POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA KUMB INVEST S.A. CNPJ: 48.892.980/0001-00 (“KUMB INVEST”)

ÍNDICE

1. OBJETIVO

Estabelecer as diretrizes necessárias para práticas de gestão e normas de segurança da informação da gestora e, para tanto descrever a conduta adequada para o manuseio, armazenamento, controle e proteção das informações contra destruição, obsolescência, alteração, divulgação indevida e acessos não autorizados, sejam acidentalmente ou intencionalmente.

2. REGRAS GERAIS

2.1. PRINCÍPIOS

Toda informação produzida ou recebida pelos colaboradores no exercício de suas funções pertence à gestora, salvo exceções formalizadas com o custodiante indicado.

Equipamentos, sistemas e informações são destinados às atividades profissionais dos colaboradores.

A empresa de TI pode monitorar o uso de recursos tecnológicos para garantir disponibilidade e segurança das informações.

Informações e documentos dos clientes serão protegidos e armazenados conforme a legislação e regulamentação pertinentes.

Uso ou divulgação externa só é permitida com autorização expressa da diretoria.

O não cumprimento desta política configura violação das regras internas e pode resultar em medidas administrativas e legais cabíveis.

2.2. DEFINIÇÕES

Ativo da Informação: É o patrimônio composto por todos os dados e informações gerados, armazenados e manipulados durante a execução dos sistemas e processos.

Ativo de Processamento: É o patrimônio composto por todos os elementos de hardware e software necessários para execução dos sistemas e processos, tanto os produzidos internamente quanto os adquiridos ou contratados.

Controle de Acesso: Restrições ou direitos ao acesso aos Ativos de Informação e Ativos de Processamento.

Proprietário da Informação: Gestor da unidade organizacional onde a informação é criada ou da unidade que é a usuária primária da informação.

Senha Forte: Composta por caracteres maiúsculos e minúsculos, letras, números e caracteres especiais.

Usuário: Qualquer pessoa que se utilize dos recursos de tecnologia da informação na realização de suas tarefas.

Acesso Restrito: O acesso é permitido somente às pessoas autorizadas.

Fornecedor, Parceiro ou Prestador de Serviços: Pessoa Física ou Jurídica que fornece material, equipamento ou algum tipo de serviço.

Incidente de Segurança: Qualquer anomalia voltada à segurança, seja ela identificada por um sistema de detecção de intrusão, sistema de monitoramento ou reconhecida por uma pessoa.

Informação: Ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a gestor e consequentemente necessita ser adequadamente protegida para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos do negócio.

LOG: Registro de transações efetuadas em um sistema como acessos, indicando pessoa, data, hora, valor incluído, alterado, deletado etc.

Mesa Limpa / Tela Limpa: Documentos não públicos devem ser protegidos e não deixados à vista. No ambiente de trabalho, documentos físicos devem ser guardados para evitar acesso não autorizado.

Acordo de Confidencialidade: Documento necessário para informar e impor que os dados/informações da gestora são confidenciais e privados ao uso do negócio.

2.3. CLASSIFICAÇÃO DE INFORMAÇÃO E RETENÇÃO

Todo ativo da informação deve estar associado a um Proprietário e deve ser classificado com base em sua relevância para a organização e no impacto para o negócio na ocorrência de sinistros que ocasionem sua indisponibilidade.

A informação deve ser classificada e rotulada para indicar o nível esperado de proteção quando de seu tratamento, conforme definido na POL-TI-005 - Política de Segurança Cibernética.

- De acordo com a importância da informação ao negócio e quanto às exigências legais, toda informação é classificada e armazenada. Esses parâmetros de classificação, retenção e destruição estão descritos nos procedimentos e controles de sistemas, banco de dados e áreas de armazenamento de documentos na rede.

- Os documentos armazenados localmente no desktop do usuário ou em impressões de papel ficam a critério do colaborador decidir sobre a guarda, sigilo e integridade da informação.

- Os documentos classificados como “confidenciais” ou “sensível” devem ser mantidos em local seguro durante a ausência do responsável, observando o princípio de manter a mesa limpa e a informação protegida.

- Os documentos impressos e inutilizados, independente da sua classificação devem ser destruídos apropriadamente pelo colaborador.

2.4. INFRAESTRUTURA

Para a infraestrutura devem ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a gestora julgar necessário para reduzir os riscos dos seus ativos de informação.

Os ambientes de tecnologia são segregados e rigidamente controlados, garantindo o isolamento necessário em relação a Ambientes de Testes, de Homologação de Sistemas e de Produção.

