Membros

Gustavo Filgueiras - 824133435

Gustavo - 824126610

Mateus - 82411982

Pedro - 824135444

Thales - 824147589

Vinicius - 82410831

BET.SECURITY

Desenvolvimento de Políticas de Segurança para Pequenas Empresas

As pequenas empresas enfrentam desafios únicos no que diz respeito à segurança da informação. Desenvolver políticas de segurança sólidas é fundamental para proteger dados, recursos e reputação empresarial.

A Importância da Segurança da Informação para Pequenas Empresas

1 Proteção de Dados Críticos

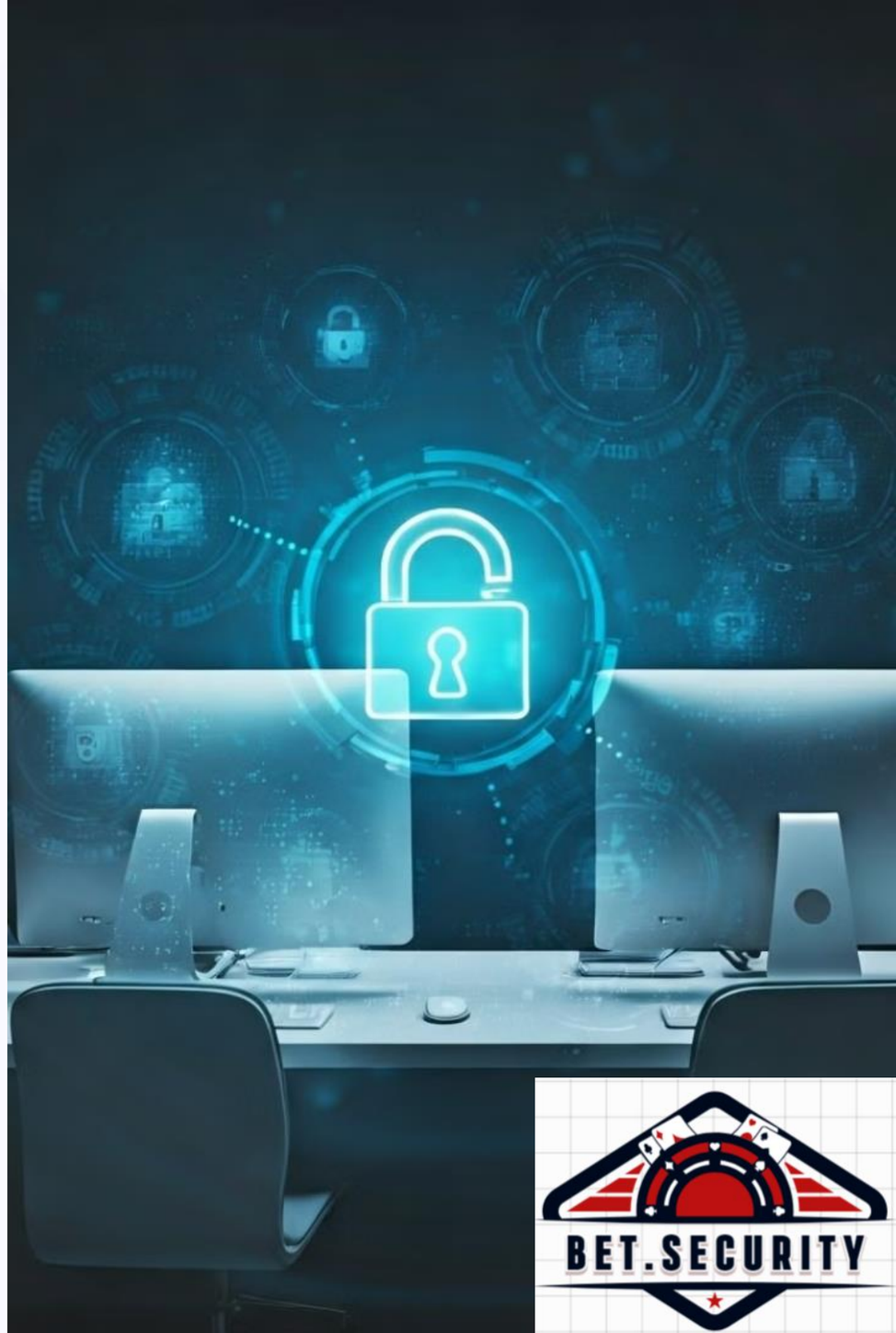
Evita a perda ou vazamento de informações confidenciais, como dados de clientes e propriedade intelectual.

2 Conformidade Regulatória

Garante o cumprimento de leis e normas aplicáveis ao setor, evitando multas e penalidades.

