1. OBJETIVO

Em atenção à Resolução nº 4.893/21 do Banco Central do Brasil e à Lei n. 13.709/2018, este documento estabelece os princípios, conceitos, valores e práticas a serem adotados visando assegurar a confidencialidade, a integridade e a disponibilidade dos dados da instituição ou por ela controlados e dos sistemas de informação por ela utilizados, permitindo à instituição prevenir, detectar e reduzir a vulnerabilidade e incidentes relacionados à segurança da informação.

2. PÚBLICO-ALVO

Este documento é dirigido a todos os sócios, administradores, colaboradores, empregados ou não, menores aprendizes, estagiários, correspondentes, prestadores de serviços e todas e quaisquer pessoas que tenham acesso aos dados da instituição ou por ela controlados.

3. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Multicred Sociedade de Crédito Direto S.A (doravante denominada **Multicred SCD**) considera primordiais a segurança e o sigilo das informações de seus clientes e usuários. Para assegurar este compromisso, faz uso de modernas tecnologias de segurança do mercado, no entanto, apenas tecnologia não garante a total proteção, é preciso o comprometimento das pessoas para mitigar os riscos existentes. Proteger efetivamente as informações sem prejudicar a excelência nos negócios é um dos maiores desafios de uma Instituição Financeira.

A Política de Segurança da Informação é composta por um conjunto de normas, instruções e procedimentos necessários à prevenção e manutenção do nível de segurança da Multicred SCD, que resumem os princípios de segurança que a Instituição reconhece como importantes e que devem estar presentes no dia a dia de todos os usuários. Aplicando-se a todos os usuários, sistemas e ambientes corporativos que compõem a Instituição.

4. DOS PRINCÍPIOS

De estabelecer as diretrizes, papéis e responsabilidades e assegurar a efetividade da gestão da segurança da informação da Multicred SCD, através da definição, análise e priorização das ações necessárias para alcance dos objetivos estabelecidos para manutenção da segurança de suas informações.

As ações da instituição regem-se pelos seguintes princípios:

- ⇒ Confidencialidade: limitação do acesso à informação, sendo permitido o acesso somente às pessoas autorizadas e em circunstâncias que se apresentem efetivamente necessário o acesso, protegendo informações que devem ser acessíveis apenas por um determinado grupo de usuários contra acessos não autorizados;
- ⇒ Disponibilidade: garantia de acesso das pessoas devidamente autorizadas à informação sempre que o acesso for necessário, prevenindo interrupções das operações da Instituição por meio de um controle físico e técnico das funções dos

sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança;

⇒ Integridade: garantia da veracidade, fidelidade e integridade da informação e dos métodos de seu processamento e eventual tratamento da informação, pois esta não deve ser alterada enquanto está sendo transferida ou armazenada, impedindo que a informação fique exposta ao manuseio por uma pessoa não autorizada e impedindo alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.

5. DIRETRIZES

A Política de Segurança da Informação estabelece o direcionamento estratégico para a proteção efetiva das informações da Multicred SCD, com as seguintes diretrizes:

⇒ Avaliação de Riscos – garantir a confidencialidade, integridade e disponibilidade da informação;

⇒ Treinamento e Conscientização – promover treinamentos e ações de conscientização de Segurança da Informação aos usuários da instituição para que haja ciência e concordância com as responsabilidades no cumprimento da Política de Segurança da Informação;

⇒ Conformidade – estar em conformidade com leis e normas vigentes aplicáveis a Multicred SCD;

⇒ Reporte de Incidentes – colaborador deverá comunicar a área de tecnologia qualquer atividade considerada suspeita. E por sua vez, a área de tecnologia deverá comunicar ao Compliance e à Presidência o descumprimento de controles estabelecidos pela Política de Segurança da Informação e todos os demais documentos que a compõem;

⇒ Acesso aos Recursos e Ativos de Informação – garantir que todos os acessos aos recursos de processamento de informação sejam devidamente autenticados e autorizados;

⇒ Proteção dos Perímetros – garantir que haja controles para prevenir o acesso físico não autorizado, danos e interferências nas instalações que abrigam ou armazenam ativos de propriedade da Multicred SCD.

