POLÍTICA DE CIBERSEGURANÇA – EXTERNA

1. OBJETIVO

A Política de Cibersegurança (“**Política**”) destinada ao público externo da Matrix Energia (“**Matrix**” ou “**Companhia**”), visa fornecer orientações claras para proteção de ameaças cibernéticas, práticas e procedimentos que são recomendados para ser seguidos para garantir a segurança, confidencialidade, integridade e disponibilidade das informações.

2. DIRETRIZES

2.1. Diretrizes Internas – Matrix

Os pilares de segurança da informação que seguimos para o conforto de nossos titulares e proteção dos sistemas contra acesso indevido ou não autorizado são:

- Confidencialidade;
- Integridade;
- Disponibilidade;
- Autenticidade; e
- Legalidade.

As diretrizes que a Matrix Energia segue rigorosamente para manter seu ambiente tecnológico protegido e seguro contra ameaças e ataques cibernéticos que são importantes para que nossos titulares saibam são:

I. Controles de segurança rigorosamente aplicados no ambiente de tecnologia e procedimentos para prevenção, identificação e tratamento de incidentes de Segurança Cibernética e mecanismos de proteção as informações de dados pessoais e sensíveis relevantes para a condução das atividades operacionais da Matrix Energia.

II. Atualização e manutenção do ambiente tecnológico de segurança dos sistemas, bem como controles de segurança da informação no descarte e manutenção segura de dados e equipamentos.

III. Monitoramento de serviços relevantes contratados referente aos riscos e boas práticas de segurança da informação.

IV. Programa de conscientização e treinamento para os colaboradores internos sobre a segurança das informações.

2.2. Diretrizes Externas – Titular

Algumas das diretrizes que consideramos importantes para seguir e boas práticas de segurança que recomendamos aos titulares dos dados:

I. **Senhas Fortes**: Crie senhas complexas e não repetidas para cada serviço/aplicativo. Use combinações de letras, números e símbolos. Um gerenciador de senhas pode ajudar a gerenciar e armazenar essas senhas de forma segura.

II. **Proteção de Dispositivos**: Configure medidas robustas de segurança, como:
   a. Senhas fortes;
   b. Controles biométricos;
   c. Mantenha seu dispositivo atualizado, sempre que possível, com a última versão. Caso não seja mais suportado pelo fabricante, opte por substituir com alternativas atualizadas; e
   d. Além disso, para serviços críticos como contas bancárias e e-mails, habilite o Múltiplo Fator de Autenticação – MFA (*Multi-factor Authentication*).

III. **Engenharia social**: É um método de ataque (*phishing* é um exemplo mais conhecido), onde um criminoso consegue persuadir, tanto pessoalmente quanto por telefone ou através de e-mails, com objetivo de "pescar" informações das vítimas. Muitas vezes abusando ou explorando da ingenuidade ou confiança do usuário, para obter informações privilegiadas. Portanto, não clique em links ou abra anexos de e-mails suspeitos. Verifique a autenticidade dos remetentes e a ortografia dos links. Desconfie de ofertas que pareçam boas demais para ser verdade e nunca envie sua senha para ninguém por qualquer meio de comunicação.

IV. **Proteção contra Malwares**: Use antivírus confiável e mantenha-o atualizado. Evite baixar programas de fontes não verificadas, pois podem conter vírus.

V. **Segurança de Dispositivos Portáteis**: Ative a funcionalidade no dispositivo para que, quando perdidos ou roubados, possam ser rastreados, apagados ou bloqueados. Em smartphones e notebooks, ative funcionalidades como rastreamento e limpeza remota de dados.

VI. **Redes Wi-Fi Públicas**: Evite realizar transações ou enviar informações sensíveis através de redes Wi-Fi públicas. Prefira redes móveis seguras.

VII. **Backups**: Faça backups regulares de dados importantes e teste a recuperação periodicamente. Armazene os backups em locais seguros e separados da fonte original.

3. CONCEITOS E SIGLAS

Autenticidade: Verificar a identidade de usuários, sistemas e dados para garantir que apenas entidades autorizadas tenham acesso.

Confidencialidade: Garantia de que as informações da Matrix Energia são acessíveis apenas por indivíduos devidamente autorizados.

Disponibilidade: Assegurar que os ativos de informação estejam acessíveis e operacionais quando necessário pelas partes autorizadas.

Integridade: Assegurar que as informações não sejam alteradas ou corrompidas de maneira não autorizada.

Legalidade: Garantir que as práticas de segurança da informação estejam em conformidade com leis e regulamentos específicos relacionados à privacidade, proteção de dados e segurança cibernética.

MFA – *Multi-factor Authentication* (Múltiplo Fator de Autenticação): Segundo método de confirmação de identidade do usuário que utiliza dois ou mais mecanismo de confirmação.

Malware: Software mal-intencionado que causa danos e infecta sistemas para roubar dados ou permitir acesso não autorizado.

Phishing: É uma tática de fraude online que simula entidades confiáveis para capturar informações pessoais ou financeiras dos usuários.