

	Política de Segurança da Informação	Código: POL-SGSI-1 Revisão: 4 Data: 14/10/2026
Unidade: BAMEX - Teresina-PI		Área: Sistema de Gestão de Segurança da Informação

1. OBJETIVO

Esta Política estabelece o compromisso da BAMEX BENEFÍCIOS INSTITUIÇÃO DE PAGAMENTO LTDA, doravante BAMEX, com a proteção das informações sob sua responsabilidade e define os princípios, as diretrizes e as responsabilidades que orientam o Sistema de Gestão de Segurança da Informação, em conformidade com a ABNT NBR ISO/IEC 27001:2022. É o documento de mais alto nível do SGSI e orienta a elaboração, a aplicação e a revisão do MAN-SGSI-1, das políticas tópicas e de todos os procedimentos, planos e controles do sistema.

2. ABRANGÊNCIA

Esta Política aplica-se às unidades BAMEX Teresina/PI e BAMEX Campinas/SP, a todos os processos incluídos no escopo do SGSI, à plataforma tecnológica BAMEX, aos sistemas corporativos, à infraestrutura hospedada em fornecedores e às informações próprias, de clientes, de estabelecimentos credenciados, de usuários da plataforma e de colaboradores, em qualquer meio, físico, digital ou verbal. Obriga a Alta Direção, os diretores, gestores, colaboradores, estagiários, aprendizes, prestadores de serviço, consultores, fornecedores, parceiros e qualquer pessoa que acesse informações ou ativos da BAMEX, independentemente do vínculo. Os limites, as interfaces e as exclusões do SGSI são os definidos na Declaração de Escopo do SGSI.

3. DECLARAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A BAMEX estabelece a segurança da informação como compromisso institucional, assegurando a confidencialidade, a integridade e a disponibilidade das informações sob sua responsabilidade. A organização compromete-se a atender aos requisitos legais, regulatórios e contratuais aplicáveis, a promover a conscientização e a capacitação dos colaboradores, a gerir os riscos e as vulnerabilidades de segurança da informação e a manter a continuidade e a disponibilidade dos serviços essenciais. Compromete-se ainda a proteger seus ativos contra ameaças internas e externas, a tratar os incidentes de segurança e a manter rotinas de cópia e recuperação de dados. A política orienta a definição dos objetivos de segurança da informação, é comunicada aos colaboradores, está disponível às partes interessadas pertinentes e é mantida sob melhoria contínua do sistema de gestão.

4. COMPROMISSO DA ALTA DIREÇÃO

A Alta Direção da BAMEX reconhece a segurança da informação como condição para a continuidade do negócio, para a confiança dos clientes e da rede credenciada na plataforma BAMEX e para o cumprimento das obrigações legais, regulatórias e contratuais, e compromete-se a estabelecer, implementar, manter e melhorar continuamente o SGSI; a prover os recursos humanos, tecnológicos e financeiros necessários; a aprovar e acompanhar os objetivos de segurança da informação; a assegurar que os riscos sejam avaliados e tratados conforme os critérios de aceitação aprovados; a integrar os requisitos do SGSI aos processos de negócio e às decisões estratégicas; a promover a cultura de segurança da informação em todos os níveis; e a exigir o cumprimento desta Política de todas as pessoas abrangidas, aplicando as consequências definidas no capítulo 10 em caso de descumprimento.

5. PRINCÍPIOS

A segurança da informação na BAMEX orienta-se pelos seguintes princípios: preservação da confidencialidade, da integridade e da disponibilidade das informações, e da autenticidade quando aplicável; abordagem baseada em riscos, com controles proporcionais à criticidade dos ativos e ao impacto potencial; menor privilégio e necessidade de conhecimento no acesso às informações; segregação de funções nas atividades críticas; responsabilidade

	Política de Segurança da Informação	Código: POL-SGSI-1 Revisão: 4 Data: 14/10/2026
Unidade: BAMEX - Teresina-PI		Área: Sistema de Gestão de Segurança da Informação

individual pelo uso das credenciais e dos ativos; rastreabilidade das atividades relevantes; conformidade com a legislação aplicável, em especial a Lei nº 13.709/2018, e com os requisitos regulatórios e contratuais; proteção da cadeia de fornecimento; e melhoria contínua com base em evidências.