6. RESPONSABILIDADES

As responsabilidades atribuídas pela Resolução nº 4.893/21 do Banco Central do Brasil são distribuídas da seguinte forma:

6.1 Política de segurança cibernética e da informação e plano de ação e de resposta a incidentes

A Política de Segurança Cibernética e da Informação, a execução do Plano de Ação e de Resposta a Incidentes e a melhoria contínua dos procedimentos relacionados com a

segurança cibernética são de responsabilidade do Diretor Presidente.

6.2 Área de Tecnologia da Informação

É responsável pela gestão e pelo direcionamento das ações de Segurança da Informação na Multicred SCD, deve definir a Política de Segurança da Informação e garantir que os controles estabelecidos sejam implementados adequadamente.
Além disso, possuem as seguintes responsabilidades:

- ⇒ Garantir que haja monitoramento e análise de alertas de segurança da informação;
- ⇒ Desenvolver e disseminar ações de conscientização em Segurança da Informação para todos os usuários da instituição;
- ⇒ Analisar o resultado de auditorias relacionadas à Segurança da Informação e medir a eficácia dos controles estabelecidos pela respectiva Política;
- ⇒ Apresentar relatórios periódicos, contendo resultados de análises e testes referentes ao nível atual de Segurança da Informação da Multicred SCD.

6.3 Gestores das Áreas de Negócios

Os gestores imediatos são responsáveis por garantir que seus colaboradores cumpram as disposições constantes neste documento, garantindo aderência e cumprimento dos controles de segurança da informação estabelecidos pelas normas e instruções da instituição.
Os gestores das áreas da Multicred SCD possuem as seguintes responsabilidades:

- ⇒ Garantir que as inconformidades ocorridas em sua área sejam identificadas e reportadas, conforme controles estabelecidos pelas normas e instruções de Segurança da Informação;
- ⇒ Impedir que usuários demitidos, demissionários ou com contrato encerrado tenham acesso aos ativos de informação, utilizando-se dos procedimentos adequados de desligamento/encerramento contratuais adotados;
- ⇒ Contribuir na proteção dos ativos de sua área, em nível físico, de acordo com os critérios definidos pela Multicred SCD;
- ⇒ Deverá aplicar as sanções previstas àqueles que deliberadamente violarem as determinações de controles desta Política de Segurança da Informação.

6.4 Revisão da Política de Segurança da Informação

A Política de Segurança da Informação e suas normas e instruções serão revisadas periodicamente e a qualquer tempo e quando houver necessidade de alteração das diretrizes contidas na Política ou dos controles contidos nas normas trazidas pelo compliance e da área de Tecnologia da Informação.

6.5 Usuários

É dever de todos os usuários, com acesso às informações e ativos de informação, não

importando o vínculo legal (conselheiros, diretores, gestores, colaboradores, estagiários, temporários e terceiros), ter pleno conhecimento de todos os controles de segurança estabelecidos nos documentos que compõem a Política de Segurança da Informação, atentando para a responsabilidade no seu cumprimento.

6.6 Sanções administrativas

Esta Política de Segurança da Informação só poderá ser eficaz se contar com o comprometimento de todos. Nenhum usuário poderá recorrer ao desconhecimento desta Política e suas normas e instruções, para justificar violações ou falta de cumprimento sem prejuízo à reparação dos danos. A Multicred SCD se reserva o direito de aplicar as sanções administrativas, legais e penais devidas à matéria.

6.7 Registro, análise de causa e do impacto e controle dos efeitos de incidentes relevantes.

O registro, a análise da causa e do impacto e o controle dos efeitos de incidentes relevantes são de responsabilidade da Área de Tecnologia da Informação.

6.8 Realização dos testes e varreduras periódicos para detecção de vulnerabilidades

A realização dos testes e varreduras para detecção de vulnerabilidades são responsabilidades da Área de Tecnologia da Informação. Sendo realizado por *software* de antivírus e antissequestro, de acordo com a necessidade encontrada a fim mitigar os riscos diários de possíveis ou tentativas de invasões.

