de serviços, estagiários e afins visando à efetividade e à real cultura de uso ético e legal dos recursos tecnológicos.
Todos os contratos da Columbia devem constar de um anexo ou da cláusula de confidencialidade para garantir o acesso aos ativos de informação.
A responsabilidade em relação à Segurança da Informação deve ser atribuída na fase de contratação, de forma a ser incluída nos contratos e monitorada durante a sua vigência.
Todos os colaboradores, prestadores de serviços, estagiários e afins que tenham acesso a informações da Columbia, devem passar por treinamento de conscientização sobre os procedimentos de segurança e o uso correto dos ativos oferecidos pela empresa. A finalidade é minimizar possíveis riscos de segurança, explicitar as responsabilidades e comunicar os procedimentos para a notificação de incidentes. Todos os requisitos de Segurança da Informação e os aspectos legais, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de um projeto ou sistema. Também devem ser justificados, acordados, documentados, implementados e testados durante a fase de execução.
A Columbia exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente e/ou imprudente dos recursos e serviços concedidos aos usuários. Reservando-se no direito de tomar as medidas administrativas e judiciais cabíveis contra os infratores, bem como analisar dados e evidências para a obtenção de provas a serem usadas em processos investigatórios e judiciais.
Esta atualização da PSI será implementada na Columbia por meio de procedimentos específicos e obrigatórios a todos os colaboradores, prestadores de serviços, estagiários e afins, independentemente do nível hierárquico ou função na instituição.
Todo incidente que afete a Segurança da Informação deverá ser comunicado inicialmente e imediatamente à Gerência de Serviços.
Toda e quaisquer atividades que não estejam sendo tratadas nesta política ou normativas específicas, devem ser realizadas apenas após consulta e autorização do gestor da área.
O não cumprimento dos requisitos previstos nesta PSIC acarretará violação às regras internas da instituição, e o usuário estará sujeito a medidas administrativas e legais cabíveis.

8 – MONITORAMENTO E AUDITORIA

Para garantir as regras mencionadas nesta PSI, bem como para fins de segurança e prevenção à fraude, a Columbia reserva-se o direito de:
• Implantar sistemas de monitoramento de acesso às estações de trabalho, servidores internos e externos, correio eletrônico, navegação, internet, dispositivos móveis ou wireless, entre outros componentes da rede. A informação gerada por esses sistemas de monitoramento poderá ser usada para identificar usuários e respectivos acessos efetuados;
• Inspecionar qualquer arquivo de posse da Columbia, que esteja armazenado, no disco local de uma estação de trabalho, em servidores e storage na rede, pendrives, cd-roms ou qualquer outra mídia interna ou externa, com localização local ou remota para assegurar o rígido cumprimento desta PSIC;
• Instalar sistemas de proteção e detecção de invasão para garantir a segurança das informações e dos perímetros de acesso;
• Instalar câmeras em suas dependências.

Os colaboradores, prestadores de serviços, estagiários e afins tomam ciência de que ambientes, recursos tecnológicos, telefones, sistemas, computadores, dispositivos móveis e redes da instituição estão sujeitos a monitoramento e a gravação, atendendo à conformidade legal.

9 – RESPONSABILIDADES

9.1 Dos usuários em geral

Colaboradores, prestadores de serviços, estagiários e afins da Columbia, em qualquer nível hierárquico, na sua esfera de competência, serão responsáveis por cumprir e zelar pela materialização e realização eficaz das normas e princípios da segurança da informação. Em atenção especial ao compromisso com os critérios legais e éticos que envolvam a organização. É de inteira responsabilidade do usuário qualquer prejuízo ou dano sofrido ou causado a Columbia e/ou a terceiros, em decorrência da não obediência às diretrizes e às normas aqui referidas. É também de responsabilidade do profissional o uso de senha segura, devendo alterá-la conforme periodicidade determinada pela Columbia. Cabe a todos os usuários as seguintes práticas:

• Cumprir fielmente as regras estabelecidas neste documento;
• Buscar orientação do superior quando houver dúvidas relacionadas à Segurança da Informação;
• Assinar o Termo de Responsabilidade, formalizando a ciência da PSIC, bem como assumindo a responsabilidade pelo seu cumprimento;
• Proteger as informações contra o acesso, a modificação, a divulgação ou a destruição não autorizada pela Columbia;
• Assegurar que os recursos tecnológicos sejam utilizados apenas para fins profissionais aprovados e de interesse da instituição;
• Prezar pela segurança das informações confidenciais, incluindo todo e quaisquer dados pessoais a que tiverem acesso;

• Atender à Lei Geral de Proteção de Dados Pessoais, protegendo os dados a que tiver acesso ou que venha a manuseá-los, sempre em conformidade às regras da Columbia.
• Comunicar imediatamente à Gerência de Serviços sobre qualquer descumprimento ou violação da PSIC.

