**Empresa: Nubank (Grupo Nubank);**

**Política de Segurança Cibernética (“Politica”)**

**Introdução**

No Nubank desenvolvemos soluções simples, seguras e 100% digitais para você ter o controle do seu dinheiro literalmente nas suas mãos. Valorizamos nossos clientes e entendemos o quanto a segurança cibernética é importante para usufruírem dos nossos serviços com tranquilidade.

Aplicamos a estratégia de defesa em profundidade por meio da implementação de mais de uma camada de segurança, com o objetivo de mitigar o possível comprometimento de uma das camadas de defesa.

A segurança das suas informações está no nosso DNA e disponibilizamos aqui um resumo da nossa Política de Segurança Cibernética ("Política") para que você possa conhecer um pouco mais das nossas diretrizes para proteção dos seus dados.

**Escopo**

Estão sujeitos à Política as empresas do Grupo Nubank ("Nubank") e todos os seus funcionários, consultores, terceiros, fornecedores e parceiros, caso acessem, armazenem, processem ou transmitam informações pertencentes, ou sob a guarda do Nubank.

**Objetivo**

1. Manter a confidencialidade, integridade e disponibilidade das informações de propriedade ou sob a guarda do Nubank;
2. Estabelecer medidas para a proteção da infraestrutura que suporta os serviços e atividades de negócio;
3. Prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

**Princípios de Segurança da Informação**

**Confidencialidade**: garantir que as informações são disponibilizadas ou divulgadas apenas a indivíduos, entidades ou processos autorizados;

**Integridade**: garantir que as informações são precisas, completas e protegidas de alterações indevidas, intencionais ou acidentais;

**Disponibilidade**: garantir que as informações são acessíveis e utilizáveis sob demanda por indivíduos, entidades ou processos autorizados.

**Diretrizes**

* O acesso a sistemas, recursos e outros ativos de informação deve ser concedido mediante a uma autenticação válida e baseado em:
* Necessidade de negócio;
* O princípio do menor privilégio; e
* Segregação de funções;
* Os acessos devem ser gerenciados através de um ciclo de vida desde a criação até a desativação, incluindo revisões periódicas quanto à precisão e adequação;
* A composição das senhas devem seguir os requisitos de complexidade e ser únicas. Não devem ser reutilizadas, compartilhadas, armazenadas em arquivos ou escritas em qualquer lugar.
* Logs e trilhas de auditoria devem ser habilitados em ambientes de produção, protegidos de acessos e alterações não autorizados e registrar:
* Que atividade foi executada;
* Quem executou a atividade;
* Quando a atividade foi executada;
* No quê a atividade foi executada;
* Algoritmos criptográficos devem ser aplicados conforme a necessidade em dados em repouso, em trânsito e/ou em uso;
* Ferramentas e processos para monitorar e impedir que informações sensíveis deixem o ambiente interno de uma organização sem autorização devem estar implementados;
* Soluções e/ou processos que permitam a prevenção, detecção, e identificação de ataques à componentes da infraestrutura do Nubank devem estar implementados;
* Um processo de gerenciamento do ciclo de vida de vulnerabilidades, desde a identificação até a remediação, incluindo diretrizes para documentação, emissão de relatórios e divulgação deve estar implementado;
* Soluções de software anti-malware de detecção, prevenção e recuperação ou controles equivalentes devem estar implementadas para proteger o ambiente do Nubank.
* Ativos de informação considerados críticos, que armazenem e/ou processem informações sensíveis, devem ser restringidos às áreas segregadas da rede, com controle de acesso apropriado;
* Bancos de dados de produção devem possuir backups suficientes para restaurar o funcionamento dos sistemas no evento de uma perda de dados ou interrupção de serviço;
* Durante o ciclo de vida de desenvolvimento de software, requisitos de segurança devem ser aplicados para garantir a confidencialidade, integridade e disponibilidade das informações;
* Deve ser feita uma avaliação de segurança antes da implementação de qualquer nova tecnologia, ferramenta ou solução em produção;
* Procedimentos e controles voltados à prevenção, tratamento, e redução da vulnerabilidade do Nubank a incidentes de segurança cibernética, além das diretrizes para registro, análise de causa e impacto, e avaliação da relevância de incidentes, devem estar implementados;
* Informações devem ser classificadas para auxiliar no mapeamento consistente dos ativos de informação e estabelecer o nível de proteção adequado em seu armazenamento, transmissão, e uso;
* O Plano de Continuidade de Negócios (PCN) visa garantir que, em situação de crise, os processos essenciais e críticos sejam devidamente mantidos, preservando assim a continuidade de funções de negócios, operações e serviços críticos. O PCN deve ser testado anualmente.
* Treinamentos de conscientização devem ser obrigatórios e realizados anualmente, apresentando os princípios de segurança da informação para auxiliar os funcionários a reconhecer situações de risco e agir corretamente;
* O consumo e compartilhamento de  informações de incidentes e ameaças com outras instituições locais e globais deve ser feito por canais seguros;
* A Política de Segurança Cibernética do Nubank deve ser revisada, no mínimo, anualmente.

**Recomendações de Segurança para Clientes**

* Crie senhas complexas e não utilize seus dados ou informações pessoais na composição (ex.: data de nascimento ou nomes de familiares). Dê preferência para senhas compostas de pelo menos 4 palavras aleatórias.
* Altere sua senha sempre que existir algum indício ou suspeita de vazamento, ou comprometimento das suas credenciais;
* Evite utilizar a mesma senha em mais de um serviço, se possível use um gerenciador de senhas para o armazenamento e gerenciamento de credenciais;
* Sua senha é pessoal e intransferível, portanto não a compartilhe e nem a anote em lugares que outras pessoas tenham fácil acesso (ex.: cadernos e bloco de notas);
* Se possível, habilite um segundo fator de autenticação (ex.: biometria ou SMS);
* Evite acessar sites e aplicativos bancários ou realizar transações em dispositivos (computadores, celulares e tablets) de terceiros, públicos (ex.: Lan House) ou não confiáveis. O mesmo vale para redes wireless (Wi-Fi) públicas;
* Mantenha seus dispositivos com os sistemas operacionais e aplicativos atualizados;
* Procure instalar uma solução de antivírus no seu computador e a mantenha atualizada;
* Evite abrir e-mails cujo remetente ou conteúdo sejam desconhecidos;
* Não clique em links disponibilizados em e-mails ou em mensagens SMS suspeitas e/ou desconhecidas;
* Não realize o download ou execute arquivos anexos em e-mails suspeitos (ex.: com erros gramaticais ou tom de urgência);
* Nunca informe dados pessoais, corporativos ou financeiros em ligações, ou mensagens recebidas de pessoas desconhecidas. O mesmo vale para sites suspeitos, sempre verifique se o site que você está acessando é realmente o verdadeiro;
* Bloqueie o dispositivo utilizado para acessar sites e aplicativos bancários quando não o estiver utilizando;
* Evite emprestar seu celular para pessoas desconhecidas;
* Mantenha sempre pelo menos uma cópia de segurança (backup) de dados importantes;