6.9 Manutenção de cópias de segurança dos dados e das informações

A execução dos *backups*, independentemente da plataforma computacional, bem como o descarte de mídias magnéticas oriundas do processo de *backup*, quando aplicável, são responsabilidades da Área de Tecnologia da Informação.

6.10. Documentação da verificação do prestador de serviço, das práticas de governança corporativa e da avaliação da relevância do serviço a ser contratado

A atividade de documentação das informações de que tratam os itens desta política, referente à verificação de capacidade do potencial prestador de serviço, das práticas de governança corporativa e referente à avaliação da relevância do serviço a ser contratado.

6.11. Comunicação de incidentes de segurança à autoridade nacional de proteção de dados

Em atenção ao Art. 48 da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD), será responsabilidade da instituição, a comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

6.12. Comunicação de incidentes relevantes relacionados ao ambiente cibernético ao Banco Central do Brasil

Em atenção ao Art. 20, inciso III, da Resolução nº 4.893/21 do Banco Central do Brasil, será

responsabilidade da instituição, comunicar ao Banco Central do Brasil a ocorrência de incidentes relevantes e das interrupções dos serviços relevantes que configurem uma situação de crise pela instituição financeira, bem como das providências para o reinício das atividades.

6.13. Comunicação de contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem

Em atenção ao Art. 15 da Resolução nº 4.893/21 do Banco Central do Brasil, será responsabilidade da instituição, comunicar ao Banco Central do Brasil a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, em conformidade com a resolução vigente.

6.14. Encarregado pelo tratamento de dados pessoais

Em atenção aos arts. 5º, inciso VIII; 23, inciso II; e 41, caput e parágrafos, todos da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD), na qualidade de "Encarregado pelo Tratamento de Dados Pessoais", a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), é responsável por:

- ⇒ aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- ⇒ receber comunicações da autoridade nacional e adotar providências;
- ⇒ orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- ⇒ executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

7. DAS DIRETRIZES DE SEGURANÇA CIBERNÉTICA

A Segurança Cibernética na Instituição segue as seguintes diretrizes:

- ⇒ As informações da Instituição, dos clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida.
- ⇒ As informações e os dados devem ser utilizados de forma transparente e apenas para as finalidades para as quais foram coletadas.
- ⇒ A identificação daqueles que têm acesso às informações da Instituição deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

⇒ Somente deve ter concedido acesso às informações e recursos de informação imprescindíveis para o pleno desempenho das suas atividades do indivíduo autorizado.

⇒ A senha é utilizada como assinatura eletrônica, sendo pessoal e intransferível, e deve ser mantida secreta, sendo proibido seu compartilhamento.

⇒ Devem ser reportados à área de Tecnologia da Informação da Instituição os riscos às informações, bem como eventuais fatos ou ocorrências que possam colocar em risco tais informações, que será responsável pelo registro e controle dos efeitos de incidentes relevantes.

2.1 Das diretrizes para tratamento da Informação

A informação deve receber proteção adequada em observância aos princípios e diretrizes da Segurança Cibernética e da Informação da Instituição em todo o seu ciclo de vida, que compreende: Coleta, Tratamento, Armazenamento, Transporte e Descarte.

2.2 Das diretrizes para classificação de dados e das informações

As informações e os dados sob responsabilidade da instituição serão classificados, conforme descrito no plano de ação, para adequação da estrutura organizacional e operacional aos princípios e às diretrizes da Política de Segurança Cibernética.
A divulgação desses dados é proibida. Sendo que os dados pessoais sensíveis deverão ser protegidos de forma mais rígida, devendo ser compatível com as funções desempenhadas e com a sensibilidade das informações. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

2.3 Das diretrizes para a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios

Deverão ser elaborados, no âmbito dos testes de continuidade de negócios, cenários de incidentes que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados pela instituição, que tenham ou possam ter a capacidade de causar interrupção nos processos de negócios da instituição.
Deverão ser consideradas para a elaboração desses cenários, considerando as ausências de ativos causadas por:

⇒ vazamento de dados;

⇒ indisponibilidade de recursos computacionais;

⇒ problemas relacionados a software, banco de dados, servidor de aplicação, rede;

⇒ quebra da integridade dos dados, via alteração ou injeção fraudulenta de dados/informações em sistemas e/ou bases de dados;

⇒ fraudes eletrônicas, incluindo a realização de transações fraudulentas em sistemas de informação da instituição;

⇒ desastres ou catástrofes, naturais ou não;

⇒ danos físicos relevantes a instalações ou equipamentos críticos, intencionais ou não;

⇒ falhas no fornecimento de energia elétrica;

⇒ ausência de colaboradores.

