Classificação: Público

POLÍTICA CORPORATIVA

SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

ID: 61 - Versão: 2
Aprovado em: 06/04/2023

1 OBJETIVO

Este documento tem por objetivo definir as diretrizes, as responsabilidades e os princípios relativos à Política de Segurança da Informação e Cibernética (Política). A Política foi elaborada em linha com as melhores práticas de mercado, considerando a natureza e a complexidade das operações, dos produtos, dos serviços, das atividades, dos processos, dos sistemas e dos requisitos de conformidade do Banco PAN S.A. ("Banco", "Companhia" ou "PAN"), bem como em conformidade com a legislação e com regulamentações aplicáveis.

2 ABRANGÊNCIA E APLICABILIDADE

A Política é aplicada ao Banco PAN e às suas controladas (Grupo PAN), exceto a Mobiauto Edição de Anúncios On Line Ltda. e a Mosaico Tecnologia ao Consumidor S.A, que dispõem de políticas próprias em razão da natureza de suas atividades, bem como aos seus administradores, colaboradores e prestadores de serviços terceirizados.

3 CONCEITOS

- **Ativos da Informação:** entende-se por ativos da informação tudo o que pode criar, processar, armazenar, transmitir e/ou excluir informações. Esses ativos podem ser tecnológicos (*software* e *hardware*) e não tecnológicos (pessoas, processos e dependências físicas).

- **Backup:** cópia de segurança de dados em mídia magnética (disco, fita ou outro instrumento tecnológico de armazenamento de dados) ou em nuvem, que pode ser restaurada pelo processo conhecido como "*restore*" em caso de perda dos dados originais.

- **Ciclo da Informação:** compreende os processos, os fluxos e as atividades de geração, acesso, manuseio, armazenamento, reprodução, transporte e de descarte da informação.

- **Conselho dos Padrões de Segurança da Indústria de Cartões de Pagamento:** esse Conselho é composto por representantes dos principais arranjos de pagamento (bandeiras de cartão) e define os padrões de segurança de dados para os meios de pagamento, além de aprovar os requisitos de qualificação das entidades independentes para a execução de auditorias, de certificação e de testes da segurança desses dados.

- **Criptografia:** mecanismo de segurança e de privacidade que torna determinada comunicação ou dados indecifráveis para quem não dispõe de acesso aos códigos de "tradução". A criptografia auxilia na proteção de todos os conteúdos armazenados ou transmitidos entre duas ou mais fontes, evitando a interceptação indevida por terceiros.

- **Crise:** um evento ou uma série de eventos de grande dimensão que possam causar danos à imagem do PAN ou prejudicar o seu relacionamento com clientes, acionistas, órgãos reguladores, investidores e demais partes interessadas, podendo ou não acarretar perdas financeiras para o PAN.

- **Incidente:** um evento ou uma série de eventos inesperados ou indesejáveis de segurança, com potencial para comprometer as operações e as atividades do PAN.

- **Informação:** resultante do processamento, manipulação e organização de dados, que constitui uma mensagem sobre um determinado assunto, fenômeno ou evento.

- **Rede Corporativa e Wireless:** é um sistema de transmissão de dados destinado a transferir informações entre diversos equipamentos, tais como estações de trabalho, *notebooks*, servidores de documentos, arquivos, impressoras e sistemas, obedecendo a uma série de regras definidas pelas áreas de Tecnologia e Segurança da Informação do PAN.

- **Risco Cibernético:** o risco cibernético se refere à probabilidade de possíveis resultados negativos associados a ataques que podem comprometer a confidencialidade, a integridade e a disponibilidade de dados ou de sistemas de computadores.

- **Segurança da Informação:** é a proteção da informação contra divulgação, transferência, modificação ou destruição não autorizada, seja de forma acidental ou intencional.

- **Segurança Cibernética:** é um domínio dentro da Segurança da Informação que tem por objetivo proteger os ativos em formato digital, por meio do tratamento de ameaças que põem em risco a informação que é processada, armazenada e transportada pelos sistemas, serviços, arquivos e bancos de dados ou de informações.

