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-se 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) 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 em perdas financeiras para o PAN.

- **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 visa 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 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:

- 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.
- 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.

Data de Criação	Data de Atualização	Data da Última Revisão
25.Mar.2019	**25.Mar.2019**	**25.Mar.2019**

- Gestão de Ativos da Informação: os ativos de informação do PAN devem ser identificados, inventariados e protegidos de acessos indevidos, através de controles físicos e lógicos.
- Utilização de Recursos da Informação: apenas os equipamentos e software, disponibilizados e/ou homologados pelo PAN, podem ser instalados e conectados à rede do PAN. Os mecanismos de proteção contra softwares maliciosos devem estar devidamente instalados e configurados nos equipamentos.
- 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.
- 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.
- Classificação da Informação: as informações devem ser atribuídas a proprietários, formalmente designados como responsáveis pela autorização de acesso às mesmas, e classificadas de acordo com a sua confidencialidade, proteção necessária, prazo de manutenção e descarte, em observância às regras estabelecidas no PAN, assim como às boas práticas de mercado e regulamentações vigentes.
- 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.
- 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.
- Segurança no Desenvolvimento de Sistemas e Serviços: o processo de desenvolvimento e manutenção de sistemas e serviços corporativos deve garantir a aderência às regras estabelecidas no PAN, assim como às boas práticas do mercado financeiro.
- Teste de Segurança: a fim de identificar vulnerabilidades nos ativos de informação, deve ser realizada, por meio de testes de segurança, a identificação de fragilidades em aplicativos móveis, serviços, sistemas corporativos e infraestrutura tecnológica.
- 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.
- Segurança na Gestão de Fornecedores: os fornecedores devem ser 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 ao PAN.
- 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 e de Crises de Segurança: devem ser realizadas a 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 do PAN devem ser reportados ao diretor responsável pela Segurança da Informação e Cibernética do PAN. Devem ser catalogados os cenários de crises cibernéticas relacionadas a incidentes de segurança, e elaborado anualmente um relatório de resposta a incidentes no ambiente lógico do PAN.

6. ESTRUTURA DE GERENCIAMENTO

A estrutura de gerenciamento da Segurança da Informação e Cibernética é composta pelas diversas áreas que participam do processo com seus respectivos papéis e responsabilidades, visando assegurar a eficiência, eficácia e efetividade desse gerenciamento, em linha com a estratégia do PAN.

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 manuais de processos e procedimentos.

7. PROCESSO DE GERENCIAMENTO

O processo de gerenciamento da Segurança da Informação e Cibernética abrange todo o ciclo da informação, contemplando os processos de definição, monitoramento e gestão dos ativos da informação, acessos lógicos a sistemas da informação, riscos de segurança, tratamento de incidentes, segurança na arquitetura e no desenvolvimento de sistemas da informação, classificação da informação, transferência e descarte da informação, segurança física do ambiente, conscientização e treinamento de segurança.

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.
- **Diretor de Segurança da Informação e Cibernética:** 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 respostas a incidentes visando à implantação da Política de Segurança da Informação e Cibernética.

Data de Criação	Data de Atualização	Data da Última Revisão
25.Mar.2019	**25.Mar.2019**	**25.Mar.2019**

- **Gestor de Riscos em Segurança da Informação:** 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.
- **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.