Relatório de Diagnóstico de Cibersegurança

Pontuação Geral:

240/500 (48.0%)

Desempenho por Categoria:

Conformidade: 5/10 (50.0%)

Conscientização e treino dos funcionários: 45/70 (64.29%)

Conscientização em Segurança: 0/10 (0.0%)

Continuidade dos Negócios: 0/10 (0.0%)

Controlos de acesso: 15/30 (50.0%)

Gerenciamento de riscos de terceiros: 10/30 (33.33%)

Gestão de Ativos: 5/10 (50.0%)

Gestão de Riscos: 10/10 (100.0%)

Governança e Políticas: 10/10 (100.0%)

Governança e políticas: 35/60 (58.33%)

Proteção de Dados: 0/10 (0.0%)

Proteção de dados: 35/60 (58.33%)

Resposta a Incidentes: 10/10 (100.0%)

Resposta de incidentes e recuperação: 15/40 (37.5%)

Segurança de Rede: 5/10 (50.0%)

Segurança de rede: 20/80 (25.0%)

controlos de Acesso: 5/10 (50.0%)

controlos de acesso: 15/30 (50.0%)

Recomendações:

Foque-se em fortalecer as seguintes áreas: Continuidade dos Negócios, Conscientização em Segurança, Proteção de Dados, Segurança de rede, Gerenciamento de riscos de terceiros, Resposta de incidentes e recuperação.

Suggested Tools for Improvement:

Proteção de Dados: VeraCrypt, BitLocker

Respostas Escolhidas:

Q1: Tem uma política de cibersegurança escrita e aprovada?

Resposta: Sim

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

Q2: A sua organização realizou uma avaliação formal de riscos no último ano?

Resposta: Sim

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

Q3: Todos os ativos da empresa estão inventariados e categorizados?

Resposta: Em progresso

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

Q4: A autenticação multifator (MFA) é obrigatória para acessar sistemas críticos?

Resposta: Em progresso

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

Q5: Você tem um plano documentado de resposta a incidentes?

Resposta: Em progresso

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

Q6: A sua organização realizou uma análise de impacto nos negócios?

Resposta: Sim

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

Q7: Os funcionários recebem treino regular em conscientização sobre cibersegurança?

Resposta: Não

Recomendação: Implemente um programa obrigatório de conscientização sobre segurança para todos os funcionários.

Q8: Os backups são realizados regularmente e testados quanto à integridade?

Resposta: Não

Recomendação: Implemente uma estratégia robusta de backup para evitar perda de dados em caso de incidentes.

Q9: Você está em conformidade com o GDPR, ISO 27001 ou outros regulamentos de proteção de dados?

Resposta: Não

Recomendação: Implemente as medidas de segurança necessárias para mitigar vulnerabilidades potenciais.

Q10: Tem uma política de controlo de acesso que define funções e privilégios dos utilizadors?

Resposta: Em progresso

Recomendação: Finalize o desenvolvimento da sua política de cibersegurança e procure validação especializada.

Q11: Mantém um log de todo o acesso do utilizador a sistemas críticos?

Resposta: Sim, com auditorias regulares

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

Q12: Você bloqueia o acesso a sites maliciosos usando uma solução de filtragem na web?

Resposta: Não

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

Q13: Você bloqueia os dispositivos não autorizados de acessar a sua rede?

Resposta: Não

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

Q14: Você realiza auditorias de terceiros do seu programa de cibersegurança?

Resposta: Sim, mas com pouca frequência

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

Q15: Você restringe o acesso a dados confidenciais com base nas funções dos funcionários?

Resposta: Sim, imposto rigorosamente

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

Q16: Você revisa e atualiza regularmente as suas políticas de cibersegurança?

Resposta: Sim, anualmente ou com mais frequência

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

Q17: Os privilégios administrativos estão restritos ao pessoal essencial?

Resposta: Não

Recomendação: Implementar mecanismos estritos de controlos de acesso para evitar acesso não autorizado.

Q18: Você precisa de fornecedores de terceiros para aderir às suas políticas de cibersegurança?

Resposta: Parcialmente

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

Q19: Você tem uma firewall instalada e configurado na sua rede?

Resposta: Não tenho certeza

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

Q20: Você usa redes privadas virtuais (VPNs) para acesso remoto?

Resposta: Sim, mas sem MFA

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

Q21: Você segenta a sua rede para isolar dados confidenciais?