2.5. GESTÃO DE ATIVOS

Os dispositivos, licenciamentos e equipamentos são inventariados e controlados pela área de TI. Este monitoramento de ativos é gerenciado remotamente pelas ferramentas administrativas da infraestrutura.

Os equipamentos disponibilizados aos colaboradores são propriedade da gestora. Cabe aos usuários a utilização de forma correta para as atividades da instituição e seguir os procedimentos operacionais fornecidos pelas gerências responsáveis. Atualizações e correções de ambientes, sistemas e equipamentos seguem o processo de Gerenciamento de Mudanças, conforme procedimento de Gestão de Mudanças de TI.

Todo equipamento deve possuir restrição de acesso conforme o perfil do usuário. A transferência ou divulgação de qualquer software ou instruções de computador para terceiros só pode ser realizada com a devida identificação do solicitante, verificação positiva e em conformidade com a classificação da informação e a necessidade do destinatário.

Arquivos pessoais ou não pertinentes ao negócio da gestora (fotos, músicas, vídeos, etc.) não devem ser copiados ou movidos para os drives de rede, evitando sobrecarga nos servidores. Esses arquivos podem ser excluídos definitivamente se identificados.

Os colaboradores devem informar à equipe de TI sobre qualquer dispositivo estranho conectado ao seu computador. A abertura ou manuseio de computadores para reparos deve ser realizado exclusivamente por técnicos de TI ou terceiros autorizados.

Os colaboradores devem manter a configuração de segurança dos equipamentos disponibilizados pela gestora e proteger todos os dispositivos com senha quando não estiverem em uso, assumindo a responsabilidade como custodiante das informações contidas nos equipamentos.

Em caso de roubo ou furto de equipamentos da empresa atribuídos aos operadores, onde se comprovar negligência ou falta de cuidado, a empresa poderá exigir o reembolso total ou parcial do valor do equipamento. Essa medida visa garantir a responsabilidade dos colaboradores na proteção e uso adequado dos ativos de TI, conforme estabelecido no Termo de Aceite e Uso de Equipamentos.

2.6. DISPOSITIVOS MÓVEIS

"Dispositivo móvel" refere-se a equipamentos portáteis de propriedade da gestora ou aprovados pela Gerência de TI, como notebooks, smartphones e pen drives.

Esta regra aplica-se a todos os colaboradores que utilizam tais equipamentos, estabelecendo critérios de manuseio, prevenção e responsabilidade.

- A gestora reserva-se o direito de inspecionar os equipamentos a qualquer momento para manutenção de segurança.
- O suporte técnico aos dispositivos móveis segue o mesmo fluxo de suporte a incidentes.
- Todos os dispositivos móveis devem ter senhas de bloqueio automático.

- Não é permitida a alteração das configurações de segurança e geração de logs dos sistemas operacionais sem autorização e supervisão da área de TI.
- A reprodução ou instalação não autorizada de software nos dispositivos móveis constitui uso indevido e infração legal.
- Em caso de furto ou roubo, o colaborador deve notificar imediatamente seu gestor direto e a área de TI, além de registrar um boletim de ocorrência (BO) com as autoridades policiais.
- O uso indevido do dispositivo móvel implica na responsabilidade exclusiva do colaborador por quaisquer danos causados à gestora e/ou a terceiros.

2.7. TRABALHO REMOTO

Para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto, são adotadas as seguintes medidas para gerenciar os riscos decorrentes do uso de dispositivos móveis:

- Utilizar somente equipamentos autorizados pela gestora;
- As informações processadas e acessos concedidos não devem ser compartilhados com terceiros ou armazenadas em ambientes e/ou equipamentos de uso pessoal;
- Aplicar a mesma política de acesso de usuário para perfis internos, conforme a atividade desempenhada;
- As políticas e controles de segurança devem ser seguidas, independentemente do acesso ser remoto;
- Controlar o uso de serviços e aplicações web conforme a classificação da informação e regras de acesso;
- Evitar trabalho remoto em locais públicos, salas de reuniões e outras áreas desprotegidas.

2.8. ACESSOS

2.8.1. Acesso Físico

Todo acesso físico em áreas seguras deve ser controlado por meio de sistema de autenticação.

As diretrizes e normas de Segurança Física aos ambientes objetivam evitar acesso não autorizado, danos e interferências às instalações físicas ou informações da gestora.

Mesa limpa e tela limpa devem ser adotados por todos os colaboradores, a fim de reduzir o risco de acesso não autorizado ou danos a papéis, mídias, recursos e instalações de processamento de informações.

Todas as pessoas que acessam as dependências da gestora, com acesso controlado, devem ser identificadas e registradas via sistema CFTV e leitor biométrico para entrada e saída por botoeira.