- **Sistema Normativo:** é um dos pilares da governança corporativa do Banco PAN, representado pelo conjunto de documentos organizados que contêm a formalização das diretrizes, princípios, papéis e responsabilidades, macroprocessos e processos, atividades e controles, regras, limites,

alçadas e das informações técnicas. O fluxo de criação, atualização, gestão e consulta das normas é definido em sistema corporativo específico.

4 PRINCÍPIOS

A Segurança da Informação e Cibernética baseia-se em 4 (quatro) princípios-chaves:

- **Confidencialidade:** assegurar que somente pessoas autorizadas tenham acesso às informações e aos Ativos da Informação de que necessitam na condução de suas atividades;
- **Integridade:** assegurar a veracidade e a totalidade das informações e os métodos de execução física ou lógica, visando proteger a informação, na guarda ou na transmissão, contra alterações indevidas, intencionais ou acidentais;
- **Disponibilidade:** assegurar que os usuários autorizados obtenham acesso às informações e aos Ativos da Informação correspondentes, sempre que necessário; e
- **Autenticidade:** assegurar a identificação do autor da informação e os meios com que a informação é processada, de modo que, quando necessário, sejam rastreáveis e comprováveis.

5 DIRETRIZES CORPORATIVAS

As diretrizes corporativas definem as linhas mestras que embasam os processos e os controles de Segurança da Informação e Cibernética. As diretrizes são as seguintes:

I. **Conscientização em Segurança da Informação:** as diretrizes de Segurança da Informação e Cibernética, bem como os princípios que norteiam esta Política, devem ser disseminados por meio de programas de conscientização e de capacitação para colaboradores e para os prestadores de serviço terceirizados. Recomendações e dicas sobre segurança da informação e cibernética devem ser disponibilizadas no site institucional do PAN, sem prejuízo da divulgação por outros meios a critério da Administração;

II. **Declaração de Responsabilidade:** os colaboradores e os prestadores de serviços, diretamente contratados pelo PAN, devem aderir formalmente ao termo de responsabilidade, comprometendo-se a atuar de acordo com esta Política;

III. **Gestão de Ativos da Informação:** os ativos de informação do Banco PAN devem ser identificados, inventariados, catalogados e classificados quanto à sua severidade a riscos por Tecnologia da Informação. A Segurança da Informação e Cibernética deve abranger a proteção dos ativos do PAN, principalmente aqueles classificados como críticos, assegurando, assim, a sua confidencialidade, integridade e disponibilidade;

IV. **Utilização de Recursos da Informação:** apenas os equipamentos corporativos, gerenciados ou homologados pelo PAN, podem ser conectados à sua rede corporativa de tecnologia da informação. Não é permitida a conexão física ou lógica à rede corporativa de equipamentos particulares não gerenciados ou não homologados pelo Banco. Os mecanismos de proteção contra softwares maliciosos devem estar devidamente instalados, atualizados e configurados nos servidores e nas estações de trabalho e nos *notebooks*. Devem ser implementados controles que previnam a modificação indevida de configurações-padrão de segurança e a instalação de softwares não homologados nos ativos da informação do PAN;

V. **Trabalho Remoto:** quando aplicável, o PAN permite o trabalho remoto de seus colaboradores e medidas de segurança da informação devem ser implementadas para garantir a proteção das informações acessadas, processadas ou armazenadas enquanto a execução do trabalho se der de forma remota;

VI. **Gestão de Acessos a Sistemas e a Serviços:** o acesso a sistemas e a serviços deve ser apropriado, autorizado e condizente com as atividades e as funções exercidas pelo solicitante, visando prevenir o acesso não autorizado e o acúmulo de privilégios, controlando, assim, a inclusão, a exclusão e a modificação do credenciamento de usuários e dos perfis de acesso. A senha é de uso pessoal, classificada como confidencial e intransferível, sendo proibido, sob qualquer circunstância, o seu compartilhamento com terceiros;

VII. **Segurança Física:** os controles e os processos de segurança física devem ser implementados pela área de Administração Predial, com o objetivo de prevenir o acesso físico não autorizado ao Banco e aos seus sistemas de tecnologia da informação.;

