POLÍTICA DE SEGURANÇA CIBERNÉTICA

1. INTRODUÇÃO

Esta Política de Segurança Cibernética ("Política") destina-se a atender à Resolução do Conselho Monetário Nacional nº 4.658, de 16 de abril de 2018, que dispõe sobre as diretrizes que devem ser observadas no estabelecimento e na implementação da Política e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

2. OBJETIVO

Esta Política estabelece práticas de governança corporativa e gestão adequadas para preservação da propriedade dos dados e sistemas de informações da Work SCD e de seus usuários, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento de informações de forma controlada, bem como o monitoramento, registro e tratamento de incidentes cibernéticos.

3. RESPONSABILIDADES

Responsabilidade da Segurança da Informação (1ª Linha de Defesa):

Todos os diretores, colaboradores, representantes e terceiros que atuem em nome da Work SCD ou, ainda, que prestem serviços à Work SCD são responsáveis:

- pelo uso das informações, sistemas e ativos de informação em linha com seu cargo, função e responsabilidades, com as suas finalidades e de acordo com as políticas, normas e diretrizes em vigor;
- pelo uso exclusivo de suas credenciais de acesso, inclusive pelas ações realizadas com uso de tais credenciais e pela segurança dos meios de autenticação; e
- pela notificação imediata ao gestor de sua equipe e à equipe de Segurança da Informação sobre qualquer violação, indício de violação aos termos desta Política e/ou de quaisquer documentos relacionados, direta ou indiretamente a esta Política.

Os gestores de equipes da Work SCD são responsáveis pela implementação das disposições estabelecidas por esta Política dentro de suas respectivas equipes, incluindo:

- a atribuição específica de papéis e responsabilidades de segurança da informação, considerando a segregação de funções, o alinhamento dos acessos concedidos às funções exercidas, bem como a garantia de exercício de funções de alto risco por pessoas qualificadas;
- a comunicação e divulgação desta Política e de quaisquer documentos relacionados, direta ou indiretamente a esta Política, a todos os integrantes de suas equipes e

terceiros que venha a envolver nas atividades de sua equipe (incluindo serviços terceirizados);

- o monitoramento, em conjunto com a equipe de Segurança da Informação, do cumprimento das disposições desta Política e de quaisquer documentos a ela relacionados pelos integrantes de suas equipes e terceiros que venha a envolver nas atividades de sua equipe (incluindo serviços terceirizados); e
- o fornecimento de informações sobre a implementação desta Política e demais documentos a ela relacionados para a equipe de Segurança da Informação, incluindo as evidências coletadas.

Supervisão da Segurança da Informação (2ª Linha de Defesa):

A equipe de Segurança da Informação é responsável pela coordenação da governança e da estrutura de segurança cibernética da Work SCD, em estrita observância aos termos da presente Política e de todos os documentos a ela relacionados (incluindo, mas não se limitando ao Plano de Ação e de Resposta a Incidentes).

4. MECANISMOS DE ACOMPANHAMENTO E CONTROLE

(a) Gestão de Acessos: a concessão de acessos ao ambiente e sistemas da Work SCD é realizada de forma individualizada, condicionado ao cargo/função e estritamente vinculado ao exercício das atividades atribuídas ao respectivo usuário;

(b) Gestão de equipamentos e dispositivos móveis: os equipamentos e dispositivos móveis utilizados para acessar o ambiente e os sistemas da Work SCD são previamente identificados e aprovados pela equipe de Tecnologia. A equipe de Segurança da Informação é responsável pela determinação dos parâmetros e requisitos técnicos aplicáveis à tais equipamentos e dispositivos;

(c) Segurança e gerenciamento da rede de dados: a segurança da rede de dados é realizada por meio do monitoramento e gerenciamento de rede pela equipe de Tecnologia, incluindo o controle dos acessos as redes internas e internet. Além dos mecanismos de autenticação, são adotados mecanismos de criptografia, prevenção e detecção de intrusão, bem como realiza testes e varreduras periódicos para detecção de intrusões;