6. DIRETRIZES

Diretriz	Conteúdo
Governança	O SGSI é dirigido pela Alta Direção, coordenado pelo Coordenador(a) do SGSI e supervisionado pelo Comitê do SGSI, ambos designados por ato formal, e é registrado, controlado e evidenciado no GSG SISTEM, repositório oficial dos documentos, riscos, ações, incidentes, auditorias, treinamentos, fornecedores, indicadores, objetivos e análises críticas do sistema.
Contexto e partes interessadas	As questões internas e externas do SGSI são mantidas no módulo de Planejamento Estratégico do GSG SISTEM e as partes interessadas e seus requisitos na Matriz de Partes Interessadas do SGSI, ambas revisadas no mínimo anualmente, conforme o POP-SGSI-1.
Ativos e classificação	Toda informação e todo ativo de informação têm proprietário designado, são inventariados e classificados como Pública, Interna, Confidencial ou Restrita, e são manuseados, transmitidos, retidos e descartados conforme a classificação, nos termos do POP-SGSI-2.
Riscos	Os riscos de segurança da informação são identificados, avaliados pelos fatores Gravidade, Frequência e Dificuldade de Detecção e tratados conforme o POP-SGSI-3; riscos não toleráveis exigem tratamento obrigatório e a aceitação de risco residual não tolerável é decisão exclusiva do Diretor Presidente. Os controles selecionados são os registrados na Declaração de Aplicabilidade.
Acessos e identidades	O acesso às informações e sistemas é concedido por perfil, mediante solicitação e aprovação formais, revisado periodicamente e revogado no mesmo dia útil do desligamento ou do fim da necessidade, conforme o POP-SGSI-4. Cada pessoa possui identidade individual e intransferível, protege suas credenciais, não as compartilha e utiliza autenticação multifator onde exigida, conforme o POP-SGSI-5. Os certificados digitais organizacionais são informação Restrita, de uso individual e rastreado.
Uso aceitável	Os recursos de tecnologia da BAMEX destinam-se às atividades profissionais. É vedado compartilhar credenciais ou certificados, instalar software não homologado, armazenar informações corporativas em contas ou dispositivos pessoais, inserir informação Confidencial ou Restrita em ferramentas de inteligência artificial externas não homologadas, enviar documentação licitatória fora do fluxo autorizado e compartilhar informação sem autorização do proprietário, conforme a POL-SGSI-2.
Operação segura	A Diretoria de Tecnologia mantém o registro e o monitoramento de eventos de segurança, a gestão controlada de mudanças, as cópias de segurança com testes de restauração, a gestão de vulnerabilidades com prazos por criticidade, a proteção contra código malicioso e os planos de continuidade dos serviços de TIC, conforme os POP-SGSI-6, 7, 8, 10, 11 e 22, com objetivos de recuperação definidos para a plataforma BAMEX.
Incidentes	Todo colaborador e terceiro comunica imediatamente qualquer suspeita de evento de segurança da informação pelo canal definido no POP-SGSI-9, sem tentar investigar ou corrigir por conta própria. Os incidentes são registrados, classificados, contidos, tratados e analisados, e os que envolvam dados pessoais são avaliados quanto à comunicação à ANPD e aos titulares.
Fornecedores	Os fornecedores são classificados como críticos ou normais, homologados antes da contratação e do acesso, vinculados por cláusulas de segurança da informação e monitorados pelas avaliações de entrega, conforme o POP-SGSI-12. Nenhum terceiro acessa informação da BAMEX sem contrato ou termo assinado.
Dados pessoais	A BAMEX trata dados pessoais de colaboradores, clientes, estabelecimentos credenciados e usuários da plataforma conforme a Lei nº 13.709/2018, com finalidade definida, minimização, segurança e atendimento aos direitos dos titulares, sob orientação do Encarregado pelo Tratamento de Dados Pessoais e conforme a POL-SGSI-3.