VIII. **Classificação da Informação e Prevenção Contra Perda de Dados:** todas as informações devem ser atribuídas a proprietários e classificadas de acordo com a sua confidencialidade, sob a proteção necessária, prazo de manutenção, de transferência, de transporte e descarte, em observância às regras corporativas estabelecidas. Devem ser implementadas ferramentas para mitigação do risco de vazamento de dados em equipamentos corporativos, em aplicativos na nuvem e em serviços de e-mail e de navegação na Internet;

IX. **Criptografia e Confidencialidade:** deve-se observar a necessidade de criptografia dos dados, em razão da confidencialidade, utilizando-a para proteger informações sensíveis ou críticas, armazenadas e/ou transmitidas;

X. **Gestão de Riscos:** os riscos de segurança da informação e cibernéticos devem ser identificados, mensurados, monitorados, tratados, reportados e mitigados, por meio de processo definido e devidamente formalizado, com o objetivo de implementar os mecanismos de proteção e os controles de segurança da informação e cibernéticos adequados, mitigando assim os riscos embutidos nas exposições do PAN e os seus impactos;

XI. **Segurança no Desenvolvimento de Sistemas e de Serviços:** o processo de desenvolvimento e de atualização de sistemas e de serviços corporativos devem assegurar a aderência às regras e às normas sobre a arquitetura de segurança da informação e de desenvolvimento seguro, disponibilizadas no Sistema Normativo do PAN;

XII. **Teste de Segurança:** a fim de identificar e de reduzir vulnerabilidades nos ativos de informação, devem ser realizadas, por meio de testes de segurança, varreduras para identificação de vulnerabilidades no ambiente de tecnologia de produção, em periodicidade mínima de 30 dias. Uma vez identificada mudança em aberto para promoção de sistemas para ambientes de produção, uma varredura de vulnerabilidade deve ser executada, conforme definido em normativo publicado no Sistema Normativo do PAN. Anualmente, será executada, por consultoria independente, teste de penetração (manual ou automatizado) nos ambientes críticos para identificação de fragilidades nos ativos da informação, sem prejuízo da avaliação sobre os controles e os processos de segurança já estabelecidos no PAN;

XIII. **Cópias de Segurança (*backup*):** deve ser garantida, de forma íntegra e confiável, a restauração de dados registrados nos sistemas de informações ou nos servidores de arquivos do PAN, com foco na preservação da confiabilidade, da integridade e da disponibilidade da informação e dos processos definidos em regras previstas no Sistema Normativo do PAN;

XIV. **Segurança na Gestão de Fornecedores:** os fornecedores devem ser classificados conforme diretrizes corporativas e, caso sejam classificados como relevantes, devem ser selecionados, analisados e gerenciados em todo o período de vigência dos contratos, visando à conformidade com os controles de segurança e regulatórios, de acordo com o tipo de serviço ou de solução fornecida. Adicionalmente, os fornecedores devem ter um score de risco atribuído, por meio de um processo formal definido pelo PAN:

- **Aquisição de Bens e Serviços**: o processo de contratação de sistemas ou de serviços, que envolva tecnologia, processamento ou armazenamento de informações do Banco PAN, deve contemplar a análise das exigências previstas na Resolução CMN 4.893, de 2021, e de requisitos de segurança da informação, de continuidade de negócios e de privacidade de dados. Quando aplicável, a comunicação da contratação de fornecedores aos órgãos reguladores deve ser realizada conforme a regulamentação vigente;

- **Restrição na Contratação de Bens e Serviços:** a área de Segurança da Informação e Cibernética pode vetar ou impor restrições para a contratação de sistemas ou de serviços que envolvam tecnologia ou processamento ou armazenamento de informações do Banco PAN quando constatar, a qualquer tempo, o não atendimento da regulamentação vigente e/ou das normas sobre a segurança da informação, definidas e publicadas no Sistema Normativo do PAN;

- **Controles e Incidentes de Segurança**: devem ser avaliados, pela área responsável no PAN, os controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por fornecedores de serviços que manuseiem dados ou informações que sejam relevantes para a condução das atividades operacionais do Banco. Incidentes relevantes relacionados às informações do Banco, armazenadas ou processadas por fornecedores, devem ser comunicadas à área de Operação de Segurança da Informação, por meio do canal: csirt@grupopan.com;