O registro do sistema de CFTV é configurado para detecção de movimento em um HD interno e replicado para armazenamento e retenção.

O acesso das pessoas fica restrito e períodos estritamente restritos a execução dos serviços relacionados às suas atividades ou a períodos autorizados.

2.8.2. Acesso Lógico

- A gestão do acesso lógico é utilizada para permitir acesso à informação digital e a serviços de informação a pessoas autorizadas, de modo a impedir os acessos não autorizados.
- Todo colaborador deve utilizar senhas de bloqueio automático para seu desktop / laptop.
- O Proprietário da informação é definido de acordo com os procedimentos de acessos e permissões de cada ambiente, equipamento e/ou sistema.
- As configurações de segurança são especificadas em documento próprio para controles de detecção, prevenção e recuperação contra códigos maliciosos e intrusões.
- A utilização de Internet em rede corporativa é submetida a regras e políticas de controles em ferramentas e equipamentos da infraestrutura da gestora, assim como a interceptação e proteção contra eventuais ataques maliciosos.

2.8.3. Gerenciamento de Operações

- Para garantir a operação segura e correta dos recursos de processamento da informação, os procedimentos operacionais são tratados em documento próprio, onde são descritos os parâmetros de segurança, acesso e controles. As mudanças autorizadas seguem o fluxo de gerenciamento de mudanças.
- Todo o ambiente de sistemas e base de dados não possui desenvolvimento interno e é terceirizado de acordo com o processo de contratação de terceiros.
- Os códigos fontes não são armazenados nas estações e/ou servidores da gestora.
- Atividades de homologação e testes são executadas em ambientes segregados para se evitar quebras de segurança por senhas de teste e/ou por erros em ambiente produtivo.
- Os sistemas devem ser implantados em Produção somente após passarem por testes de homologação pelas áreas responsáveis e após a aprovação do requisitante.

2.8.4. Gestão de Incidentes de Segurança

- Os colaboradores e prestadores de serviços devem ser instruídos a reportarem pontualmente todo incidente que possa comprometer a Segurança da Informação. A informação deve ser imediatamente comunicada a área de TI para providencias cabíveis.
- Toda ocorrência de incidente é registrada na ferramenta de Service Desk para registro, tratativas e controles, com o objetivo de atuar na causa e criar ferramentas, melhorias e métodos preventivos contra futuras reincidências.
- Todos os colaboradores recebem o devido treinamento na Política de Segurança da Informação anualmente, mantendo todos atualizados e conscientizados da importância em se seguir às normas determinadas na Política de Segurança da Informação.

2.8.5. Gestão da Continuidade do Negócio

Para garantir a continuidade dos processos considerados críticos ao negócio da gestora, e objetivando minimizar impactos em virtude de eventuais paralisações, foram mapeados os riscos e seus respectivos planos de ação.

2.8.6. Registros e Monitoramento

O monitoramento utilizado pela gestora registra os eventos e atividades de sistemas, usuários e recursos de infraestrutura no que diz respeito a acessos, exceções, falhas e eventos de segurança da informação produzidos. Estes registros são mantidos e analisados regularmente para preservação e segurança da Informação.

Estes registros são utilizados para melhorias e apresentação à área de Gestão de Riscos, ao Comitê de Gestão de Riscos e Capital, bem como às requisições de auditorias.

2.8.7. Acordo de Confidencialidade

O acordo de confidencialidade é necessário e deve ser utilizado para informar e impor que os dados/informações da gestora são confidenciais e privados ao uso do negócio.

Os funcionários, pessoas, e/ou empresas contratadas devem assinar o acordo de confidencialidade como parte dos termos e condições iniciais de contratação.

Para colaboradores casuais e prestadores de serviços que não sejam cobertos por um contrato existente, devem assinar o acordo de confidencialidade, antes de ter acesso às instalações e informações de processamento da informação.

2.8.8. Ausência ou Desligamento do Funcionário

Na ausência temporária (igual ou superior a cinco dias úteis) ou no desligamento de um funcionário, o RH ou gestor responsável deve comunicar a área de TI para que os acessos às dependências, aos bens e às informações deste usuário sejam bloqueados / retirados.

A exceção deve ser somente aos usuários com permissão de férias.

Em caso de desligamento, devem ser devolvidos à gestora os bens e chaves disponibilizados, cancelados todos os poderes e permissões a ele concedidos e todos os acessos a recursos tecnológicos concedidos anteriormente.

3. RESPONSABILIDADES

Detalhes das responsabilidades por área de atuação:

3.1. DIRETORIA

- Aprovar a política de Segurança da Informação;
- Disponibilizar ferramentas e recursos computacionais necessários para atender as regras de segurança e executar atividades da organização;
- Promover a cultura de segurança da informação em toda a organização.

