

J. Política de Segurança da Informação

Considerações Gerais

A Eco-Oil assume o compromisso de proteger as informações da organização contra acessos indevidos, perdas, alterações ou divulgações não autorizadas, promovendo um ambiente seguro para o uso da informação de processo, gestão ou outras arquivadas nos sistemas de suporte comuns e nos computadores dos seus Colaboradores.

Nesse sentido é estabelecida a política e ações práticas de proteção da informação e que se aplica a todos os colaboradores, fornecedores e terceiros que tenham acesso à rede informática e respectivas informações e sistemas da organização.

Princípios aplicáveis

- **Confidencialidade:** Assegurar que apenas pessoas autorizadas tenham acesso às informações.
- **Integridade:** Garantir que os dados sejam precisos e não alterados de forma indevida.
- **Disponibilidade:** Assegurar que as informações e sistemas estejam disponíveis quando necessários.

Ações de Suporte

- **Gestão de Acesso**
 - Cada usuário deve ter um login individual e protegido por senha.
 - O acesso será concedido com base no princípio do menor privilégio: apenas o necessário para realizar suas funções.
 - Os proprietários da informação decidem sobre o acesso e os privilégios dos seus recursos.
- **Proteção de Dados**
 - Informações confidenciais devem ser armazenadas de forma segura, preferencialmente em sistemas aprovados pela organização.
 - Dados sensíveis não devem ser compartilhados por canais inseguros, como redes sociais ou e-mails pessoais.
- **Dispositivos e Equipamentos**
 - Somente dispositivos autorizados podem ser usados para aceder informações da organização.
 - Mantenha os dispositivos protegidos com senha ou biometria e atualizados com as versões mais recentes dos softwares e antivírus.
- **Comunicação e Internet**
 - Evite aceder a informações corporativas em redes Wi-Fi públicas.
 - Não clique em links ou abra anexos de fontes desconhecidas.
 - Dados submetidos a programas públicos de inteligência artificial devem ser anonimizados ou expurgados de informação relevante sobre a organização.
- **Relato de Incidentes**
 - Qualquer situação suspeita, como perda de dispositivos, e-mails de phishing ou acessos não autorizados, deve ser comunicada de imediato.
- **Conscientização**
 - Todos os usuários devem seguir as boas práticas descritas de segurança da informação.
- **Sanções**
 - O não cumprimento desta política poderá resultar em advertências, medidas disciplinares ou rescisão contratual, conforme a gravidade da infração.