XV. **Segurança dos Dados de Cartão de Pagamento:** devem ser protegidos os ambientes do PAN que armazenam, processam e transmitem dados de cartões de pagamento relacionados aos processos de adquirência. Os testes da efetividade da segurança desses ambientes devem ser executados por entidade externa independente devidamente aprovada pelo Conselho dos Padrões de Segurança da Indústria de Cartões de Pagamento, no mínimo uma vez ao ano;

XVI. **Proteção de Perímetro:** a fim de proteger a infraestrutura do PAN contra-ataques externos, devem ser implementados ferramentas e controles contra: softwares e mensagens maliciosas; invasão de dispositivos de rede e servidores; ataques a aplicativos e a sistemas corporativos; ataques de negação de serviço; e ameaça persistente avançada. Devem ser implementados controles de acesso e de segmentação da rede corporativa, de maneira a mitigar o risco de acessos não autorizados;

XVII. **Registro e Monitoramento:** os eventos lógicos de sistemas e de serviços, bem como os eventos físicos, capturados e/ou identificados por câmeras, catracas ou áreas restritas, devem ser devidamente registrados e monitorados, conforme regras do PAN;

XVIII. **Gestão de Incidentes:** devem ser realizadas ações de prevenção, identificação, registro e resposta a incidentes e a crises de segurança do ambiente tecnológico do PAN, que possam comprometer a confidencialidade, a integridade e a disponibilidade dos ativos da informação. Os incidentes de Segurança da Informação e Cibernéticos classificados como relevantes devem ser reportados, de imediato, ao Gestor de Riscos em Segurança da Informação e Cibernética do PAN:

- **Registro do Incidente:** o incidente deve ser registrado e classificado de acordo com o seu nível de criticidade, determinado pela exposição e pela relevância dos ativos da informação relacionados com a

ocorrência, incluindo a probabilidade de exploração da vulnerabilidade por meio de ameaças e o potencial impacto ao Banco;

- **Compartilhamento de Incidentes:** informações sobre incidentes relevantes, que possam impactar outras instituições financeiras, devem ser compartilhadas com as demais instituições, com objetivo de reduzir o risco de segurança cibernética no mercado financeiro como um todo, seguindo diretrizes dos órgãos reguladores;

- **Relatório de Segurança Cibernética:** anualmente, a área de Operações de Segurança da Informação e Cibernética deve elaborar relatório de resposta a incidentes, contendo o resumo dos resultados obtidos na implementação de rotinas, de processos e de tecnologias utilizados na prevenção e na reposta a incidentes, bem como incidentes cibernéticos relevantes e os resultados dos testes dos cenários de crise cibernética. O relatório deve ser submetido à Comissão de Riscos do PAN e encaminhado para ciência e eventuais providências do Conselho de Administração, nos termos da regulamentação vigente.

XIX. **Cenários de Crise Cibernética:** deve ser realizado o registro, em forma de catálogo, sobre os testes periódicos de cenários e de situações nas quais incidentes de segurança de dimensões e com danos significativos, com capacidade de comprometer operações críticas e a reputação do PAN, possam se materializar nos seus ativos de informação. Devem ser catalogadas as informações sobre os cenários de crises cibernéticas relacionadas aos incidentes de segurança e inseridas no relatório de resposta a incidentes relevantes ocorridos no período, incluindo também os resultados dos testes de continuidade desses cenários; e

XX. **A Política de Segurança da Informação e Cibernética e o Plano de Resposta a Incidentes:** devem ser aprovados pelo Conselho de Administração do Banco PAN. A revisão deve ocorrer, no mínimo, anualmente, seguindo as diretrizes constantes da regulamentação e do Sistema Normativo do PAN.

6 ESTRUTURA DE GERENCIAMENTO

O Banco PAN conta com estrutura de Segurança da Informação e Cibernética compatível com a natureza, com o porte, com a complexidade, com o perfil de risco e com o modelo de negócios, tendo como função principal assegurar o efetivo gerenciamento dos Riscos de Segurança da Informação e Cibernéticos.