(d) Segurança física da infraestrutura de rede e sistemas: os recursos e instalações de processamento de informações críticas para as atividades da Work SCD são mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e recursos de controle de acesso. Os equipamentos críticos possuem proteção contra desastre físico e recursos para combate a incêndio;

(e) Manutenção de estações de trabalho e telas limpas: todos os computadores e terminais utilizados pela Work SCD são mantidos desligados ou protegidos com mecanismos de travamento de tela controlado por senha quando não estão sendo monitorados ou utilizados. Quaisquer documentos e papéis que contenham informações sensíveis ou

confidenciais são armazenadas em lugar seguro quando não em uso, especialmente quando as estações de trabalho não estão sendo monitoradas;

(f) Classificação de relevância e sensibilidade dos dados e informações: os dados e informações processados e/ou armazenados no ambiente e nos sistemas da Work SCD são classificados quanto à sua relevância e sensibilidade com base na propriedade e confidencialidade de tais dados e informações;

(g) Manutenção de cópias de segurança: são efetuadas, periodicamente, cópias backup das informações e dados armazenados de seus servidores e bancos de dados para um ambiente de contingência apartado do ambiente de produção em operação regular;

(h) Desenvolvimento de sistemas e adoção de novas tecnologias: o desenvolvimento dos sistemas e adoção de novas tecnologias pela Work SCD estão sujeitos a avaliação e aprovação prévia da equipe de Segurança da Informação. O processo de avaliação visa assegurar que, nestes processos, os padrões de segurança da Work SCD sejam integralmente observados, que a segurança das informações, do ambiente e dos sistemas da Work SCD não sejam afetados, assegurando a não ocorrência de erros, perdas, modificações não autorizadas ou utilização indevida de informações e ativos da Work SCD; e

(i) Contratação de serviços relevantes de processamento e armazenamento de dados e computação em nuvem: em se tratando de serviços de processamento de dados e computação em nuvem, a sua relevância deve ser determinada pela equipe de Segurança da Informação, antes de qualquer contratação, com base na criticidade do serviço e na sensibilidade dos dados e informações a serem processados, armazenados ou gerenciados pelo respectivo fornecedor.

5. TRATAMENTO DE INCIDENTES

(a) Parâmetros para avaliação da relevância dos incidentes: são considerados incidentes relevantes de segurança cibernética aqueles que:

- Afetarem (ou com potencial de afetar) a confidencialidade, integridade e/ou a disponibilidade dos ativos considerados críticos;
- Ocasionarem (ou com potencial de ocasionar) a violação, pela Work SCD, de quaisquer leis e/ou regulamentações aplicáveis; e/ou
- Causarem (ou com potencial de causar) danos financeiros ou reputacionais à Work SCD.

(b) Diretrizes para tratamento dos incidentes classificados como relevantes: todo e qualquer incidente de segurança cibernética classificado como relevante é registrado pela equipe de Segurança da Informação, juntamente com as evidências e comunicações referentes ao respectivo incidente;

(c) Diretrizes para elaboração dos cenários de incidentes considerados nos testes de continuidade: os cenários de incidentes consideram impactos na confidencialidade, integridade ou disponibilidade de sistema de produção ou dados da Work SCD ou seus clientes; e

(d) Iniciativas para compartilhamento de informações sobre os incidentes relevantes entre instituições reguladas pelo Banco Central do Brasil: a Work SCD observará todos os requisitos e procedimentos que vierem a ser estabelecidos pelo Banco Central do Brasil para adotar o compartilhamento de informações sobre os incidentes relevantes identificados no curso de suas atividades.

6. PUBLICIDADE E DIVULGAÇÃO

A Work SCD divulgará a Política e suas futuras revisões a todos os seus colaboradores e prestadores de serviços. A versão atual da Política está disponível para consultas por meio de sistemas de compartilhamento de informações internas.

Este resumo atualizado da Política deve ser mantido disponível para consulta pelo público no *website* da Work SCD (www.workscd.com.br).