2.4 Das diretrizes para a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços

Na elaboração de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços, considerando as características do serviço a ser prestado e níveis de complexidade, abrangência e precisão, deverão ser analisados cenários de incidentes que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados.
Uma vez identificados os possíveis cenários, serão analisados os controles voltados à prevenção e ao tratamento dos incidentes já utilizados pela prestadora, e, caso necessário, deverão ser estabelecidos com a respectiva prestadora de serviços outros procedimentos e controles de prevenção e tratamento dos incidentes a serem adotados.

2.5 Das diretrizes para definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes

Os parâmetros a serem utilizados na avaliação da relevância dos incidentes deverão considerar a frequência e o impacto dos cenários de incidentes que impliquem em dano ou perigo de dano à instituição e ao sigilo dos dados e dos sistemas de informação utilizados, que tenham ou possam ter a capacidade de causar interrupção nos processos de negócios da instituição.

8. PROCEDIMENTOS E OS CONTROLES

A Multicred SCD, visando a integração dos dados como forma de otimizar e aumentar a qualidade da atividade com base na orientação do BACEN e de acordo com a Lei de Proteção de Dados vigente n°13.709/2018. Para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética, a instituição, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias, adotará os seguintes procedimentos e os controles:

3.1 Acessos

⇒ Acesso a ambiente servidor: apenas pessoas autorizadas poderão ter acesso ao ambiente que compõem a estrutura organizacional da instituição;

⇒ Usuários administrativos - ambiente corporativo: no processo de controle e de segurança da informação, fica restrito o acesso administrativo em toda instituição

para ambientes internos, ficando dentro dos padrões pré-estabelecido a todos os usuários;

⇒ Usuários administrativos - ambiente de sistemas: fica restrito o acesso administrativo em toda instituição para ambientes sistêmicos. Os usuários serão criados e/ou alterados com base na classificação dos níveis de perfis correspondentes a função do colaborador, permitindo seus acessos dentro dos padrões pré-estabelecidos a todos os usuários de cada nível.

3.2 Autenticação

Em segurança da informação, a autenticação é um processo que busca verificar a identidade digital do usuário de um sistema, normalmente, no momento em que ele requisita um login (acesso) em um programa ou computador, delimitando e controlando o acesso às informações.
Os seguintes acessos exigem autenticação:

⇒ Sistema de e-mails;

⇒ Sistemas ERP;

⇒ Diretórios e arquivos na rede;

⇒ Estação de trabalho.

3.3 Criptografia

Esta instituição classifica suas informações de acordo com o seu sigilo. Assim criptografa as informações consideradas sigilosas, indiferente se estão na base de dados ou em sistemas de arquivos na rede.

3.4 Prevenção de vazamento de informações

Esta instituição também utiliza recursos tecnológicos para prevenir o vazamento de informações.

3.5 Testes e varreduras periódicos para detecção de vulnerabilidades

Teste de varredura ocorrerá automaticamente com ferramentas especializadas de análise e detecção de vulnerabilidade como o antivírus e antissequestro.

3.6 Controles de acesso

Esta Instituição utiliza mecanismos de controle de acesso por autenticação e todos os sistemas listados, permitem que apenas usuários autorizados possam acessar as informações, de acordo com o nível de sigilo e acesso.

3.7 Manutenção de cópias de segurança dos dados e das informações

Esta instituição instituiu a política de backup, na qual são registradas todas as decisões sobre armazenamento de dados, processos, tipos e métricas dos backups da instituição.