3 Manutenção da Reputação

Preserva a confiança dos clientes e parceiros comerciais, fortalecendo a imagem da empresa.



Políticas de Acesso e Controle de Usuários

Senhas Fortes

Exigir senhas com complexidade adequada e realizar alterações a cada 120 dias.

Controle de Acesso

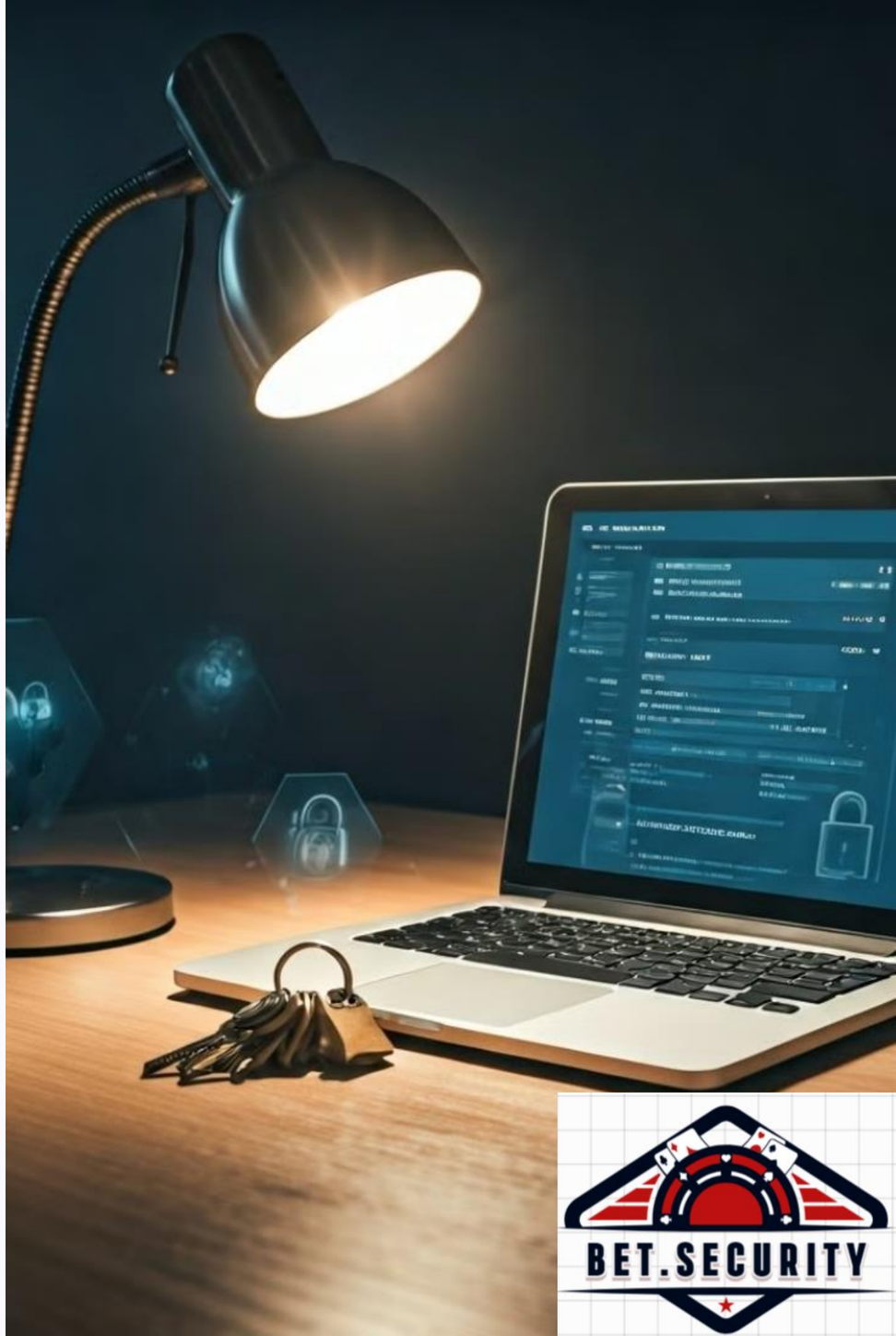
Limitar o acesso físico e lógico aos recursos da empresa.

Gestão de Permissões

Atribuir permissões com base no princípio do menor privilégio.

Educação de Usuários

Capacitar os colaboradores sobre boas práticas de segurança da informação.



Políticas de Uso de Dispositivos Móveis e Redes

1

Controle de Dispositivos

Estabelecer regras para o uso de dispositivos pessoais e corporativos, incluindo criptografia e controle remoto.

2

Acesso à Rede

Implementar redes seguras, com autenticação forte e controle de tráfego para prevenir invasões.

