16. Política de Segurança de Dispositivos e Acesso Remoto

1. Contexto e Finalidade

O modelo de trabalho híbrido e o acesso remoto ao Sistema Web de Mentoria ampliam a necessidade de proteger os dispositivos utilizados pela equipe e parceiros da Paez Gestão.
Esta política estabelece controles e boas práticas para o uso seguro de **computadores, notebooks, tablets e smartphones corporativos e pessoais**, assegurando que a mobilidade não comprometa a confidencialidade, a integridade e a disponibilidade das informações corporativas.

A finalidade é padronizar os critérios de segurança aplicáveis ao uso de dispositivos, conexão remota, armazenamento local e acesso a dados da empresa, mitigando riscos de vazamento, infecção por malware e interceptação de comunicações.

---

2. Âmbito de Aplicação

Aplica-se a todos os dispositivos utilizados para acesso aos sistemas e dados da Paez Gestão, incluindo equipamentos próprios dos colaboradores (BYOD – Bring Your Own Device), desde que autorizados pelo setor de TI.
Abrange acessos via rede corporativa, VPN, conexões móveis e Wi-Fi.

---

3. Diretrizes Principais

1. **Configuração segura:** todos os dispositivos devem possuir antivírus atualizado, firewall habilitado e bloqueio automático de tela.
2. **Controle de acesso:** cada usuário deve possuir credenciais individuais e senhas seguras, sem compartilhamento.
3. **Proibição de uso indevido:** é vedado o uso de dispositivos corporativos para atividades pessoais, redes sociais privadas ou downloads não autorizados.
4. **Atualizações automáticas:** sistemas operacionais e aplicativos devem ser mantidos atualizados.
5. **VPN obrigatória:** o acesso remoto aos sistemas da empresa deve ocorrer apenas por rede virtual privada, configurada e monitorada pela TI.
6. **Armazenamento local:** é proibido armazenar dados corporativos em dispositivos pessoais sem criptografia.
7. **Perda ou roubo:** qualquer incidente com dispositivo que contenha dados da empresa deve ser comunicado imediatamente ao DPO.

8. **Descarte:** equipamentos substituídos devem passar por limpeza completa (wipe seguro).

---

4. Procedimentos Operacionais

- **Cadastro de dispositivos:** todos os equipamentos utilizados devem ser registrados junto ao setor de TI.
- **Configuração inicial:** a TI instala softwares de segurança e define políticas de bloqueio e senha.
- **Acesso remoto:** apenas dispositivos certificados e com VPN ativa podem acessar o banco de dados ou o sistema de mentoria.
- **Monitoramento:** logs de conexões são registrados para auditoria.
- **Desligamento:** ao término do contrato ou vínculo, o dispositivo deve ser devolvido ou ter acesso remoto revogado.

---

5. Monitoramento e Conformidade

A equipe técnica realiza inspeções trimestrais de conformidade nos dispositivos registrados.
O DPO supervisiona incidentes relacionados a acessos remotos, verificando se foram seguidas as medidas preventivas.
Qualquer descumprimento desta política pode resultar em suspensão de acesso, responsabilização disciplinar e comunicação à ANPD em caso de vazamento.
A Paez Gestão adota o princípio da **segurança pela configuração**, priorizando prevenção em vez de correção.