Relatório de Diagnóstico de Cibersegurança

Pontuação Geral:

235/500 (47.0%)

Desempenho por Categoria:

Conscientização e treinamento dos funcionários: 25/70 (35.71%)

Controle de acesso: 35/80 (43.75%)

Gerenciamento de riscos de terceiros: 30/50 (60.0%)

Governança e políticas: 35/70 (50.0%)

Proteção de dados: 35/70 (50.0%)

Resposta de incidentes e recuperação: 20/70 (28.57%)

Segurança de rede: 55/90 (61.11%)

Recomendações:

Foque-se em fortalecer as seguintes áreas: Controle de acesso, Resposta de incidentes e recuperação, Conscientização e treinamento dos funcionários.

Respostas Escolhidas:

Q1: Sim

Q2: Sim, documentado e designado

Q3: Ocasionalmente

Q4: Não

Q5: Sim, orçamento suficiente

Q6: Sim

Q7: Não tenho certeza

Q8: Sim, mas não contínuo

Q9: Sim, mensalmente ou com mais frequência

Q10: Sim

Q11: Não tenho certeza

Q12: Não

Q13: Sim, mas atrasado

Q14: Não

Q15: Sim, monitoramento em tempo real

Q16: Sim, mas criptografia fraca

Q17: Sim, sempre

Q18: Não

Q19: Sim, mas sem armazenamento externo

Q20: Sim, mas com menos frequência

Q21: Sim, mas com menos frequência

Q22: Sim, imposto por contratos

Q23: Sim, mas superficialmente

Q24: Não

Q25: Sim, mas as atualizações são opcionais

Q26: Não

Q27: Sim, imposto rigorosamente

Q28: Sim, com o MFA habilitado

Q29: Parcialmente aplicado

Q30: Sim, com auditorias regulares

Q31: Sim, mas sem medidas de segurança

Q32: Não

Q33: Não

Q34: Sim, com relatórios obrigatórios

Q35: Não

Q36: Não

Q37: Não

Q38: Não

Q39: Não

Q40: Não

Q41: Não

Q42: Parcialmente implementado

Q43: Não

Q44: Sim, anualmente

Q45: Sim, pelo menos anualmente

Q46: Não

Q47: Sim, com verificações regulares de conformidade

Q48: Sim, mas com pouca frequência

Q49: Não

Q50: Sim, mas não integrado