POLÍTICA CORPORATIVA

Segurança da Informação e Cibernética

Unidade Reponsável: SEGURANÇA CORPORATIVA

1. OBJETIVO

Este documento ("Política") tem por objetivo definir as diretrizes, responsabilidades e princípios relativos à Segurança da Informação e Cibernética, em linha com as melhores práticas de mercado, considerando a natureza e a complexidade de nossos produtos, serviços, atividades, processos e sistemas e a conformidade com os requerimentos legais e regulatórios no Conglomerado Prudencial PAN ("PAN").

2. ABRANGÊNCIA E APLICABILIDADE

A Política aplica-se a todas as empresas do PAN, assim como a 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 uma informação. Podem ser tecnológicos ("software" e "hardware") e não tecnológicos (pessoas, processos e dependências físicas).
- **Backup**: cópia de segurança de dados em mídia magnética (disco ou fita) ou em nuvem que pode ser restaurada pelo processo conhecido como "*Restore*" em caso da perda dos dados originais.
- **Ciclo da Informação**: compreende os processos, fluxos e atividades de geração, acesso, manuseio, armazenamento, reprodução, transporte e descarte da informação.
- **Criptografia**: mecanismo de segurança e privacidade que torna determinada comunicação ou dados indecifráveis para quem não tem 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 por terceiros.
- **Crise:** um evento ou série de eventos de grande dimensão que possam trazer danos à imagem da organização ou prejudicar seu relacionamento com clientes, acionistas, órgãos reguladores, investidores e demais partes interessadas, podendo ou não acarretar perdas financeiras para o PAN.

Data de Criação	Data da Última Aprovação	Data da Última Revisão
25.Mar.2019	**30.Mar.2021**	**30.Mar.2021**

- **Incidente:** um evento ou série de eventos inesperados ou indesejáveis de segurança, com probabilidade de 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 que transfere informações entre diversos equipamentos, tais como estações de trabalho, notebooks, servidores de documentos, arquivos, impressoras e sistemas, obedecendo uma série de regras definidas pelas áreas de Tecnologia e Segurança da Informação.
- **Risco Cibernético**: o risco cibernético mensura a probabilidade de possíveis resultados negativos associados a ataques que podem comprometer a confidencialidade, integridade e disponibilidade de dados ou sistemas de computadores.
- **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 de informação.

4. PRINCÍPIOS

A Segurança da Informação e Cibernética baseia-se em 04 (quatro) princípios chaves:

- **Confidencialidade:** assegurar que somente pessoas autorizadas tenham acesso às informações e aos Ativos da Informação que necessitam no âmbito de suas atividades;
- **Integridade:** assegurar a veracidade e totalidade das informações e os métodos de execução física ou lógica, visando proteger a informação, na guarda ou 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 o autor da informação e os meios com que a informação foi processada, de modo que quando necessário, sejam comprováveis e rastreáveis.

5. DIRETRIZES CORPORATIVAS

As diretrizes corporativas definem as linhas mestras sobre as quais os principais processos e controles de Segurança da Informação e Cibernética devem estar embasados:

I. **Conscientização em Segurança da Informação:** os princípios e diretrizes de Segurança da Informação devem ser disseminados por meio de programas de conscientização e capacitação para colaboradores e prestadores de serviço. Dicas de Segurança e de Prevenção à Fraudes também devem ser disponibilizadas no site institucional e rede sociais.

Data de Criação	Data da Última Aprovação	Data da Última Revisão
25.Mar.2019	**30.Mar.2021**	**30.Mar.2021**

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

III. **Gestão de Ativos da Informação:** os ativos de informação do PAN devem ser identificados, inventariados e catalogados por Tecnologia da Informação. A Segurança da Informação deve proteger estes ativos contra acessos indevidos, através de controles físicos e lógicos.

IV. **Utilização de Recursos da Informação:** apenas os equipamentos corporativos, ou gerenciados, ou homologados pelo PAN, podem ser conectados à rede corporativa. Não será permitida a conexão física ou lógica à rede corporativa, por equipamentos particulares não gerenciados ou não homologados. Os mecanismos de proteção contra softwares maliciosos devem estar devidamente instalados e configurados nos equipamentos.

V. **Gestão de Acessos a Sistemas e Serviços:** o acesso à sistemas e serviços deve ser apropriado, autorizado e condizente com as funções exercidas pelo solicitante, visando prevenir o acesso não autorizado e o acúmulo de privilégios. A senha é de uso pessoal, classificada como confidencial e intransferível, sendo proibido, sob qualquer circunstância, seu compartilhamento.

