Classificação: Público Interno

POLÍTICA CORPORATIVA

SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

ID: 61 - Versão: 4
Aprovado em: 09/04/2025

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), 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 se aplica ao PAN e suas controladas (Grupo PAN), com exceção da Mobiauto Edição de Anúncios On Line Ltda. e da Mosaico Tecnologia ao Consumidor S.A., que possuem políticas próprias devido à natureza de suas atividades. Esta Política também se aplica aos administradores, colaboradores e prestadores de serviços terceirizados do PAN, que utilizam informações do PAN em suas funções e/ou na execução de contratos.

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 (PCI DSS)**: 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.
- **Correio Eletrônico:** serviço de comunicação por e-mail fornecido pelo PAN para fins corporativos.
- **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.
- **IA (Inteligência Artificial):** Refere-se à habilidade de computadores e sistemas automatizados realizarem tarefas que, normalmente, requerem inteligência humana, como aprendizado, raciocínio, resolução de problemas e tomada de decisões.
- **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.
- **Mensageria:** ferramenta para troca instantânea de mensagens.
- **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 seja de forma 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 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.

POLÍTICA CORPORATIVA

SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

ID: 61 - Versão: 4
Aprovado em: 09/04/2025

4 PRINCÍPIOS

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

- **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 implementados no PAN.

I. Declaração de Responsabilidade: os colaboradores e os prestadores de serviços, diretamente contratados pelo PAN, devem aderir formalmente ao Termo de Confidencialidade e Responsabilidade pela Segurança das Informações, comprometendo-se a atuar de acordo com esta Política.

II. Conscientização: as diretrizes de Segurança da Informação e Cibernética, bem como os princípios que norteiam esta Política, devem ser disseminados por meio de programas de comunicação, conscientização e de capacitação, para colaboradores e prestadores de serviço terceirizados.

III. Classificação da Informação e Prevenção Contra Perda de Dados: 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.

IV. Gestão de Ativos da Informação: os ativos de informação do PAN devem ser identificados, inventariados, catalogados e classificados quanto à sua severidade. A Segurança da Informação deve abranger a proteção dos ativos do PAN, principalmente aqueles classificados como críticos, assegurando,

assim, a sua confidencialidade, integridade e disponibilidade.

V. Gestão de Riscos: os riscos de segurança da informação e cibernéticos devem ser identificados, categorizados, 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.

VI. Inteligência Artificial (IA): a IA deve ser usada de forma ética, transparente e livre de vieses discriminatórios. Todo uso de IA deve atender as regras de segurança e legislações aplicáveis, incluindo, mas não se limitando a Lei Geral de Proteção de Dados (LGPD).

VII. Gestão de Acessos Lógicos: o acesso a sistemas e a serviços deve ser apropriado, autorizado e condizente com as atividades e as funções exercidas pelo colaborador ou prestador de serviço terceirizado, visando prevenir o acesso não autorizado e o acúmulo de privilégios.

VIII. Utilização de Recursos da Informação: apenas os equipamentos corporativos, gerenciados ou homologados pelo PAN, podem ser conectados à sua rede corporativa, conforme explicitado no Termo de Acesso e Uso de Sistemas e Informações.

IX. 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.

X. Segurança Física: controles e processos de segurança física devem ser implementados, com o objetivo de prevenir o acesso físico não autorizado as dependências do PAN, incluindo salas cofres e data centers.

XI. Segurança na Gestão de Fornecedores: fornecedores devem ser classificados conforme as diretrizes corporativas e, caso sejam considerados relevantes, devem passar por um processo formal de seleção, análise e gestão durante toda a vigência do contrato, garantindo conformidade com requisitos de segurança da informação, privacidade de dados e normas regulatórias. A contratação de serviços de tecnologia, que processam ou armazenam dados em nuvem, devem atender às exigências da Resolução CMN 4.893/2021 e demais requisitos aplicáveis, incluindo a comunicação aos órgãos reguladores, quando necessário. A Segurança da Informação pode vetar ou impor restrições a contratações que não atendam às regulamentações vigentes.

XII. 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, quando aplicável ao ambiente do PAN.

XIII. Privacidade de Dados: devem ser estabelecidas diretrizes para assegurar a proteção e o uso adequado de dados pessoais, em conformidade com as legislações aplicáveis, como Lei Geral de Proteção de Dados (LGPD) e outras normas locais.

XIV. Correio Eletrônico e Serviço de Mensageria: o e-mail e as ferramentas de mensageria corporativas devem ser utilizadas exclusivamente para atividades relacionadas as funções profissionais, de forma ética, adequada e segura.

XV. 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.

XVI. Criptografia e Confidencialidade: deve ser observada a necessidade da aplicabilidade da criptografia dos dados, em razão da confidencialidade, utilizando-a para proteger informações sensíveis ou críticas.

XVII. Segurança no Desenvolvimento de Sistemas e de Serviços: o processo de desenvolvimento e de atualização de sistemas e de serviços corporativos deve assegurar a aderência às regras e as boas práticas de desenvolvimento seguro.