3.2. COMPLIANCE

- Aprovar a nomeação dos “proprietários” da informação;
- Garantir que as políticas, procedimentos e manuais internos estejam em conformidade com a regulamentação vigente e melhores práticas;
- Realizar a publicação e divulgação dos documentos internos nas plataformas de acesso dos colaboradores;

- Gerenciar todos os documentos emitidos e garantir a revisão e atualização periódica junto aos responsáveis;
- Assegurar que o processo de aprovação de todos os documentos siga as regras e alçadas estabelecidas.

3.3. PROPRIETÁRIO DA INFORMAÇÃO

- Realizar a classificação dos ativos de informação e revisar periodicamente;
- Aprovar direitos de acesso conforme as definições funcionais e para exceções não previstas;
- Definir o tempo de retenção da informação com base em orientações regulatórias e legais;
- Aprovar novas categorias de utilização para a informação e mudanças relevantes em sistemas antes de entrarem em produção;
- Revisar relatórios de tentativas de intrusão ou violação da informação;
- Revisar regularmente os níveis e perfis funcionais de acesso à informação;
- Designar um substituto capacitado para assumir responsabilidades na ausência do proprietário.

3.4.GESTORES

- Controlar e proteger as informações geradas ou confiadas à área de negócio durante todo o seu ciclo de vida;
- Informar os usuários sobre as políticas de segurança e procedimentos estabelecidos;
- Identificar e classificar as informações conforme os critérios adotados pela gestora, revisando periodicamente essa classificação;
- Autorizar e revisar periodicamente os acessos à informação e aos sistemas sob sua responsabilidade;
- Informar à Tecnologia da Informação sobre a ausência ou desligamento de usuários especiais para bloquear ou revogar credenciais de acesso.

3.5. TECNOLOGIA DA INFORMAÇÃO – TI

- Coordenar esforços e implementar ferramentas e controles para reduzir riscos;
- Desenvolver e divulgar programas de capacitação em segurança da informação;
- Monitorar o uso e a adesão às políticas e regras estabelecidas;
- Detectar incidentes de segurança e privacidade da informação e implementar medidas corretivas.

3.6. RECURSOS HUMANOS – RH

- Garantir que novos colaboradores recebam treinamento e assinem termos de responsabilidade;
- Comunicar a área de Tecnologia da Informação a ausência, desligamento ou afastamento de usuário para bloqueio ou revogação de credenciais de acesso físico e a recursos computacionais da gestora;

- Garantir que os ativos de informação confiados aos usuários sejam devolvidos quando ocorrer desligamento ou afastamento.

3.7. TODAS AS ÁREAS

- Cumprir a todas as diretrizes determinadas pelo Proprietário da Informação;
- Receber treinamento adequado para que possam cumprir as determinações corretamente.

4. DOCUMENTOS INTERNOS RELACIONADOS

- POL-TI-005 - Política de Segurança Cibernética;
- Termo de Responsabilidade para Utilização de Recursos Tecnológicos.

5. REGULAMENTAÇÃO EXTERNA

- Resolução 4.893 de 26.08.2021 do CMN – 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 autorizadas a funcionar pelo Banco Central do Brasil.
- ABNT NBR ISO/IEC 27002:2013.

6. GLOSSÁRIO

- AZURE: é uma plataforma de armazenamento e execução de mídias, com vários serviços de nuvem interligados. O software apresenta junção de análise, computação, banco de dados, serviços móveis, rede, armazenamento e Web.
- AWS: Amazon Web Services (ou AWS) serviços de infraestrutura de TI para empresas por meio de serviços web – a chamada computação na nuvem.
- CFTV: Circuito Fechado de TV) é um sistema de captação e retenção de imagens feita por câmeras digitais ou analógicas e que permite a videovigilância através de monitores conectados à uma rede central.
- CPD: centro de processamento de dados, também conhecido como data center, é um local onde estão concentrados os sistemas computacionais de uma empresa ou organização, como um sistema de telecomunicações ou um sistema de armazenamento de dados, além do fornecimento de energia para a instalação.
- TI: Tecnologia da Informação.

7. COMPLIANCE

Em caso de dúvidas quanto ao disposto nesta Política, o colaborador deve entrar em contato com a área de Compliance.

8. DIVULGAÇÃO

O conteúdo desta Política é propriedade da gestora e destina-se ao uso e divulgação interna e externa.

INFORMAÇÕES DE CONTROLE

Vigência: 04.2026 a 04.2027

Versão	Área Responsável	Descrição resumida da alteração	Data da Publicação
05	Tecnologia da Informação	Revisão	04.2026