3.8 Registro, análise da causa e do impacto e controle dos efeitos de incidentes relevantes

Para que seja possível a melhoria contínua dos procedimentos relacionados à segurança cibernética, permitindo que sejam realizadas as adequações necessárias à correção de vulnerabilidades nas medidas e procedimentos relativos à segurança cibernética, deve ser realizado o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição, abrangendo, inclusive, informações recebidas de empresas prestadoras de serviços, sendo elaborado relatório próprio pela área responsável.

3.9 Gestão de Prestadores de Serviços

Quando da contratação de prestadores de serviço, inclusive serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, a Instituição adotará práticas de governança corporativa e de gestão para os prestadores contratados.

8.9.1

Abrangência

Devem ser consideradas para fins de aplicação do disposto nesta política aquelas empresas prestadoras de serviços que tiverem acesso:

I. aos dados da instituição, ou por ela controlados; ou
II. aos sistemas por ela utilizados; ou
III. aos ambientes físicos ou tecnológicos, que possam ser utilizados para acessar aos dados e sistemas de que tratam os incisos I e II.

8.9.2 Cláusulas contratuais

Os contratos com empresas prestadoras de serviços deverão conter cláusulas de confidencialidade e responsabilidade entre as partes, bem como cláusulas que garantam que os profissionais das empresas prestadoras de serviços:

⇒ Protejam e zelem pelo sigilo das informações da Instituição;

⇒ Tenham conhecimento e cumpram esta Política;

⇒ Cumpram as leis e normas que regulamentam a propriedade intelectual e a proteção de dados, especialmente a Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais) e a Resolução nº 4.893/21 do Banco Central do Brasil;

⇒ Comuniquem imediatamente qualquer violação desta Política e/ou outras Normas.

9. COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A instituição comunicará à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados a ocorrência de incidente de segurança, seja ele relativo ao ambiente

cibernético ou não, que possa acarretar risco ou dano relevante aos titulares.
A referida comunicação deverá ser feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

- ⇒ a descrição da natureza dos dados pessoais afetados;
- ⇒ as informações sobre os titulares envolvidos;
- ⇒ a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- ⇒ os riscos relacionados ao incidente;
- ⇒ a causa do incidente;
- ⇒ o impacto do incidente;
- ⇒ os motivos da demora, no caso de a comunicação não ter sido imediata; e
- ⇒ as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente.

10. COMUNICAÇÃO DE INCIDENTES RELEVANTES RELACIONADOS AO AMBIENTE CIBERNÉTICO AO BANCO CENTRAL DO BRASIL

A instituição comunicará ao Banco Central do Brasil as ocorrências de incidentes relevantes e das interrupções dos serviços relevantes que configurem uma situação de crise pela instituição financeira, bem como das providências para o reinício das suas atividades.

11.....MECANISMOS PARA DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA NA INSTITUIÇÃO

A instituição promoverá a disseminação dos princípios e diretrizes da Segurança Cibernética por meio de programas de conscientização e capacitação, com o objetivo de fortalecer a cultura de segurança e realizará avaliação periódica dos colaboradores.
Para a disseminação da cultura de segurança cibernética a instituição adotará os seguintes mecanismos:

- ⇒ a instituição promoverá a disseminação dos princípios e diretrizes da Segurança Cibernética por meio de programas de conscientização, capacitação e avaliação periódica de pessoal;
- ⇒ a política e as regras de Segurança da Informação e Segurança Cibernética serão divulgadas e compartilhadas com todo o público-alvo desta política, e devem ser disponibilizadas de maneira que seu conteúdo possa ser consultado a qualquer momento, protegidas contra alterações;
- ⇒ a prestação, na página da instituição na internet, de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros;

⇒ a divulgação ao público, na página da instituição na internet, de resumo contendo as linhas gerais da Política de Segurança Cibernética.

