POLÍTICA DE SEGURANÇA CIBERNÉTICA

A segurança das informações de nossos clientes e das suas transações é um dos pilares da nossa empresa. Assim, a Conta Xip desenvolveu diversas etapas e processos de segurança com o intuito de mitigar quaisquer comprometimentos destas informações e fortalecer a gestão do risco de segurança cibernética com o objetivo de:

"Estabelecer os princípios, diretrizes e atribuições relacionadas à segurança da informação, protegendo as informações da instituição, dos clientes e do público em geral, observando as melhores práticas de mercado e regulamentações aplicáveis. Além de orientar os colaboradores e prestadores de serviços quanto aos procedimentos e controles da Conta Xip em relação à segurança cibernética".

Neste passo, toda informação de propriedade da Conta Xip seja protegida de forma a não comprometer a:

I. Confidencialidade: *garantir que somente pessoas autorizadas tenham acesso à informação;*
II. Integridade: *assegurar a exatidão das informações divulgadas, e*
III. Disponibilidade: *garantir que as informações estejam disponíveis para as pessoas devidas.*

DIRETRIZES GERAIS

- A Conta xip assume o compromisso de manter a continuidade dos negócios em caso de incidentes que possam comprometer o funcionamento de suas atividades;
- Os procedimentos e controles voltados à prevenção e ao tratamento de incidentes em relação aos prestadores de serviço de Tecnologia são previamente definidos em contratos;
- Classificação da criticidade dos Incidentes;
- A elaboração e acompanhamento do plano de ação são coordenados pela Diretoria Executiva e a Área de Segurança da Informação, com participação de outras áreas.
- Compromisso de compartilhar com o BACEN todos os incidentes relevantes, tempestivamente, sempre que solicitado.
- Toda contratação de serviços de processamento e armazenamento de dados e de computação em nuvem devem estar aderentes com as diretrizes indicadas na Resolução 3.909 do BACEN.
- O Diretor Presidente é o responsável pela Política de Segurança Cibernética
- É feito o monitoramento contínuo do ambiente tecnológico por meio de métodos diversos para assegurar a conformidade e adesão a esta Política. Caso haja violação das regras nela dispostas, bem como às demais normas e procedimentos de Segurança da Informação, mesmo que por omissão ou tentativa não consumada, tal violação pode ser classificada como incidente de segurança cibernética, os quais são passíveis de penalidades
- Quaisquer indícios de irregularidades no cumprimento das determinações desta política serão alvo de investigação interna.

RECOMENDAÇÕES DE SEGURANÇA PARA OS CLIENTES

- Crie senhas seguras, alfanuméricas e não utilize seus dados ou informações pessoais na composição;
- Sua senha é pessoal e intransferível, desta forma, não a compartilhe e não a mantenha anotada em fácil acesso;
- Ao suspeitar ou ler algum indício de acesso não autorizado, ou comprometimento das suas credenciais, altere sua senha imediatamente;
- Evite utilizar a mesma senha em mais de um serviço;
- Evite acessar sites e aplicativos bancários ou realizar transações em equipamentos de terceiros, públicos ou não confiáveis, inclusive em redes wi-fi públicas; e ainda mantenha a seus dispositivos com os sistemas operacionais e aplicativos atualizados e com uma solução de antivírus instalada e atualizada;
- Evite abrir e-mails e links cujo remetente ou conteúdo sejam desconhecidos; bem como não execute downloads ou e/ou arquivos anexos em e-mails suspeitos;
- Nunca informe dados pessoais, corporativos ou financeiros quando solicitados ativamente em ligações ou mensagens recebidas de pessoas e de sites suspeitos. É indicado que sempre verifique se o site que você está navegando é de fato o verdadeiro;
- Evite emprestar seu celular para terceiros.