	Política de Segurança da Informação	Código: POL-SGSI-1 Revisão: 4 Data: 14/10/2026
Unidade: BAMEX - Teresina-PI		Área: Sistema de Gestão de Segurança da Informação
Diretriz	Conteúdo	
Pessoas	As competências de segurança da informação de cada função constam do Perfil de Cargo, todos recebem integração antes do acesso e reciclagem anual, e a conscientização é contínua, conforme o POP-SGSI-17. As responsabilidades de segurança da informação integram as atribuições de cada cargo e permanecem após o desligamento no que se refere à confidencialidade.	
Documentação e conformidade	Os documentos do SGSI são controlados no módulo de Documentos do GSG SISTEM conforme o POP-SGSI-13, e somente versões vigentes são utilizadas. A conformidade do SGSI é verificada por auditoria interna anual conforme o POP-SGSI-14, as não conformidades são tratadas com análise de causa raiz conforme o POP-SGSI-15 e a Alta Direção analisa criticamente o sistema ao menos uma vez por ano conforme o POP-SGSI-16.	

7. OBJETIVOS DE SEGURANÇA DA INFORMAÇÃO

A Alta Direção estabelece os objetivos de segurança da informação a seguir, validados em 25/06/2026, coerentes com a declaração do capítulo 3 e com os riscos priorizados. Cada objetivo é cadastrado no GSG SISTEM com meta, prazo, ação, recursos e responsável, e vinculado a indicador do módulo de Indicadores. As metas numéricas são calibradas a partir do tratamento de riscos do requisito 6.1 e a forma de avaliação é o acompanhamento dos indicadores na análise crítica do SGSI, com registro de desvios e ações corretivas.

Objetivo	Indicador	Meta de referência	Periodicidade	Responsável
Conscientizar os colaboradores em segurança da informação	Percentual de colaboradores treinados	100%	Ciclo de implantação	RH e TI
Reduzir vulnerabilidades críticas em sistemas	Nº de vulnerabilidades críticas abertas	Zero em produção	Trimestral	TI
Assegurar a disponibilidade dos serviços essenciais	Disponibilidade mensal dos serviços	Meta a definir	Mensal	TI
Testar a restauração de backups	Nº de testes de restauração bem-sucedidos	Ao menos um por ciclo	Trimestral	TI
Tratar os riscos de SI priorizados	Ações de tratamento concluídas no prazo	100%	Conforme plano	Comitê do SGSI

Novos objetivos podem ser estabelecidos pela Alta Direção na análise crítica ou sempre que o contexto, os riscos ou os requisitos o exigirem.

8. POLÍTICAS TÓPICAS

Esta Política desdobra-se nas políticas tópicas abaixo, aprovadas pela Direção em 25/06/2026, cujas regras operacionais constam dos documentos indicados. A aplicabilidade de cada uma é confirmada pelo escopo, pela avaliação de riscos e pela Declaração de Aplicabilidade. As políticas tópicas são aprovadas no nível apropriado, comunicadas às partes pertinentes e analisadas criticamente em intervalos planejados ou quando ocorrerem mudanças significativas.

Política tópica	Documento que a desdobra
Controle de acesso	POP-SGSI-4 Gestão e Controle de Acessos; POP-SGSI-5 Gestão de Identidades e Autenticação; TAB-SGSI-3 Matriz de Perfis e Direitos de Acesso