A estrutura está alocada na Superintendência Executiva de Segurança Corporativa (Superintendência de

Segurança Corporativa) e se reporta ao Diretor de Controladoria e Compliance, encontrando-se, portanto, segregada das unidades de negócios, de suporte corporativo e de Auditoria Interna, de forma a assegurar a eficácia e a autonomia de sua atuação, dispondo de recursos, pessoas e livre acesso às informações necessárias ao desempenho de suas atividades.

A estrutura da Superintendência de Segurança Corporativa está segregada em 5 (cinco) linhas estruturais, sendo: (i) Governança, Riscos e Compliance de Segurança da Informação; (ii) Operações de Segurança da Informação; (iii) Privacidade e Proteção de Dados; (iv) Inspetoria e Inteligência Corporativa; e (v) Prevenção a Fraudes. Em consonância com a estrutura de gerenciamento da Superintendência de Segurança Corporativa, várias outras áreas participam do processo de acordo com os seus respectivos papéis e responsabilidades, visando assegurar a eficiência, a efetividade e o aperfeiçoamento contínuo dos controles e dos processos de gerenciamento, em linha com as estratégias do PAN.

Essa estrutura segue as diretrizes constantes da governança corporativa estabelecida no PAN por meio de comitês e alçadas definidas pela Administração, bem como as normas que definem o processo de tomada de decisão. Os processos e os sistemas que suportam e viabilizam o funcionamento da estrutura de gerenciamento da Segurança da Informação e Cibernética estão descritos nas normas da área responsável e publicadas no Sistema Normativo do PAN.

6.1 PROCESSO DE GERENCIAMENTO

O processo de gerenciamento da Segurança da Informação e Cibernética, que é utilizado para subsidiar à Alta Administração do Banco PAN para análise e para tomada de decisão, abrange todo o ciclo da informação, contemplando os processos de definição, de monitoramento e de gestão dos ativos da informação, acessos lógicos a sistemas da informação, segurança na arquitetura e no desenvolvimento de sistemas da informação, classificação da informação, análise de riscos sob a ótica de segurança da informação e cibernética, acompanhamento do *rating* cibernético, registro e tratamento de incidentes, elaboração e revisão dos cenários de crises cibernéticas, implementação de controles detectivos e preventivos no ambiente tecnológico, transferência e descarte da informação de forma segura, conscientização e treinamentos sobre segurança da informação e cibersegurança para colaboradores e para prestadores de serviço.

7 RESPONSABILIDADES

As áreas e os órgãos colegiados que compõem a estrutura de gerenciamento da Segurança da Informação e Cibernética do Banco PAN atuam de acordo com as seguintes responsabilidades:

- **Conselho de Administração:** definir a orientação geral para o gerenciamento de riscos relacionados à Segurança da Informação e Cibernética do Banco PAN, fazendo parte de suas atribuições a aprovação da política corporativa de prevenção a esses riscos.

- **Comissão de Riscos PAN** ("Comissão de Riscos"): órgão colegiado responsável por avaliar, acompanhar e prover a estrutura para execução do Programa de Segurança Cibernética e promover o comprometimento, o apoio e a aprovação do Plano de Ação e de Resposta a Incidentes, bem como a aderência da atuação dos colaboradores ao processo de Segurança da Informação e Cibernética do PAN. A Comissão de Riscos é um órgão não estatutário, deliberativo e de caráter permanente, o qual tem por finalidade, no que se refere à gestão de riscos e de capital do PAN, deliberar sobre assuntos de sua competência e assessorar o Conselho de Administração do PAN no desempenho de suas responsabilidades.

- **Comitê de Segurança Corporativa e de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (Comitê de Segurança Corporativa e de PLD/FT)**: órgão colegiado responsável por estabelecer diretrizes e apresentar, discutir e deliberar sobre assuntos de Segurança Corporativa e de PLD/FT, alinhadas com esta Política, com a Política Corporativa de Gestão da Continuidade de Negócios ("PCGCN") e com a Política Corporativa de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo ("PCPLD/FT"), bem como assessorar as Diretorias do Banco PAN ("Diretoria") e de suas controladas no desempenho de suas responsabilidades.