3

Conscientização de Usuários

Treinar os colaboradores sobre os riscos de acesso não autorizado e uso inadequado de dispositivos e redes.

Diretrizes para Respostas a Incidentes de Segurança

Detecção

Implementar soluções de monitoramento e ferramentas de detecção de ameaças.

Análise

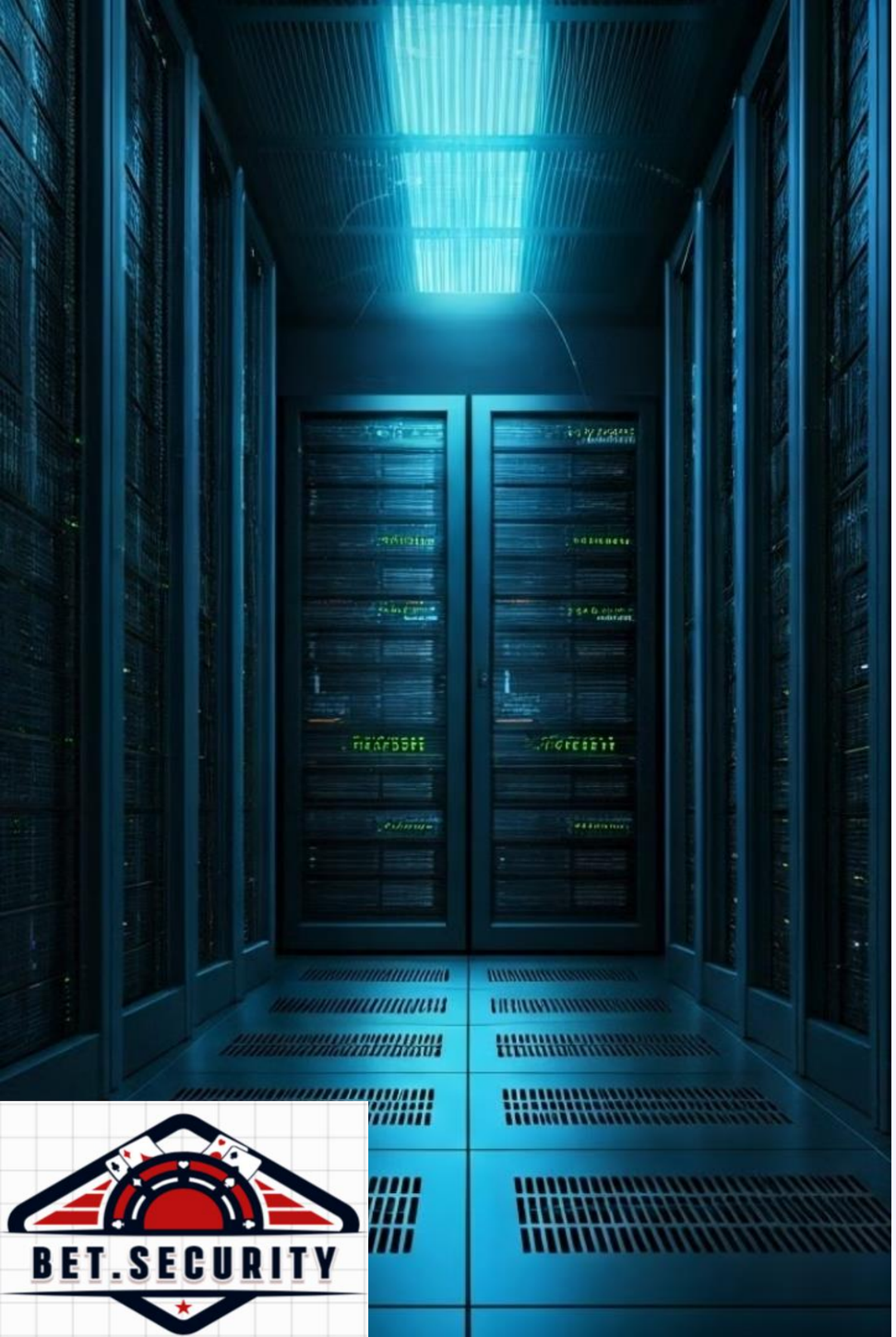
Investigar e compreender a natureza do incidente para determinar a melhor resposta.

Resposta

Definir e executar ações para conter, erradicar e recuperar-se do incidente.

Aprendizado

Avaliar o incidente e melhorar continuamente os processos de segurança.



Políticas de Backup e Recuperação de Desastres

1

Backup Regulares

Realizar backups periódicos de todos os dados críticos da empresa.

2

Armazenamento Seguro

Guardar backups em local remoto, protegido contra desastres e acessos não autorizados.

3

Testes de Recuperação

Testar periodicamente a restauração dos backups para garantir a integridade dos dados.