VI. **Segurança Física:** os controles e processos de segurança física devem prevenir o acesso físico não autorizado, danos e interferências nos ativos da informação, de acordo com a criticidade das informações previamente mapeadas e declaradas pela área Segurança da Informação à área Administração Predial.

VII. **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, proteção necessária, prazo de manutenção e descarte, em observância às regras corporativas estabelecidas. Devem ser implementadas ferramentas para mitigação do risco de vazamento de dados em equipamentos corporativos, utilitários corporativos de nuvem, serviço de e-mail e de navegação à Internet.

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

IX. **Gestão de Riscos:** os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação, com objetivo de implementar as proteções e controles adequados.

X. **Segurança no Desenvolvimento de Sistemas e Serviços:** o processo de desenvolvimento e manutenção de sistemas e serviços corporativos deve garantir a aderência às regras de desenvolvimento seguro e as boas práticas de segurança estabelecidos no PAN.

Data de Criação	Data da Última Aprovação	Data da Última Revisão
25.Mar.2019	**30.Mar.2021**	**30.Mar.2021**

XI. **Teste de Segurança:** a fim de identificar e reduzir vulnerabilidades nos ativos de informação, devem ser realizadas, por meio de testes de segurança, varreduras para identificação de vulnerabilidades no ambiente de tecnologia produtivo, minimamente a cada 30 dias. Uma vez identificada mudança em aberto para promoção de sistemas para ambientes de produção, uma varredura de vulnerabilidade deverá ser executada sob demanda. Anualmente, será executada, por consultoria independente, testes de penetração (manuais ou automatizadas) nos ambientes críticos para identificação de fragilidades nos ativos da informação, não excluindo a avaliação sobre os controles e processos de segurança já estabelecidos no PAN.

XII. **Cópias de Segurança (backup):** deve-se garantir de forma íntegra e confiável a restauração de qualquer tipo de dado registrado nos sistemas de informações e servidores de arquivos do PAN, pautado pela preservação da confiabilidade, integridade e disponibilidade da informação.

XIII. **Segurança na Gestão de Fornecedores:** os fornecedores devem ser classificados conforme diretrizes corporativas e caso sejam classificados como relevantes, serão selecionados, analisados e gerenciados em todo o ciclo de contratação e prestação de serviços, visando atender aos controles de segurança e regulatórios estabelecidos, de acordo com o tipo de serviço ou solução prestada e ter atribuído a ele um score de risco.

- **Aquisição de Bens e Serviços:** o processo de contratação de sistemas ou serviços que envolvam tecnologia ou processamento ou armazenamento de informações do PAN deve contemplar a análise de requisitos de segurança, com o procedimento de prova de conceitos, assim como a formalização da coleta de evidências dos requisitos analisados. Quando aplicável, a comunicação da contratação de fornecedores aos órgãos reguladores deverá ser realizada conforme regulamentação vigente.

- **Restrição na Contratação de Bens e Serviços:** a área de Segurança da Informação poderá vetar ou impor restrições para a contratação de sistemas ou serviços que envolvam tecnologia ou processamento ou armazenamento de informações do PAN quando constatar, a qualquer tempo, o não atendimento as regulamentações vigentes e/ou às políticas de segurança estabelecidas.

- **Controles e Incidentes Segurança:** devem ser avaliados os controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por fornecedores de serviços que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais do banco. Incidentes relevantes relacionados às informações do banco, armazenadas ou processadas pelo fornecedor, devem ser comunicadas à Segurança da Informação do PAN, através do canal csirt@grupopan.com.

XIV. **Proteção de perímetro:** a fim de proteger a infraestrutura do PAN contra-ataques externos, devem ser implementados, minimamente, ferramentas e controles contra: softwares e

mensagens maliciosas, invasão de dispositivos de rede e servidores, ataques a aplicativos e sistemas corporativos, ataques de negação de serviço e ameaça persistente avançada. Devem ser implementados controle de acesso de segmentação da rede corporativa, mitigando o risco contra acessos não autorizados.

XV. **Registro e Monitoramento:** os eventos lógicos de sistemas e serviços, assim como os eventos físicos, capturados e/ou identificados por câmeras, catracas e áreas restritas, devem ser devidamente registrados e monitorados, conforme regras estabelecidas no PAN.