- **Diretor de Segurança da Informação e Cibernética**: responsável por atuar no engajamento em Segurança da Informação e Cibernética do PAN, garantindo que as exigências legais e setoriais sejam devidamente atendidas, apoiando o Gestor de Riscos em Segurança da Informação no gerenciamento estratégico do tema. É responsável também pela execução do Plano de Ação e de Resposta a Incidentes, visando à implantação desta Política.

- **Gestor de Riscos em Segurança da Informação**: superintendente executivo, responsável por prover informações estruturadas e consolidadas dos principais riscos de Segurança da Informação e Cibernética para os membros da Diretoria e do Conselho de Administração do PAN. Ademais, cabe a ele apontar soluções de segurança de acordo com a necessidade dos negócios, produtos, processos e tecnologia, executando a gestão dos riscos de Segurança da Informação e Cibernética, conforme a exposição do ativo da informação do PAN.

- **Governança de Segurança da Informação**: área responsável pela conscientização, pela governança, pela gestão de riscos e pela conformidade e garantias de Segurança da Informação e Cibernética do Banco PAN. Atua no gerenciamento das ações de conscientização sobre segurança dos colaboradores e dos prestadores de serviços, na manutenção da conformidade normativa da segurança, na análise de riscos e de conformidade de fornecedores de tecnologia, na avaliação da segurança dos dados de cartão de pagamento e no gerenciamento do processo de identificação de potenciais vulnerabilidades de segurança nos ativos de informação do Banco PAN. Adicionalmente, gerencia o *rating* cibernético e gera indicadores de segurança da informação e cibersegurança para apoio no processo de tomada de decisão da Diretoria e do Conselho de Administração do Banco PAN.

- **Operação de Segurança da Informação**: área responsável pela identificação, registro, prevenção e respostas a Incidentes e a crises de Segurança da Informação e Cibernética do Banco PAN que possam comprometer a confidencialidade, a integridade e a disponibilidade dos ativos da informação. Adicionalmente, atua diretamente no atendimento das demandas de projetos institucionais e de tecnologia, na implementação e no gerenciamento de controles preventivos e de segurança lógica do Banco PAN, segurança ofensiva, segurança em nuvem e segurança na arquitetura, no desenvolvimento de sistemas da informação e na gestão de chaves criptográficas e de certificados digitais.

- **Gestores das Áreas de Tecnologia da Informação**: atuar na gestão dos riscos associados à Segurança da Informação e Cibernética, inerentes à aplicação de controles de segurança na infraestrutura e em sistemas informatizados, desenvolvendo as soluções corporativas de forma segura e mantendo o parque tecnológico disponível e atualizado conforme as regras corporativas publicadas no Sistema Normativo. Devem assegurar que as exposições a esses riscos estejam compatíveis com os limites definidos pela Alta Administração e em linha com as estratégias de negócio do Banco PAN.

- **Gestores das Áreas de Negócio**: atuar na gestão dos riscos associados à Segurança da Informação e Cibernética, inerentes aos produtos, aos clientes e às operações, sob sua responsabilidade, de acordo com as diretrizes, os princípios e as responsabilidades definidas nesta Política. Devem assegurar que as exposições a esses riscos estejam compatíveis com os limites definidos e em linha com as estratégias de negócio do PAN.

- **Colaboradores e Prestadores de Serviço**: observar e seguir os princípios, as diretrizes e as responsabilidades definidas nesta Política e acionar imediatamente à área de Operações de Segurança

da Informação e Cibernética sobre eventuais descumprimentos ou ainda sobre indícios de irregularidades, comportamentos, operações atípicas ou suspeitas que possam divergir das diretrizes desta Política.

A violação das diretrizes desta Política sujeita aos responsáveis sanções disciplinares na forma prevista na Política Corporativa de Consequências e no Código de Conduta e Ética do Banco PAN.

Sistema normativo	
Este documento:	4 - Deve estar disponível a todos colaboradores.
1 - É exclusivo para uso interno.	5 - Ser divulgado somente pelo Sistema Normativo.
2 - Deve ser mantido atualizado pela área responsável.	
3 - Deve ser coerente entre a prática e suas determinações.	