12.....PROGRAMA DE SEGURANÇA CIBERNÉTICA

Conforme sua criticidade, o programa de segurança cibernética divide-se em:

⇒ Ações críticas: Correções emergenciais e imediatas para mitigar riscos iminentes;

⇒ Ações de Sustentação: Iniciativas de curto/médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro e permitindo que ações de longo prazo/estruturantes possam ser realizadas;

⇒ Ações Estruturantes: Iniciativas de médio/longo prazo que tratam a causa raiz dos riscos, voltadas para o futuro da Instituição.

13.....SEGURANÇA NO DESENVOLVIMENTO DE SISTEMAS DE APLICAÇÃO

O processo de desenvolvimento de sistemas de aplicação deve garantir a aderência às políticas de segurança da instituição e às boas práticas de segurança.

14.....MANUTENÇÃO DE DOCUMENTAÇÃO

Devem ficar à disposição do Banco Central do Brasil pelo prazo de 5 (cinco) anos:

⇒ o documento relativo à Política de Segurança Cibernética;

⇒ o documento relativo ao plano de ação;

⇒ o documento relativo ao plano de resposta a incidentes;

⇒ os relatórios anuais de que trata esta política;

⇒ a documentação referente às práticas de governança corporativa e de gestão e a verificação da capacidade do potencial prestador de serviço;

⇒ os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem, contado o prazo a partir da extinção do contrato;

⇒ os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle da implementação e da efetividade:

→ da Política de Segurança Cibernética, contado o prazo a partir da implementação;

→ do plano de ação, contado o prazo a partir da implementação;

→ do plano de resposta a incidentes, contado o prazo a partir da implementação;

→ dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, contado o prazo a partir da implementação.

15.....DA DIVULGAÇÃO

A Política de Segurança Cibernética e da Informação e as demais políticas e normas complementares da Instituição aqui referenciadas devem ser divulgadas ao Público-Alvo, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações, devendo estar disponíveis em local acessível aos colaboradores e protegidas contra alterações.
Além disso, será divulgado ao público, na página da instituição na internet, resumo contendo as linhas gerais da Política de Segurança Cibernética.

16.....MEDIDAS DISCIPLINARES

As violações a esta política estão sujeitas às sanções disciplinares previstas, nas normas internas da Instituição e na legislação vigente no Brasil e nos países onde as empresas estiverem localizadas, tais como: advertências (verbal e/ou escritas), suspensões e demissões com e sem justa causa.

17.....GLOSSÁRIO

Para efeitos deste documento e sobre sua divulgação, conceitua-se por:

- ⇒ Instituição: termo que remete à Multicred Sociedade de Crédito Direto S.A (Multicred SCD).
- ⇒ Colaboradores: o termo “colaboradores” inclui os administradores (conselheiros de administração e dirigentes/gestores), conselheiros fiscais e demais empregados, estagiários, trainees e temporários.
- ⇒ Compliance: Estar em conformidade com leis e regulamentos externos e internos.

18.....DISPOSIÇÕES FINAIS

É de responsabilidade de todos os acionistas, dirigentes e colaboradores conhecer as regras deste documento e adotar postura alinhada às boas práticas de Governança Corporativa.
Toda e qualquer situação, que não esteja contemplada neste documento, será analisada e orientada pela área de *Compliance*, e submetida a Diretoria Executiva.

19.....REVISÃO ANUAL

A área de TI, a diretoria da Multicred SCD, juntamente com a área de *Compliance*, são os responsáveis pela revisão e atualização anual desta política. Em casos de alterações na legislação vigente e mudanças na estrutura organizacional ou em processos da Instituição, os responsáveis poderão, a qualquer momento, iniciar o processo de revisão deste documento.

20.....REVISÕES EXCEPCIONAIS

Esta política será atualizada conforme ocorra novas inclusões e remoções de informações, se necessário, para que sejam integradas as respectivas modificações a serem implementadas no curto, médio e longo prazo, conforme plano de ação da instituição.

21.....COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO

A Diretoria da instituição, ao aprovar esta Política de Segurança Cibernética e da Informação, institui um compromisso para com a melhoria contínua dos procedimentos relacionados com a segurança cibernética e da informação, buscando sempre manter a instituição em conformidade com normas legais, permitindo à instituição prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados à segurança da informação e ao ambiente cibernético e proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.