Darkbyte

Políticas de acesso e controle de usuários:

Autenticação forte: Todos usuários devem possuir uma senha forte, utilizando letras maiúsculas, minúsculas números e caracteres especial. Sendo no mínimo 8 caracteres.

Desativação de contas: Contas que não são usadas durante 30 dias devem ser desativadas.

Revisão: trimestralmente todos os usuários devem altera a sua senha, sem poder ser igual a antiga.

Politica de Uso de Dispositivos móveis e redes:

Uso de redes públicas: é proibido qualquer acesso as informações da empresa em redes públicas.

Uso de redes privadas: É obrigatório o uso de uma VPN segura em todos os dispositivos moveis

Compartilhamento e armazenamento: É proibido armazenar ou compartilhar qualquer dado sensível da empresa em dispositivos moveis sem criptografia.

Diretriz para respostas a incidentes de Segurança:

Registro de incidentes: Todos os incidentes e formas de ataque devem ser documentadas.

Equipe de resposta: Essa equipe será encarregada de investigar e mitigar qualquer tipo de incidente imediatamente.

Treinamento: A cada 1 mês fazer treinamentos com toda a equipe, abordando novos tipos de ameaças e os procedimentos de respostas.

Política de backup e recuperação de dados:

Backup: Fazer uma cópia dos dados semanalmente, para não correr risco de ter que pagar um possível sequestro.

Teste de recuperação: A cada 3 messes fazer teste de recuperação para ver se o backup foi copiado corretamente.

Backup diário: as informações mais sensíveis da empresa deverão ter um backup diário.