	Política de Segurança da Informação	Código: POL-SGSI-1 Revisão: 4 Data: 14/10/2026
Unidade: BAMEX - Teresina-PI		Área: Sistema de Gestão de Segurança da Informação
Política tópica	Documento que a desdobra	
Uso aceitável de ativos	POL-SGSI-2 Termo de Uso Aceitável de Ativos, Recursos de TI e Trabalho Remoto	
Classificação da informação	POP-SGSI-2 Gestão de Ativos e Classificação da Informação	
Cópias de segurança	POP-SGSI-8 Gestão de Backup e Recuperação	
Criptografia e gestão de chaves	POP-SGSI-24 Criptografia, Chaves e Certificados Digitais	
Dispositivos móveis e trabalho remoto	POL-SGSI-2 Termo de Uso Aceitável de Ativos, Recursos de TI e Trabalho Remoto	
Gestão de vulnerabilidades	POP-SGSI-10 Gestão de Vulnerabilidades	
Proteção contra malware	POP-SGSI-22 Serviços em Nuvem, Configuração Segura e Gestão de Ativos de TI	
Transferência de informações	POP-SGSI-2 Gestão de Ativos e Classificação da Informação; POP-SGSI-23 Retenção, Mascaramento, Prevenção de Vazamento e Descarte Seguro	
Desenvolvimento seguro	POP-SGSI-19 Desenvolvimento Seguro e Gestão de Ambientes	
Gestão de incidentes	POP-SGSI-9 Gestão de Incidentes de Segurança da Informação	
Continuidade da segurança	POP-SGSI-11 Continuidade dos Serviços de TIC e Recuperação de Desastres; PLA-SGSI-3 Plano de Continuidade de TIC e Gestão de Crise	

9. RESPONSABILIDADES

Função	Responsabilidade
Diretor Presidente	Aprova esta Política e os objetivos, provê os recursos, preside a análise crítica, decide sobre a aceitação de risco residual não tolerável, aprova as comunicações externas sobre incidentes e aplica as consequências do descumprimento.
Diretores de área	Aplicam esta Política nas suas diretorias, aprovam os documentos dos seus processos, atuam como proprietários dos ativos e riscos das suas áreas e respondem pelo tratamento das não conformidades.
Diretor de Tecnologia	É o proprietário dos ativos e riscos tecnológicos, responde pela operação segura da plataforma BAMEX, da infraestrutura e dos sistemas e pela relação com os fornecedores de tecnologia.
Coordenador(a) do SGSI	Coordena a implementação, a manutenção e a melhoria do SGSI, mantém a estrutura documental, coordena riscos, incidentes, auditorias, treinamentos, objetivos e indicadores e relata o desempenho do SGSI à Alta Direção.
Comitê do SGSI	Supervisiona o SGSI, valida riscos, controles, Declaração de Aplicabilidade e resultados, delibera sobre exceções e escala à Alta Direção o que exceder sua alçada.
Encarregado pelo Tratamento de Dados Pessoais	Função exercida pelo Coordenador do SGSI, formalmente designado como Encarregado pelo Tratamento de Dados Pessoais (DPO); apoia a conformidade com a Lei nº 13.709/2018, atua como canal de comunicação com a ANPD e os titulares e orienta os colaboradores quanto às práticas de proteção de dados pessoais.
Gestores de processo	Aplicam esta Política nos seus processos, atuam como proprietários dos ativos e riscos vinculados, aprovam os acessos das suas equipes, comunicam eventos e tratam as não conformidades.
Colaboradores, estagiários, aprendizes e terceiros	Cumrem esta Política e os procedimentos do SGSI, protegem as credenciais e as informações a que têm acesso, participam dos treinamentos, comunicam eventos e respondem individualmente pelo uso dos ativos.
Fornecedores	Cumrem os requisitos de segurança da informação contratados, comunicam incidentes e mudanças e devolvem ou eliminam as informações da BAMEX ao término da relação.

	Política de Segurança da Informação	Código: POL-SGSI-1 Revisão: 4 Data: 14/10/2026
Unidade: BAMEX - Teresina-PI		Área: Sistema de Gestão de Segurança da Informação

10. SANÇÕES E CONSEQUÊNCIAS DO DESCUMPRIMENTO

O descumprimento desta Política, das políticas tópicas, dos procedimentos do SGSI ou das regras de uso aceitável sujeita o infrator a medidas proporcionais à gravidade, à intenção, à reincidência e ao impacto, apuradas com registro no módulo de Ações e Ocorrências do GSG SISTEM e com direito de manifestação do envolvido, conforme a escala a seguir.