Gestão de Incidentes: devem ser realizadas ações de prevenção, identificação, registro e resposta a incidentes e crises de segurança do ambiente tecnológico do PAN, que possam comprometer a confidencialidade, integridade e disponibilidade dos ativos da informação. Os incidentes de Segurança da Informação e Cibernéticos devem ser reportados ao diretor responsável pela 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, determinada pela exposição e relevância dos ativos da informação relacionados na ocorrência, incluindo a probabilidade da vulnerabilidade a ser explorada por ameaças e seu respectivo impacto no banco.

- **Compartilhamento de Incidentes:** incidentes relevantes que possam impactar outras instituições financeiras, devem ser compartilhadas com as demais instituições, com objetivo de reduzir o risco, seguindo diretrizes regulamentares.

- **Relatório de Segurança Cibernética:** anualmente a área de Segurança da Informação elaborará um relatório de resposta a incidentes, contendo o resumo dos resultados obtidos na implementação de rotinas, processos e tecnologias utilizados na prevenção e reposta a incidentes, assim como incidentes cibernéticos relevantes e os resultados dos testes dos cenários de crise cibernéticas. Este relatório deverá ser submetido ao Comitê de Riscos e apresentado ao Comitê de Administração até 31 de março do ano seguinte ao da data-base.

XVI. **Cenários de Crise Cibernética:** deve existir um registro em forma de catálogo, sobre os testes periódicos de cenários e situações onde incidentes de segurança de dimensões e danos significativos, com capacidade de comprometer operações críticas, reputação de negócios, possam se materializar nos ativos de informação do PAN. Devem ser catalogados os cenários de crises cibernéticas relacionadas aos incidentes de segurança, e inserido no relatório de resposta a incidentes relevantes ocorridos dentro do período, incluindo também os resultados dos testes de continuidade sobre estes cenários.

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

Data de Criação	Data da Última Aprovação	Data da Última Revisão
25.Mar.2019	**30.Mar.2021**	**30.Mar.2021**

6. ESTRUTURA DE GERENCIAMENTO

O PAN possui uma unidade específica de Segurança da Informação, compatível com a natureza, o porte, a complexidade, a estrutura, o perfil de risco e o modelo de negócio do PAN, e tem como função assegurar o efetivo gerenciamento do Risco de Segurança da Informação e Cibernético. Esta unidade está na estrutura da Segurança Corporativa, no qual reporta-se ao Diretor de Controladoria e Compliance e, portanto, encontra-se apartada das unidades de negócios/suporte e Auditoria Interna, estando alocada de forma a garantir a eficácia e autonomia de sua atuação, dispondo de recursos, pessoas e livre acesso às informações necessárias ao desempenho de suas atividades.

A estrutura da superintendência da Segurança Corporativa está dividida em 06 (seis) linhas estruturais, sendo: (a) Governança, Riscos e Compliance de Segurança da Informação, (b) Operações de Segurança da Informação, (c) Privacidade e Proteção de Dados, (d) Inspetoria, (e) Prevenção à Fraudes e (f) Governança de Tecnologia da Informação. Em consonância com a estrutura de gerenciamento da superintendência, diversas outras áreas participam do processo com seus respectivos papéis e responsabilidades, visando assegurar a eficiência, eficácia e efetividade dos controles e processos de gerenciamento, em linha com a estratégia do banco.

Esta estrutura utiliza-se da governança estabelecida no PAN por meio de comitês e alçadas estabelecidos pela administração, assim como a normatização que define o processo de tomada de decisão. Os processos e sistemas, que suportam e viabilizam a estrutura de gerenciamento de Segurança da Informação e Cibernética, estão descritos nas respectivas normas e procedimentos.

7. PROCESSO DE GERENCIAMENTO

O processo de gerenciamento da Segurança da Informação e Cibernética que dá subsídios à alta administração do PAN, abrange todo o ciclo da informação, contemplando os processos de definição, monitoramento e 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, registro e tratamento de incidentes, cenários de crises cibernéticas, implementação de controles preventivos e de segurança lógica no ambiente, transferência e descarte da informação, conscientização e treinamentos sobre segurança para colaboradores e prestadores de serviço.