9.2 Dos gestores

Cabe a todo gestor de área:
▪ Manter postura em relação à Segurança da Informação e servir de modelo de conduta para os colaboradores, prestadores de serviços, estagiários e afins sob a sua gestão;
▪ Cumprir esta política de Segurança da Informação;
▪ Garantir acesso e conhecimento a esta política;
▪ Observar e zelar pela aplicação das regras e legislação de Proteção de Dados Pessoais;
▪ Comunicar imediatamente à Gerência de Serviços toda e qualquer violação de Segurança da Informação, incluindo violação de dados pessoais, que deverá informar a ocorrência de infrações provenientes de funcionários, bem como informar as demais áreas quando houver necessidades específicas.

9.3 Da Gerência de Serviços

A Gerência de Serviços será responsável pela gestão do uso de tecnologias necessárias ao bom andamento dos negócios da Columbia e de ações preventivas. São suas responsabilidades:
• Apresentar as atualizações da PSIC para aprovação e posterior publicação;
• Propor as metodologias e processos específicos para a Segurança da Informação, como a avaliação de risco;
• Propor e apoiar iniciativas que visem à segurança dos ativos de informação da Columbia;
• Promover com a área de Pessoas e Cultura, a conscientização dos colaboradores, prestadores de serviços, estagiários e afins quanto à relevância da Segurança da Informação para as atividades da Columbia por meio de campanhas, palestras, treinamentos, entre outros meios;
• Apoiar a avaliação e a adequação dos controles específicos da Segurança da Informação para novos sistemas ou serviços;
• Desenvolver normas e regras específicas conforme à Lei de Proteção de Dados Pessoais;
• Promover adequação dos recursos técnicos e de infraestrutura necessários para atender à Lei de Proteção de Dados Pessoais;
• Indicar o encarregado pela Proteção de Dados Pessoais;

9.4 Da área de Pessoas e Cultura

Cabe à Gerência de Pessoas:
• Atribuir, na fase de contratação dos colaboradores, prestadores de serviços, estagiários e afins, e formalizar nos contratos individuais de trabalho, a

responsabilidade quanto ao cumprimento da PSI e sua responsabilidade para com a Proteção de Dados Pessoais;
• Colher e arquivar a assinatura do Termo de Responsabilidade e ciência da Política Segurança da Informação dos profissionais já contratados;
• Comunicar formalmente e imediatamente à Gerência de Serviços toda e qualquer alteração no quadro funcional da organização, contratações, demissões, alterações de cargos, funções, entre outros, no prazo mínimo de 24 horas, e de imediato em casos específicos, a fim de evitar acessos não autorizados e/ou desnecessários;
• Receber da Gerência de Serviços informações sobre violações da Política e Normas e promover as tratativas e a instauração de processo disciplinar, quando cabível;
• Apoiar e promover com a Gerência de Serviços ações de conscientização e de capacitação em Segurança da Informação e Proteção de Dados Pessoais para todos os profissionais da Columbia;
• Zelar e promover a devida proteção de dados pessoais, em conformidade com as normas internas e legislação pertinentes.

10 – PROTEÇÃO DE DADOS PESSOAIS

A Columbia em atendimento e respeito à Lei Geral de Proteção de Dados Pessoais deverá garantir a disponibilidade, integridade, confidencialidade e autenticidade dos dados pessoais, em todo seu ciclo de vida, sendo esta categoria de dados tratados de forma permanente como dados confidenciais.
Todo tratamento de dados pessoais deverá estar atrelado a uma finalidade específica, informada ao titular e devidamente atrelada a uma ou mais bases legais previstas nos artigos 7º e 11º da Lei Geral de Proteção de Dados Pessoais, atentando-se aos princípios da necessidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e prestação de contas.
O detalhamento dos requisitos e regras para tratamento de dados pessoais serão disponibilizados em norma específica, sendo necessário que todos os colaboradores e prestadores de serviços tomem ciência e sejam sensibilizados sobre o tema e a respectiva norma.

11 – 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.

12 – 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