Medida	Aplicação
Orientação formal registrada	Descumprimento sem impacto e sem intenção, como uso de canal não oficial ou omissão de ciência de documento.
Advertência escrita	Descumprimento com impacto limitado ou reincidência de descumprimento orientado, como armazenamento de informação corporativa em conta pessoal ou instalação de software não homologado.
Suspensão	Descumprimento com impacto relevante ou reincidência de conduta advertida, como compartilhamento de credencial ou envio de informação Confidencial fora do fluxo autorizado.
Rescisão do contrato de trabalho	Descumprimento doloso ou de impacto severo, inclusive por justa causa nas hipóteses da legislação trabalhista, como compartilhamento de certificado digital, exposição intencional de informação Restrita ou de dados pessoais, fraude ou sabotagem.
Terceiros e fornecedores	Revogação imediata dos acessos, rescisão contratual e aplicação das penalidades contratuais.
Qualquer caso	Comunicação às autoridades e adoção das medidas cíveis e criminais cabíveis quando a conduta configurar ilícito.

As medidas aplicáveis a colaboradores são conduzidas pelo Departamento Pessoal e Recursos Humanos com o gestor da área e o Jurídico, e as aplicáveis a terceiros pelo gestor contratante com o Jurídico. A aplicação de sanção não dispensa o tratamento do incidente ou da não conformidade correspondente.

11. COMUNICAÇÃO, REVISÃO E APROVAÇÃO

Esta Política é comunicada a todos os colaboradores e terceiros com acesso na admissão, na contratação e a cada revisão, com registro de ciência no módulo de Documentos do GSG SISTEM, reforçada na reciclagem anual e disponibilizada às partes interessadas externas pertinentes, conforme o POP-SGSI-18. É revisada no mínimo anualmente e sempre que houver mudança significativa no contexto, no escopo, nos riscos, nos requisitos legais, regulatórios ou contratuais ou nos resultados do SGSI, conforme o POP-SGSI-13, e sua aprovação é registrada no módulo de Documentos pelo Diretor Presidente.

12. DOCUMENTOS RELACIONADOS

MAN-SGSI-1, Manual do Sistema de Gestão da Segurança da Informação.

Declaração de Escopo do SGSI e Matriz de Partes Interessadas do SGSI.

POL-SGSI-2 e POL-SGSI-3, políticas complementares.

POP-SGSI-1 a POP-SGSI-24, procedimentos do SGSI.

TAB-SGSI-1, Declaração de Aplicabilidade dos Controles do Anexo A.

Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais.

	Política de Segurança da Informação	Código: POL-SGSI-1 Revisão: 4 Data: 14/10/2026
Unidade: BAMEX - Teresina-PI		Área: Sistema de Gestão de Segurança da Informação

ABNT NBR ISO/IEC 27001:2022 e sua Emenda 1:2024; ABNT NBR ISO/IEC 27002:2022.

		Arquivo Ativo		Arquivo Morto	
Local de Armazenamento:		GSG Sistem		NA	
Proteção / Preservação:		GSG Sistem		NA	
Ordem de Arquivamento / Recuperação:		GSG Sistem		NA	
Caminho de Rede:		NA		NA	
Retenção / Tempo:		5 anos		5 anos	
Descarte ou Disposição:		NA		NA	
Histórico da Alteração:		Ajustar razao social			
Elaborado por:		Alana Alves da Silva		Data:	14/10/2026
Analisado por:		O. Comitê de SGSI		Data:	14/10/2026
Aprovado por:		Fernando José Dini Pinto Junior		Data:	14/10/2026
Publicado para Entrar em Vigor por:		Fernando José Dini Pinto Junior		Data:	14/10/2026
Documento oficial da empresa. Proibida a reprodução. Todos os direitos reservados.					