POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

EXCLUSIVO PARA USO INTERNO

ÍNDICE

1.	OBJETIVO	3
2.	ABRANGÊNCIA	3
3.	VIGÊNCIA, REVOGAÇÃO E CICLO DE REVISÃO	3
4.	DEFINIÇÃO	3
5.	DIRETRIZES GERAIS	3
6.	PAPÉIS E RESPONSABILIDADES	4
7.	NORMAS	6
8.	DESCUMPRIMENTO DA PSI	7
9.	REGULAMENTAÇÕES APLICAVÉIS	7

1. OBJETIVO

A Política de Segurança da Informação ("PSI") visa preservar a confidencialidade, integridade e disponibilidade das informações, descrevendo a conduta adequada para o seu manuseio, controle, proteção, descarte e compromisso, preservando as informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os colaboradores da KSM.

2. ABRANGÊNCIA

As diretrizes aqui estabelecidas deverão ser seguidas por todos colaboradores da KSM.

3. VIGÊNCIA, REVOGAÇÃO E CICLO DE REVISÃO

A PSI entrará em vigor na data de sua publicação e permanecerá vigente por prazo de 18 meses, podendo ser revisada antes deste período, no caso de alteração na legislação ou se houver alguma alteração das práticas de negócios da KSM.

4. DEFINIÇÃO

Colaborador: Funcionários de quaisquer cargos, estagiários e prestadores de serviços;

Confidencialidade: Informação acessível ou divulgada somente às pessoas autorizadas;

Disponibilidade: Pessoas autorizadas com acesso à informação sempre que necessário;

Integridade: Informações mantidas integras em seu formato original;

Normas de Segurança da Informação: Especificam os processos e controles que devem ser implementados para o alcance dos objetivos de segurança da informação definidos nesta política;

Prestadores de serviços: Pessoa jurídica ou física que mantenha contrato de prestação de serviço na KSM.

Segurança da Informação: É o conjunto de controles que visam garantir a preservação dos aspectos de confidencialidade, integridade e disponibilidade das informações;

Termos de ciência de Segurança: Declaração onde o colaborador atesta a ciência sobre todos os termos tratados nessa PSI, normas a ela vinculadas e a sua estrutura de funcionamento;

Visitante: Todo indivíduo que não mantenha qualquer vínculo formal com a KSM, ou seja, aqueles que não se enquadram na definição de Colaborador, conforme acima.

5. DIRETRIZES GERAIS

As diretrizes de Segurança da KSM têm os seguintes objetivos principais:

I. Garantir a confidencialidade, integridade e disponibilidade das informações dos seus clientes e proteger os dados e os sistemas da informação, contra acessos indevidos, pessoas e alterações não autorizadas;

II. Assegurar o treinamento contínuo e atualizado nas políticas e nos procedimentos de segurança da informação;

III. Definir controles que permitam a proteção das informações de acordo com seu grau de classificação;

IV. Criar e manter atualizados mecanismos de proteção contra arquivos maliciosos;

V. Avaliar e propor controles que visem oferecer segurança no desenvolvimento de sistemas

VI. Zelar para que os colaboradores estejam cientes do Termo de Ciência de Segurança da Informação ao iniciar as atividades na instituição;

VII. Assegurar que a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem no país ou no exterior, contemple as políticas, estratégias e estruturas necessárias para o adequado gerenciamento dos riscos quanto à terceirização de serviços;

VIII. Comunicar imediatamente à área de Segurança da Informação, bem como ao Compliance, qualquer violação desta PSI e/ou das demais normas e procedimentos de segurança da informação, a fim de se aplicar as medidas de remediação e penalidades previstas.

IX. Monitorar constantemente o ambiente tecnológico, avaliando e implementando medidas técnicas e melhoria de processos relacionadas a disciplina de Segurança.

6. PAPÉIS E RESPONSABILIDADES

Compete ao Colaborador:

I. Cumprir as regras estabelecidas na PSI, normas e procedimentos de segurança da informação, bem como as demais leis, regulamentos e normas aplicáveis pelos órgãos reguladores;

II. Proteger as informações contra acessos indevidos, divulgação não autorizados e descarte de forma segura;

III. Zelar para que os recursos tecnológicos sejam utilizados de forma eficaz, dentro das finalidades corporativas e de conhecimento pela KSM;

IV. Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (elevadores, taxi e quaisquer outros meios de transporte, restaurantes, etc.) ou com terceiros não autorizados;

V. Não compartilhar ou divulgar credenciais de acesso ou equipamentos sem a autorização explicita da área de Segurança da Informação. As senhas são de responsabilidade do usuário, sendo individual e intransferível, sendo substituídas de forma periódica;

VI. Estar atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da área de Segurança da Informação sempre que estiver com dúvidas;

VII. Solicitar quaisquer acessos ou perfis necessários as atividades profissionais por meio de ferramenta de chamados, contendo as aprovações do gestor imediato;

VIII. Não criar, adquirir ou realizar uso de softwares não homologados e não instalados pela área de Tecnologia.

IX. Comunicar a área de Segurança da informação quaisquer riscos de segurança da informação existentes na área de atuação.

