Política de Segurança Cibernética e da Informação

1. Apresentação

Alinhada com os objetivos e requisitos do negócio, a Conpay estabelece nesta Política de Segurança Cibernética e da Informação, regras e direcionamentos a serem seguidos e aplicados a pessoas, processos e tecnologia, de forma a proteger as informações, de seus colaboradores, consultores, fornecedores, parceiros de negócios, e clientes. A informação é um ativo essencial para os negócios da Conpay e sendo assim, deve ser adequadamente protegida. Seguir as diretrizes desta política, significa proteger as informações, contra fraudes e zelar pela privacidade.

2. Escopo

Abrange todas as áreas de negócio, funcionários, consultores, terceiros, fornecedores, parceiros, e clientes; caso acessem, armazenem, processem ou transmitam informações pertencentes às demais operações.

3. Objetivo

- Garantir medidas de proteção da infraestrutura e continuidade de negócio;
- Prevenir, detectar e reduzir a vulnerabilidade a incidentes referente ao ambiente cibernético;
- Assegurar medidas de proteção à infraestrutura.

4. Conceitos e Definições

- Confidencialidade: Garantia de que a informação somente será acessada por pessoas efetivamente autorizadas;
- Disponibilidade: Garantia que a informação não será alterada ou violada indevidamente, por pessoas não autorizadas;
- Integridade: Garantia que a informação esteja disponível a pessoas autorizadas.

5. Diretrizes

- Zelar pela integridade da infraestrutura tecnológica em relação ao armazenamento, processamento ou quaisquer formas de tratamento de dados;
- Realizar classificação adequada das informações conforme princípios indicados nas políticas internas sobre esse tema;
- Garantir o monitoramento, controle ao acesso ao ativos e a informação, incluindo revisões periódicas;

- Aplicar varreduras periódicas para detecção de vulnerabilidades, incluindo documentação e relatórios;
- As senhas devem seguir padrões de complexidade. Não devem ser compartilhadas ou reutilizadas;
- Garantir a menor permissão possível, conforme descrito em normas internas específicas;
- Criptografia deve ser aplicada de acordo com cada necessidade, sempre que possível, conforme descrito em normas internas específicas;
- Garantir a manutenção das cópias de segurança dos dados e das informações;
- Garantir a continuidade de seus negócios (PCN), protegendo de interrupções críticas causadas por falhas, por meio de procedimentos e controles voltados à prevenção e tratamento de incidentes, bem como, a revisão anual do documento interno: plano de resposta a incidentes;
- Os incidentes de segurança e ameaças devem ser documentados em canais seguros;
- Elaborar um plano de backup;
- Os treinamentos de conscientização devem ser obrigatórios e realizados no mínimo anualmente;
- A política cibernética da Conpay deve ser revisada em um período não superior a um ano, quando será publicada uma nova versão, caso haja necessidade de ajustes.

6. Orientações de Segurança ao Clientes Conpay

- Utilizar senhas fortes, com combinações de letras maiúsculas, minúsculas, números e caracteres especiais;
- Não compartilhar suas senhas;
- Alterar sua senha periodicamente e sempre que houver comprometimento ou vazamento;
- Habilitar autenticação de dois fatores (exemplo: biometria, sms);
- Manter o sistema operacional e aplicativos do seu dispositivo atualizados com as últimas correções;
- Manter o sistema operacional do seu computador atualizado, um anti malware/antivírus instalado e atualizado;
- Evitar instalar softwares desconhecidos no mesmo dispositivo que você utiliza para acessar bancos;
- Evitar acessar sites bancários em redes Wi-fi públicas;
- Evitar abrir e-mails de remetente ou com conteúdo suspeito (Exemplo: anexos não solicitados, que contenham erros gramaticais, links desconhecidos ou suspeitos);
- Manter um backup dos dados importantes.