Relatório de Diagnóstico de Cibersegurança

Report Date: 2025

Desempenho por Categoria

Conformidade: 0/10 (0.0%)

Conscientização e treino dos funcionários: 30/70 (42.86%)

Conscientização em Segurança: 0/10 (0.0%)

Continuidade dos Negócios: 10/10 (100.0%)

Controlos de acesso: 20/30 (66.67%)

Gerenciamento de riscos de terceiros: 5/30 (16.67%)

Gestão de Ativos: 10/10 (100.0%)

Gestão de Riscos: 10/10 (100.0%)

Governança e Políticas: 10/10 (100.0%)

Governança e políticas: 20/60 (33.33%)

Proteção de Dados: 0/10 (0.0%)

Proteção de dados: 30/60 (50.0%)

Resposta a Incidentes: 0/10 (0.0%)

Resposta de incidentes e recuperação: 10/40 (25.0%)

Segurança de Rede: 5/10 (50.0%)

Segurança de rede: 50/80 (62.5%)

controlos de Acesso: 5/10 (50.0%)

controlos de acesso: 15/30 (50.0%)

Recomendações

Governança e Políticas

• Garanta que a política seja atualizada regularmente e alinhada com as ameaças de cibersegurança em evolução.

Gestão de Riscos

• Continue a realizar avaliações de risco regularmente e refine as estratégias de mitigação.

Gestão de Ativos

• Mantenha a adesão às melhores práticas e melhore continuamente os controlos de segurança.

controlos de Acesso

• Finalize a implementação das medidas de segurança e realize testes de validação.

Segurança de Rede

• Conclua o plano de resposta a incidentes e treine a equipa no manuseamento de incidentes.

Resposta a Incidentes

• Implemente as medidas de segurança necessárias para mitigar vulnerabilidades potenciais.

Continuidade dos Negócios

• Continue com as formações regulares de cibersegurança e introduza simulações de phishing.

Conscientização em Segurança

• Implemente uma estratégia robusta de backup para evitar perda de dados em caso

de incidentes.

Proteção de Dados

• Implemente as medidas de segurança necessárias para mitigar vulnerabilidades potenciais.

Conformidade

• Desenvolva uma política formal de cibersegurança, garantindo funções e responsabilidades claras.

Controlos de acesso

• Aprimore as medidas de controlos de acesso implementando a autenticação multifatorial.

• Aprimore as medidas de controlos de acesso implementando a autenticação multifatorial.

• Continue aplicando controlos rígidos de acesso e revise as políticas regularmente.

Segurança de rede

• Revise e atualize regularmente as configurações de segurança de rede e as redes de segmentos adequadamente.

• Fortalecer a segurança da rede adicionando controlos adicionais de monitorização e segmentação.

• Fortalecer a segurança da rede adicionando controlos adicionais de monitorização e segmentação.

• Revise e atualize regularmente as configurações de segurança de rede e as redes de segmentos adequadamente.

• Fortalecer a segurança da rede adicionando controlos adicionais de monitorização e segmentação.

• Implementar firewall, IDS/IPS e segmentação de rede para melhorar a segurança.

• Fortalecer a segurança da rede adicionando controlos adicionais de monitorização e segmentação.

• Revise e atualize regularmente as configurações de segurança de rede e as redes de segmentos adequadamente.

Governança e políticas

• Mantenha uma forte estrutura de governança e revise as políticas periodicamente.

• Aumente as medidas de governança alinhando -se às melhores práticas do setor.

• Desenvolva políticas formais de segurança e garantir a aplicação da organização.

• Desenvolva políticas formais de segurança e garantir a aplicação da organização.

• Desenvolva políticas formais de segurança e garantir a aplicação da organização.

• Aumente as medidas de governança alinhando -se às melhores práticas do setor.

Proteção de dados

• Verifique se os padrões de criptografia permanecem atualizados e revise as políticas de proteção de dados regularmente.

• Implementar ferramentas de criptografia e prevenção de perda de dados para proteger dados sensíveis.

• Implementar ferramentas de criptografia e prevenção de perda de dados para proteger dados sensíveis.

• Verifique se os padrões de criptografia permanecem atualizados e revise as políticas de proteção de dados regularmente.

• Expanda as medidas de criptografia e proteção de dados para cobrir todas as informações críticas.

• Expanda as medidas de criptografia e proteção de dados para cobrir todas as informações críticas.

controlos de acesso

• Aprimore as medidas de controlos de acesso implementando a autenticação

multifatorial.

• Continue aplicando controlos rígidos de acesso e revise as políticas regularmente.

• Implementar mecanismos estritos de controlos de acesso para evitar acesso não autorizado.

Gerenciamento de riscos de terceiros

• Implemente um programa de gerenciamento de riscos de fornecedores para avaliar a segurança de terceiros.

• Fortalecer as avaliações de segurança do fornecedor e requer documentação de conformidade.

• Implemente um programa de gerenciamento de riscos de fornecedores para avaliar a segurança de terceiros.

Resposta de incidentes e recuperação

• Desenvolva e implemente um plano de resposta a incidentes para minimizar o tempo de inatividade.

• Expanda e formalize o plano de resposta a incidentes com ações de resposta clara.

• Expanda e formalize o plano de resposta a incidentes com ações de resposta clara.

• Desenvolva e implemente um plano de resposta a incidentes para minimizar o tempo de inatividade.

Conscientização e treino dos funcionários

• Aumente a frequência de treino e introduza programas de conscientização de segurança interativos.

• Aumente a frequência de treino e introduza programas de conscientização de segurança interativos.

• Desenvolva um programa obrigatório de treino de segurança para educar os funcionários sobre riscos.

• Aumente a frequência de treino e introduza programas de conscientização de

segurança interativos.

• Aumente a frequência de treino e introduza programas de conscientização de segurança interativos.

• Desenvolva um programa obrigatório de treino de segurança para educar os funcionários sobre riscos.

• Continue simulações regulares de treino e phishing de conscientização de segurança.

Ferramentas Recomendadas

Conformidade:

Conscientização e treino dos funcionários:

Conscientização em Segurança:

Gerenciamento de riscos de terceiros:

Governança e políticas:

Proteção de Dados:

Resposta a Incidentes:

Resposta de incidentes e recuperação: