Título:	**SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA**	**Código:**	**PLT_012**
VP:	Riscos, *Compliance*, Prevenção e Segurança	**Versão:**	07

Histórico de Revisões

Versão:	Data Aprovação:	Histórico:
01	03/06/2014	Elaboração do Documento.
	13/11/2014	Por não haver alterações, o documento foi revalidado por mais 2 anos pelo diretor de Controles Internos, Sr. Eduardo Magalhães, portanto, não será gerada uma nova versão.
02	26/06/2015	Inclusão dos itens Abrangência (II), Documentação Complementar (III) e Disposições Gerais (VIII); Atualização dos itens Conceitos e Siglas (IV), Responsabilidades (V) e Gestão de Consequências (VII).
03	07/07/2017	Atualização dos itens II. Abrangência, III. Documentação Complementar, IV. Conceitos e Siglas e subitens 1.2 e 1.4 das VI. Diretrizes.
04	29/10/2019	Atualização no título da Política para "Segurança da Informação e Cibernética". Alteração dos itens I. Objetivo, II. Abrangência, III. Diretrizes subitens 1.1, 1.2, 1.3 e 1.4, V. Responsabilidades, VI. Documentação Complementar, VII. Conceitos e Siglas e VIII. Disposições Gerais. Inclusão no item III. Diretrizes, subitens 1, 1.1.1, 1.1.2, 1.1.3, 2, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6,2.7, 2.8, 2.9, 2.10, 2.10.1,2.10.2, 2.10.3 e 2.11.
05	29/06/2020	Alteração dos itens II. Abrangência; III. Princípios, Regras e Procedimentos - subitens 1.1.4, 1.4, 2., 2.1, 2.2; V. Responsabilidades; VI Documentação complementar; e VII. Conceitos e Siglas. Inclusão dos subitens 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.2.1, 2.2.2., 2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.2.7, 2.2.8, 2.2.9, 2.2.10, 2.2.11, 2.2.12, 2.2.13, 2.2.14, 2.2.15, 2.2.16 no item III. Princípios, Regras e Procedimentos. Exclusão dos subitens 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.10.1, 2.10.2, 2.10.3, 2.11. no item III. Princípios, Regras e Procedimentos.
06	26/04/2021	Atualização dos subitens 1.1.4, 1.1.5, 1.1.6, 1.2, 2.2.12, 2.2.15.2 do item III. Princípios, Regras e Procedimentos. Alterações nos itens V. Responsabilidades e VI. Documentação Complementar.
07	20/04/2022	Atualização dos itens: I. Objetivo, II. Abrangência, III. Princípios, Regras e Procedimentos subitens 1.1, 1.2, 1.2.5, 1.3, 1.5, 2, 2.1, 2.1.4, 2.2.1, 2.2.5, 2.2.6, 2.2.8, 2.2.12, 2.2.13, IV. Gestão de Consequências, V. Responsabilidades, VI. Documentação Complementar e VII. Conceitos e Siglas.

Índice

I. Objetivo

A presente Política de Segurança da Informação e Cibernética ("Política") tem por objetivo estabelecer diretrizes que permitam à Cielo S.A. salvaguardar seus ativos de informação, nortear a definição de normas e procedimentos específicos de Segurança da Informação e Cibernética, bem como a implementação de controles e procedimentos para reduzir a vulnerabilidade a incidentes.

II. Abrangência

Todos os membros do Conselho de Administração, dos Comitês de Assessoramento e da Diretoria-Executiva ("Administradores"), membros do Conselho Fiscal e colaboradores, independente de cargo ou função exercidos, das empresas Cielo S.A., Servinet Serviços Ltda., Aliança Pagamentos e Participações Ltda. e Stelo S.A., doravante denominadas de ("Cielo" ou "Companhia").

Todas as Sociedades Controladas da Companhia devem definir seus direcionamentos a partir das orientações previstas na presente Política, considerando as necessidades específicas e os aspectos legais e regulamentares a que estão sujeitas.

Em relação às Sociedades Coligadas, os representantes da Companhia que atuem na administração das Sociedades Coligadas devem envidar esforços para que elas definam seus direcionamentos a partir das orientações previstas na presente Política, considerando as necessidades específicas e os aspectos legais e regulamentares a que estão sujeitas.

III. Princípios, Regras e Procedimentos

1. Sobre a Segurança da Informação e Cibernética

1.1. A Companhia possui como objetivo desenvolver processos e produtos considerando os pilares e as boas práticas de segurança da informação, apoiada

na gestão dos riscos cibernéticos como assunto estratégico ao negócio e ao fomento da cultura de segurança entre todos os colaboradores para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

1.2. A Companhia estabelece os seguintes pilares:

1.2.1. **Confidencialidade**: garantir que a informação somente estará acessível para pessoas autorizadas;

1.2.2. **Integridade**: garantir que a informação, armazenada ou em trânsito, não sofrerá qualquer modificação não autorizada, seja esta intencional ou não;

1.2.3. **Disponibilidade**: garantir que a informação estará disponível sempre que for necessário;

1.2.4. **Autenticidade**: garantir que a informação é proveniente da fonte original e que não foi alvo de alterações.

1.2.5. **Irretratabilidade ou não repúdio**: garantir que o legítimo autor da informação não possa negar sua autoria.

1.2.6. **Conformidade**: garantir que os processos da Companhia estejam de acordo com os regulamentos, normativos e leis vigentes, de forma a seguir rigorosamente todos os protocolos exigidos no setor de atuação da Companhia em decorrência das suas atividades realizadas.

1.3. A Companhia considera que os ativos de informações são todas as informações geradas ou desenvolvidas para o negócio e podem estar presentes em diversas formas, tais como: arquivos digitais, consentimentos de clientes e pessoas ligadas à Companhia (*opt-in* e *opt-out),* equipamentos, mídias externas, documentos impressos, documentos digitalmente assinados, sistemas, dispositivos móveis, bancos de dados, conversas e gravações.

1.4. A Companhia determina que, independentemente da forma apresentada, compartilhada ou armazenada, os ativos de informação devem ser utilizados apenas para a sua finalidade devidamente autorizada, sendo sujeitos a monitoramento e auditoria.

1.5. A Companhia estabelece que todo o ativo de informação de sua propriedade possui um responsável, seja devidamente classificado quanto ao seu nível de confidencialidade de acordo com os critérios estabelecidos em norma específica e adequadamente protegido de quaisquer riscos, bem como de ameaças que possam comprometer o seu negócio.

2. Diretrizes Gerais de Segurança da Informação e Cibernética

2.1. A Companhia possui como diretrizes gerais:

2.1.1. Resguardar a proteção dos dados contra acessos indevidos, bem como contra modificação, destruição ou divulgação não autorizada;

2.1.2. Realizar a adequada classificação das informações e garantir a continuidade do processamento das mesmas, conforme os critérios e princípios indicados nos normativos internos vigentes sobre o tema;

2.1.3. Garantir que os sistemas e dados sob sua responsabilidade estejam devidamente protegidos e sejam utilizados apenas para o cumprimento de suas atribuições;

2.1.4. Zelar pela integridade da infraestrutura tecnológica na qual são armazenados, processados ou de qualquer outra forma tratados os dados, adotando as medidas necessárias para prevenir ameaças lógicas, como vírus, programas nocivos ou outras falhas que possam ocasionar acessos, manipulações ou usos não autorizados a dados internos e confidenciais.

2.1.5. Atender às leis e normas que regulamentam as atividades da Companhia.

2.2. Em vistas ao cumprimento das diretrizes acima elencadas, a Companhia:

2.2.1. Adota procedimentos e controles de segurança para atender aos objetivos de segurança cibernética, dentre eles: a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações, conforme normativos internos vigentes.

2.2.2. Controla, monitora, restringe o acesso aos ativos de informação a menor permissão e privilégios possíveis, conforme descrito em normas internas específicas.

2.2.3. Aplica os procedimentos e controles citados anteriormente, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da Companhia.

2.2.4. Possui controles específicos, incluindo os voltados para a rastreabilidade da informação, que buscam garantir a segurança das informações sensíveis.

2.2.5. Realiza ações para prevenir, identificar, registrar e responder incidentes e crises de segurança que envolvam o ambiente tecnológico da Companhia e que possam ocasionar o comprometimento dos pilares de segurança da informação ou gerar impacto de imagem, financeiros ou operacionais.

2.2.6. Classifica os incidentes de segurança da informação e cibernética conforme sua relevância e de acordo com (i) a classificação das informações envolvidas; e (ii) o impacto na continuidade dos negócios da Companhia, conforme descritos em normas internas específicas. A

definição de relevância dos incidentes no ambiente tecnológico segue o padrão corporativo de riscos estabelecido em documento específico.

2.2.7. Realiza o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da Companhia, que abrangem, inclusive, informações recebidas de empresas prestadoras de serviços a terceiros.

2.2.8. Estabelece e documenta em normativo interno os critérios que configurem situações de crises, bem como elabora inventário dos cenários de crises cibernéticas relacionados aos incidentes de segurança considerados nos testes de continuidade de serviços de pagamento prestados e realiza testes anuais para garantir a eficácia dos processos, além de produzir anualmente um relatório de resposta a incidentes no ambiente tecnológico da Companhia.

2.2.9. Possui critérios para classificação da relevância dos serviços de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, conforme procedimento interno.

2.2.10. Previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem serão adotados os procedimentos previstos na regulamentação do Banco Central do Brasil ("BCB") em vigor específica sobre o tema.

2.2.11. Avalia, previamente à contratação de empresas prestadoras de serviços que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução de atividades operacionais da Companhia, se adotam procedimentos e controles voltados à prevenção e ao tratamento de incidentes em níveis de complexidade, abrangência e precisão compatíveis com os adotados pela Companhia.

2.2.12. Realiza a avaliação periódica de empresas prestadoras de serviço que realizam o tratamento de informações relevantes à Companhia com objetivo de acompanhar o nível de maturidade de seus controles de segurança, dentre eles, os utilizados para a prevenção e o devido tratamento dos incidentes.

2.2.13. Adota iniciativas para compartilhamento de informações sobre os incidentes relevantes por meio da filiação em fóruns de discussão.

2.2.14. Estabelece regras e padrões para assegurar que a informação receba o nível adequado de proteção quanto à sua relevância conforme normativo interno. Toda informação possui um proprietário, é obrigatoriamente classificada e recebe os devidos controles que garantam a confidencialidade da mesma, condizendo com as boas práticas de mercado e regulamentações vigentes.

2.2.15. Adota mecanismos para disseminação da cultura de segurança da informação e cibernética na Companhia, incluindo:

2.2.15.1. A implementação de programa de treinamento anual para colaboradores;

2.2.15.2. A implementação de programa de avaliação periódica de colaboradores quanto ao nível de conhecimento do tema segurança da informação e cibernética;

2.2.15.3. A prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos; e

2.2.15.4. O comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética.

IV. Gestão de Consequências

Colaboradores, fornecedores ou outros *stakeholders* (públicos de interesse) que observarem quaisquer desvios às diretrizes desta Política, poderão relatar o fato ao Canal de Ética nos canais abaixo, podendo ou não se identificar:

- https://canaldeetica.com.br/cielo
- Telefone, ligação gratuita: 0800 775 0808

Internamente, o não cumprimento das diretrizes desta Política enseja a aplicação de medidas de responsabilização dos agentes que a descumprirem conforme a respectiva gravidade do descumprimento, e de acordo com normativos internos.

V. Responsabilidades

- **Administradores, Colaboradores e Prestadores de Serviço:** Observar e zelar pelo cumprimento da presente Política e, quando assim se fizer necessário, acionar a Vice-Presidência de Riscos, Compliance, Prevenção e Segurança para consulta sobre situações que envolvam conflito com esta Política ou mediante a ocorrência de situações nela descritas. É imprescindível que cada pessoa compreenda o papel da segurança da informação em suas atividades diárias e participe dos programas de conscientização.
- **Vice-Presidência de Riscos, *Compliance*, Prevenção e Segurança:** Cumprir as diretrizes estabelecidas nesta Política, mantê-la atualizada anualmente de forma a garantir que quaisquer alterações no direcionamento da Companhia sejam incorporadas a mesma e esclarecer dúvidas relativas ao seu conteúdo e a sua aplicação.
- **Administradores, Colaboradores e Prestadores de Serviço:** Atuar de forma ética e responsável quando tomar conhecimento de incidentes, compartilhando informações com os responsáveis pelo seu tratamento em tempo hábil e tomando todas as ações cabíveis para minimizar os potenciais danos, de acordo com o procedimento Plano de Resposta a Incidentes – CSIRT Cielo.
- **Conselho de Administração**: Após a emissão de recomendação favorável pelos Comitês de Assessoramento competentes, deliberar sobre a aprovação anual do (i)

relatório sobre a implementação do plano de ações e de resposta a incidentes para cumprimento da Política de Segurança da Informação e Cibernética da Companhia, e (ii) Plano de Resposta a Incidentes – CSIRT Cielo.

- **Fórum Gestor de Segurança da Informação e Prevenção a Fraudes:** Atuar de forma proativa, apoiando a gestão de Segurança da Informação no cumprimento das tarefas relacionadas à proteção dos negócios da Companhia e dos seus clientes, bem como prestar assessorar à Diretoria-Executiva em relação aos temas objetivos do escopo do fórum.
- **Fornecedores**: Observar e zelar pelo cumprimento das melhores práticas de Segurança da Informação, bem como dos requisitos de segurança da informação e cibernética exigidos contratualmente durante o vínculo com a Companhia. Atuar de forma ética e responsável quando tomar conhecimento de incidentes, compartilhando informações com os responsáveis pelo seu tratamento em tempo hábil e tomando todas as ações cabíveis para minimizar os potenciais danos, de acordo com o procedimento Plano de Resposta a Incidentes – CSIRT Cielo.

VI. Documentação Complementar

- ABNT NBR ISO 27001 - Segurança da Informação.
- Código de Conduta Ética da Cielo.
- Lei Nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet.
- Lei Nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais ("LGPD").
- Normas e procedimentos internos aperfeiçoados constantemente, aprovados pelas alçadas competentes e disponibilizados a todos os colaboradores.
- PCI-Data Security Standard.
- Plano de Resposta a Incidentes – CSIRT Cielo.
- Política de Gestão Corporativa de Continuidade de Negócios.
- Resolução BCB nº 85/21.

VII. Conceitos e Siglas

- **Clientes:** Pessoa física ou jurídica que utiliza os produtos e/ou serviços oferecidos pela Cielo.
- **Conselho de Administração:** é um órgão de deliberação colegiada que visa satisfazer as atribuições de orientar e fiscalizar a gestão da Diretoria-Executiva e decidir sobre as grandes questões do negócio, incluindo-se a tomada das decisões estratégicas, de investimento e de financiamento, entre outros assuntos previstos no artigo 142 da Lei das Sociedades por Ações e/ou Estatuto Social da Companhia.
- **Comitês de Assessoramento:** é um órgão de deliberação colegiada que visa satisfazer as atribuições de orientar e fiscalizar a gestão da Diretoria-Executiva e

decidir sobre as grandes questões do negócio, incluindo-se a tomada das decisões estratégicas, de investimento e de financiamento, entre outros assuntos previstos no artigo 142 da Lei das Sociedades por Ações e/ou Estatuto Social da Companhia.

- **Dado(s) e/ou Informação(ões):** são todos os dados referentes às atividades desenvolvidas pela Companhia na execução de seu objeto social, incluindo dados de Clientes, pessoais ou não, e classificados de acordo com a norma interna específica sobre o tema.
- **Diretoria-Executiva:** é o órgão responsável pela gestão dos negócios da sociedade, executando a estratégia e as diretrizes gerais aprovadas pelo Conselho de Administração. Por meio de processos e políticas formalizados, a Diretoria-Executiva viabiliza e dissemina os propósitos, princípios e valores da organização.
- **Incidentes:** qualquer ocorrência que realmente ou potencialmente comprometa a confidencialidade, integridade ou disponibilidade de um sistema de informação ou a informação que o sistema processa, armazena ou transmite ou que constitui uma violação ou ameaça iminente de violação de políticas de segurança, procedimentos de segurança ou políticas de uso aceitáveis.
- **Prestador de Serviço:** pessoa física ou jurídica, devidamente contratada pela Companhia, prestadora de serviços: (i) de tecnologia; (ii) de armazenamento ou qualquer forma de tratamento de Dados e Informações; ou (iii) que venha a ter acesso, por conta do escopo de sua contratação, a Dados confidenciais, como classificados nesta Política.
- **Riscos Cibernéticos:** são os riscos de ataques cibernéticos, oriundos de *malware*, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, entre outros, que possam expor Dados, redes e sistemas da Companhia, causando danos financeiros e/ou de reputação consideráveis, podendo, em algumas circunstâncias, prejudicar a continuidade das atividades da Companhia.
- **Segurança da Informação:** conjunto de conceitos, técnicas e estratégias, as quais visam proteger os ativos de informação da Companhia.
- **Segurança Cibernética:** conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado.
- **Stakeholders (públicos de interesse):** todos os públicos relevantes com interesses pertinentes à Companhia, bem como indivíduos ou entidades que assumam algum tipo de risco, direto ou indireto, em face da sociedade. Entre outros, destacam-se: acionistas, investidores, colaboradores, sociedade, clientes, fornecedores, credores, governos, órgãos reguladores, concorrentes, imprensa, associações e entidades de classe, usuários dos meios eletrônicos de pagamento e organizações não governamentais.
- **Sociedades Coligadas:** são as sociedades nas quais a Companhia tenha influência significativa, sendo que, nos termos do artigo 243, §4° e §5 da Lei das Sociedades por Ações, (i) há influência significativa quando a Companhia detém ou exerce o poder de participar nas decisões das políticas financeira ou operacional de uma

sociedade, sem, contudo, controlá-la; e (ii) a influência significativa será presumida quando a Companhia for titular de 20% (vinte por cento) ou mais do capital votante da respectiva sociedade, sem, contudo, controlá-la.

- **Sociedades Controladas:** são as sociedades nas quais a Companhia, direta ou indiretamente, é titular de direitos de sócia ou acionista que lhe assegurem, de modo permanente, preponderância nas deliberações sociais e o poder de eleger a maioria dos administradores, nos termos do artigo 243, §2º da Lei das Sociedades por Ações.
- **Plano de Resposta a Incidentes – CSIRT Cielo:** Procedimento estabelecido para que os incidentes de Segurança da Informação e Cibernética sejam identificados e respondidos conforme as diretrizes estabelecidas internamente.
- ***Opt-In*:** Opção para receber informações.
- ***Opt-Out*:** Opção para não receber informações.

VIII. Disposições Gerais

É competência do Conselho de Administração da Companhia alterar esta Política sempre que se fizer necessário.

Esta Política entra em vigor na data de sua aprovação pelo Conselho de Administração e revoga quaisquer documentos em contrário.

Barueri, 20 de abril de 2022.

Cielo S.A.