Compete à Gestão da área de Segurança

I. Determinar as diretrizes de Segurança da Informação;

II. Aprovar e revisar periodicamente PSI;

III. Apresentação de assuntos relevantes a Diretoria quando cabível.

Compete às Gerências da KSM:

I. Reforçar junto as equipes o cumprimento das diretrizes de Segurança da Informação, bem como servir como replicador das boas práticas e controles.;

II. Propor ajustes e ferramentas à área de Segurança da Informação que auxilie nos processos de negócio das áreas;

III. Informar, à área de Segurança da Informação, sobre o encerramento de contratos em que os prestadores de serviços possuam qualquer tipo de acesso físico ou lógico às informações;

IV. Contribuir nos processos de revisão periódica de acessos ou em outras situações em que forem acionados pela área de Segurança da Informação.

Compete à área de Segurança da Informação:

I. Propor controles e melhorias relacionados ao tema segurança da informação;

II. Definir e documentar as políticas e procedimentos relacionados a operacionalização da segurança da informação;

III. Monitorar e analisar os alertas e informações relacionadas à segurança das informações;

IV. Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços;

V. Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais

VI. Disseminar a cultura de Segurança junto as demais áreas da Instituição;

VII. Participar dos projetos em que a área estiver envolvida acompanhando e sugerindo questões relacionadas ao tema da área.

Compete à área de Gente e Gestão:

I. Disponibilizar a política e as normas de Segurança da Informação para todos colaboradores e assegurar que o mesmo esteja ciente das diretrizes, normas e procedimentos internos;

II. Informar à área de Segurança da Informação todos os desligamentos, transferências, férias e modificações no quadro de funcional;

III. Garantir que os colaboradores tenham ciência e assinem o Termo de Ciência de Segurança da Informação no processo de integração.

Cabe à área de Infra de Tecnologia da Informação (TI):

I. Realizar as cópias de segurança do ambiente tecnológico;

II. Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos nesta PSI e normas adicionais;

III. Planejar, implantar, fornecer e monitorar a capacidade de armazenamento, processamento e transmissão necessárias para ambiente computacional.

Compete ao Compliance:

I. Aplicar as penas previstas na Matriz de Penalidades, após deliberação do Comitê de Compliance em casos onde necessitarem desta ação;

II. Avaliar as ações de remediação previstas para os casos de não conformidade a PSI e suas normas;

III. Receber e analisar os eventos de riscos de segurança da informação, sugerindo ações de remediação.

Compete à área Jurídica:

I. Requerer a inserção de cláusulas que obriguem o cumprimento desta PSI e demais leis, regulamentos e normas aplicáveis aos prestadores de serviços, cujos contratos tenham sua análise requerida ao departamento, assegurando que as informações sejam utilizadas apenas para sua finalidade dentro da KSM e preservando sua confidencialidade.

7. NORMAS

As informações geradas e os ambientes tecnológicos utilizados por seus respectivos usuários são de exclusiva propriedade da KSM, sendo vedada a sua utilização para fins pessoais ou quaisquer outros, que não os estabelecidos nos termos das normas e procedimentos.

Maiores detalhes de normas e procedimentos vinculados as atividades e processos, estão disponibilizados no portal da Intranet.

8. DESCUMPRIMENTO DA PSI

Na hipótese de violação desta PSI ou das normas de segurança da informação, a Diretoria, com o apoio das áreas de Segurança da Informação, *Compliance* e Recursos Humanos, determinarão as sanções administrativas que serão aplicadas ao infrator, sendo que:

i. Para os colaboradores, pode acarretar na aplicação de advertência e/ou suspensão ou desligamento formal conforme previsto na Matriz de Penalidades;

ii. Para os prestadores de serviços, pode acarretar na aplicação rescisória imediata do respectivo contrato estabelecido violado.

9. REGULAMENTAÇÕES APLICAVÉIS

- Resolução CMN, nº 4.658/2018 que dispõe sobre a política de segurança cibernética 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;

- Roteiro Básico de Programa de Qualificação operacional (PQO) da B3.