Resposta: Não

Recomendação: Implementar firewall, IDS/IPS e segmentação de rede para melhorar a

segurança.

Q22: Você aloca um orçamento específico para iniciativas de cibersegurança?

Resposta: Não

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

Q23: Você monitora o tráfego de rede em busca de atividades suspeitas?

Resposta: Não

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

Q24: Você tem um método seguro para compartilhar informações confidenciais internamente?

Resposta: Parcialmente implementado

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

Q25: Você tem ferramentas automatizadas para detectar e responder a incidentes de segurança?

Resposta: Sim, parcialmente automatizado

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

Q26: As tentativas de login são monitorizadas quanto a atividades suspeitas?

Resposta: Não

Recomendação: Implementar mecanismos estritos de controlos de acesso para evitar acesso não autorizado.

Q27: Você conduz exercícios de simulação de phishing?

Resposta: Sim, anualmente ou com mais frequência

Recomendação: Continue simulações regulares de treino e phishing de conscientização de segurança.

Q28: Você treina funcionários com segurança usando dispositivos móveis e pessoais para o trabalho?

Resposta: Sim, mas com pouca frequência

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

Q29: Os dados sensíveis são criptografados em trânsito?

Resposta: Às vezes

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

Q30: Todos os funcionários têm credenciais exclusivas de login?

Resposta: Não tenho certeza

Recomendação: Aprimore as medidas de controlos de acesso implementando a autenticação multifatorial.

Q31: Os backups regulares dos dados críticos são executados?

Resposta: Sim, com armazenamento externo

Recomendação: Teste e refine o plano de resposta a incidentes regularmente para melhorar a eficácia.

Q32: Você conduz treino obrigatório de conscientização sobre cibersegurança para novas contratações?

Resposta: Sim, mas atrasado

Recomendação: Aumente a frequência de treino e introduza programas de

conscientização de segurança interativos.

Q33: Você fornece treino sobre práticas de navegação segura?

Resposta: Sim, mas com pouca frequência

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

Q34: Você realiza avaliações de segurança nos serviços em nuvem usados

por sua organização?

Resposta: Sim, mas apenas uma vez durante a adoção

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

Q35: As funções e responsabilidades de cibersegurança são claramente definidas em sua organização?

Resposta: Sim, mas informal

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

Q36: Os funcionários relatam tentativas de phishing e e -mails suspeitos?

Resposta: Sim, mas voluntário

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

Q37: Você comunica regularmente atualizações de cibersegurança aos funcionários?

Resposta: Sim, mas com menos frequência

Recomendação: Aumente a frequência de treino e introduza programas de

conscientização de segurança interativos.

Q38: Você usa sistemas de detecção e prevenção de intrusões (IDS/IPS)?

Resposta: Não tenho certeza

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

Q39: As contas de funcionários rescindidos são prontamente desativados?

Resposta: Sim, mas atrasado

Recomendação: Aprimore as medidas de controlos de acesso implementando a autenticação multifatorial.

Q40: Você mantém um registro de todos os incidentes de segurança e violações?

Resposta: Não

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

Q41: Você realiza avaliações anuais de risco de cibersegurança?

Resposta: Ocasionalmente

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

Q42: Você exige que os fornecedores sigam os regulamentos de proteção de dados (por exemplo, GDPR, HIPAA)?

Resposta: Sim, mas sem verificações de conformidade

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

Q43: Você realiza exercícios de treino regular de resposta a incidentes?

Resposta: Não

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

Q44: Você tem um programa de conscientização sobre cibersegurança para funcionários?

Resposta: Sim, em progresso e obrigatório

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

Q45: Você aplica uma política de retenção e exclusão de dados?

Resposta: Sim, mas pouco seguido

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

Q46: Você garante que os fornecedores tenham seguro de cibersegurança?

Resposta: Não

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

Q47: Você implementa os controlos de acesso baseados em funções (RBAC)?

Resposta: Sim, estritamente aplicado

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

Q48: Você fornece treino contínuo para identificar e prevenir ataques de phishing?

Resposta: Sim, trimestralmente ou com mais frequência

Recomendação: Continue simulações regulares de treino e phishing de conscientização de segurança.

Q49: A autenticação multifatorial (MFA) é ativada para todos os sistemas críticos?

Resposta: Sim para todos os sistemas

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

Q50: Você aplica políticas de senha fortes em toda a organização?

Resposta: Não

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