8. RESPONSABILIDADES

As áreas e os órgãos colegiados, que formam a estrutura de gerenciamento de Segurança da Informação e Cibernética do PAN, atuam conforme as seguintes responsabilidades:

- **Conselho de Administração:** definir a orientação geral para o gerenciamento de riscos relacionados à Segurança da Informação do PAN, fazendo parte de suas atribuições, a aprovação da política corporativa de prevenção a estes riscos.
- **Comitê de Gestão Integrada de Riscos e Alocação de Capital**: órgão colegiado responsável por avaliar, acompanhar e prover a estrutura para execução do Programa

Data de Criação	Data da Última Aprovação	Data da Última Revisão
25.Mar.2019	**30.Mar.2021**	**30.Mar.2021**

de Segurança Cibernética, e promover comprometimento, apoio e aprovação do Plano de Ação e de Resposta a Incidentes, bem como a aderência dos colaboradores ao processo de Segurança da Informação e Cibernética do PAN.

- **Diretor de Segurança da Informação e Cibernética:** diretor estatutário indicado pelo Conselho de Administração, 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 na gestão estratégica do tema. É responsável também pela execução do Plano de Ação e de Resposta a Incidentes visando à implantação da Política Corporativa de Segurança da Informação e Cibernética.
- **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 a Alta Administração. 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.
- **Operação de Segurança da Informação - Cibersegurança:** área responsável pela prevenção, identificação, registro e resposta de Incidentes e Crises de Segurança da Informação ou Cibernética do PAN que possam comprometer a confidencialidade, integridade e disponibilidade, em parte ou totalmente, dos ativos da informação. Nesse aspecto, tem como responsabilidade, estabelecer canais de comunicação para incidentes, atuar proativamente na identificação de potenciais vulnerabilidades, utilizar os casos dos Incidentes na conscientização dos colaboradores e detalhar todas as ações de emergência adotadas no tratamento dos Incidentes.

  Gestores das Áreas de Tecnologia da Informação: atuar na gestão dos riscos associados à Segurança da Informação e Cibernética, inerentes a aplicação de controles de segurança na infraestrutura, desenvolver as soluções corporativas de forma segura, manter o parque tecnológico disponível e atualizado conforme as regras corporativas. Devem assegurar que as exposições a estes riscos estejam dentro dos limites definidos e em linha com as estratégias de negócio do PAN.
- **Gestores das Áreas de Negócio:** atuar na gestão dos riscos associados à Segurança da Informação e Cibernética, inerentes aos produtos, clientes e operações, sob sua responsabilidade, de acordo com as diretrizes, princípios e responsabilidades definidos nesta Política. Devem assegurar que as exposições a estes riscos estejam dentro dos limites definidos e em linha com as estratégias de negócio do PAN.
- **Colaboradores e Prestadores de Serviço:** observar e seguir os princípios, diretrizes e responsabilidades definidos nesta Política, e acionar imediatamente a área de Segurança da Informação sobre quaisquer eventuais descumprimentos ou ainda indícios de irregularidades, comportamentos, operações atípicas ou suspeitas que possam divergir com as diretrizes da Política.

Data de Criação	Data da Última Aprovação	Data da Última Revisão
25.Mar.2019	**30.Mar.2021**	**30.Mar.2021**

As violações das diretivas desta Política, estão sujeitas às sanções disciplinares previstas nas regras corporativas e no Código de Conduta e Ética do PAN

9. CONTROLE DE ATUALIZAÇÕES

Informar as principais alterações e/ou inclusão de conteúdo ocorridas na revisão do Normativo.

Descrição da Atualização:	Responsável:	Data da Revisão:
Ajuste em 10 diretrizes corporativas da Política, atualizando com os novos controles e trazendo mais detalhes aos itens relacionadas a: Conscientização em Segurança da Informação, Gestão de Ativos da Informação, Utilização de Recursos da Informação, Gestão de Acessos a Sistemas e Serviços, Classificação da Informação, Segurança no Desenvolvimento de Sistemas e Serviços, Teste de Segurança, Segurança na Gestão de Fornecedores, Gestão de Incidentes e de Crises de Segurança Inclusão de 7 novas diretrizes, ampliando os controles e processos de segurança, relacionadas a: Aquisição de Bens e Serviços, Restrição na Contratação de Bens e Serviços, Controles e Incidentes Segurança, Proteção de perímetro, Registro do Incidente, Compartilhamento de Incidentes e Relatório de Segurança Cibernética, Ajuste na estrutura e no processo de gerenciamento, em decorrência das mudanças da área de Segurança Corporativa. Ajustes nas responsabilidades, com a inclusão de 3 novas responsabilidades, sendo: Comitê de Gestão Integrada de Riscos e Alocação de Capital, Operação de Segurança da Informação – Cibersegurança e Gestores das Áreas de Tecnologia da Informação	Luiz Gustavo Buonanato	30/03/2021