XVIII. Teste de Segurança: a fim de identificar e de reduzir vulnerabilidades nos ativos de informação, devem ser realizadas, por meio de testes de segurança (manuais e/ou automatizadas), varreduras para identificação de vulnerabilidades.

XIX. 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.

XX. 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 do PAN, devem ser devidamente registrados e monitorados.

XXI. Gestão de Incidentes: incidentes de segurança da informação e cibernéticos devem ser registrados e classificados de acordo com o seu nível de criticidade, determinado pela exposição e pela relevância dos ativos da informação envolvidos. As ações de contenção, erradicação e de recuperação devem ser documentadas. Os incidentes relevantes, que possam impactar outras instituições ou mercado financeiro com um todo, devem ser reportadas e compartilhadas, conforme diretrizes dos órgãos reguladores vigentes.

XXII. Cenários de Crise Cibernética: devem ser catalogados os cenários de crises cibernéticas relacionados a incidentes de segurança e inseridos no relatório de resposta a incidentes relevantes ocorridos no período, incluindo também os resultados dos testes de continuidade desses cenários; e

XXIII. A Política Corporativa de Segurança da Informação e Cibernética e o Relatório de Segurança Cibernética: devem ser submetidos e aprovados pelo Conselho de Administração do PAN, no mínimo, anualmente. O Relatório de Segurança Cibernética deve conter o resumo dos resultados obtidos na implementação de rotinas, de processos e de tecnologias utilizados na prevenção e na reposta a incidentes de segurança, bem como incidentes cibernéticos relevantes e os resultados dos testes dos cenários de crise cibernética.

6 ESTRUTURA DE GERENCIAMENTO

O PAN conta com estrutura de Segurança da Informação e Cibernética compatível com a sua natureza, com o porte, com a complexidade, com o perfil de risco e com o modelo de negócio, tendo como função principal assegurar a efetiva gestão dos Riscos de Segurança da Informação e Cibernéticos.

O reporte é feito para o CISO Global do Banco BTG Pactual, empresa líder do conglomerado. Fazem parte da Segurança da Informação as seguintes estruturas:

- Security Governance, Risk and Compliance;
- Security Architecture;
- Application Security;
- Cyber Defense Center;

- Data Privacy;
- IDM (Identity Management).

A Segurança da Informação tem autonomia, encontrando-se, portanto, segregada das unidades de negócios, do suporte corporativo e da Auditoria Interna, de forma a assegurar a eficácia e a autonomia de sua atuação, dispondo de recursos, pessoas e livre acesso às informações necessárias para o desempenho de suas atividades.

Em consonância com a estrutura de gerenciamento da Segurança da Informação, 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.

A estrutura segue as diretrizes constantes da governança corporativa estabelecida no conglomerado, 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 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 para análise e 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, privacidade e proteção de dados, 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 da postura cibernética, 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

Sistema normativo

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

POLÍTICA CORPORATIVA

SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

ID: 61 - Versão: 4
Aprovado em: 09/04/2025

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

Conselho de Administração: responsável por definir a orientação geral para o gerenciamento de riscos relacionados à Segurança da Informação e Cibernética do 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.

CISO (*Chief Information Security Officer*): responsável por atuar no engajamento em Segurança da Informação e Cibernética do conglomerado prudencial do Banco BTG Pactual, incluindo o PAN, garantindo que as exigências legais e setoriais sejam devidamente atendidas, atuando no gerenciamento estratégico do tema. É responsável também pela execução do Plano de Ação e de Resposta a Incidentes, visando à implantação desta Política.

Gestores das Áreas de Segurança da Informação: responsáveis pela defesa cibernética do conglomerado prudencial do Banco BTG Pactual, incluindo o PAN, garantindo a proteção dos ativos digitais e do ambiente através da prevenção, detecção, e resposta aos incidentes, com o objetivo de minimizar a vulnerabilidade da instituição às atividades maliciosas. Devem identificar e repostar os riscos associados à Segurança da Informação e Cibernética, evoluir de forma contínua a defesa cibernética, aumentar a resiliência e a eficácia dos controles, para apoio no processo de tomada de decisão do CISO e da Alta Administração.

Gestores das Áreas de Tecnologia da Informação: devem 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, assegurando que as exposições a esses riscos estejam compatíveis com os limites definidos pela Alta Administração e em linha com as estratégias de negócio do

PAN.

Gestores das Áreas de Negócio: devem 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, assegurando 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: devem observar e seguir os princípios, as diretrizes e as responsabilidades definidas nesta Política e acionar imediatamente à área de Segurança da Informação sobre eventuais descumprimentos ou ainda sobre indícios de irregularidades, comportamentos, operações atípicas ou suspeitas que possam divergir com as diretrizes desta Política.

A violação das diretrizes dispostas nesta Política por parte dos colaboradores e prestadores de serviço terceirizados, está sujeita a sanções disciplinares conforme previsto na Política Corporativa de Consequências e no Código de Conduta e Ética do PAN.

Sistema normativo

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