Autoavaliação de Cibersegurança

CyberScore: 

Data de geração do relatório: **08/11/2026 20:16**

> Este relatório é uma simples autoavaliação do seu nível de segurança da informação, baseada exclusivamente nas suas respostas ao questionário elaborado pelos especialistas da Oxydian. Ele não constitui, em hipótese alguma, uma auditoria técnica aprofundada. Embora ofereça uma primeira visão dos seus pontos fortes e vulnerabilidades em cibersegurança, ele não substitui uma análise rigorosa da sua infraestrutura e dos seus sistemas. Para ir além e contar com uma auditoria técnica completa, fale com a gente:
>
> contact@oxydian.fr

Resumo:

O seu nível de segurança apresenta fragilidades significativas que merecem atenção imediata. O risco de exploração de algumas vulnerabilidades é elevado, o que pode comprometer a segurança global da sua organização. Recomendamos fortemente a adoção de medidas corretivas e um acompanhamento especializado para realizar uma auditoria aprofundada.

Detalhamento das notas por categoria (40.0%)

Senhas

Segurança dos dados



Monitoramento e detecção



Segurança interna



Segurança externa



Gestão da segurança



Identificação de riscos



Segurança física



Plano de ação personalizado:

Este plano de ação se baseia nos resultados da sua avaliação. Recomendamos seguir estas orientações para melhorar a sua segurança da informação.

Armazenamento seguro das senhas
Garanta que todas as senhas sejam armazenadas em um gerenciador de senhas seguro, e não em meios não seguros.

Usar um antivírus
Garanta que todos os seus servidores e computadores tenham um antivírus atualizado para detectar e bloquear ameaças.

Substituição dos computadores obsoletos
Substitua ou migre os computadores obsoletos (Windows XP, Vista, 7, 8 ou Windows Server 2003 / 2008 / 2012) para reduzir os riscos de vulnerabilidades sem correção.

Separar os direitos de usuário e de administrador
Essa prática consiste em atribuir contas distintas para as tarefas do dia a dia e para as tarefas administrativas. Isso reduz consideravelmente os riscos de comprometimento, limitando o acesso a privilégios elevados apenas às operações específicas que exigem administração.

Implantação de uma política de senhas
Implante uma política de senhas rigorosa para garantir que as senhas sejam seguras, complexas e renovadas regularmente.

Proteção do e-mail com 2FA
Ative a autenticação de dois fatores (2FA) em todas as contas de e-mail da empresa (Microsoft 365, Google Workspace etc.). O comprometimento de e-mail é o vetor de ataque mais frequente contra PMEs, e a 2FA bloqueia a grande maioria desses ataques.

Análise regular das senhas
Faça análises regulares das suas senhas com um profissional ou com o seu diretor de TI para detectar senhas fracas e reutilizadas e reforçar a segurança.

Implantação da criptografia de disco
Recomendamos fortemente ativar a criptografia de disco em todos os computadores e servidores, usando soluções como o BitLocker para Windows ou o LUKS para Linux, a fim de proteger os seus dados sensíveis contra acessos não autorizados.

Testes de restauração dos backups
Programe testes de restauração regulares (pelo menos uma vez por trimestre) para verificar se os seus backups realmente funcionam e medir o tempo necessário para retomar as suas atividades.

Mapeamento dos ativos externos
Atualize e complete regularmente o mapeamento dos seus ativos expostos na internet para melhorar a gestão da segurança.

Implantação da 2FA na VPN
Ative a autenticação de dois fatores (2FA) em todos os acessos à VPN para reforçar a segurança das conexões remotas.

Procedimento de resposta a incidentes
Formalize um procedimento de resposta a incidentes: primeiras ações a tomar, lista de contatos de emergência (prestador especializado, seguradora, autoridade de proteção de dados em caso de vazamento) e papéis internos. Teste-o pelo menos uma vez por ano por meio de um exercício de mesa (tabletop).

Implantação da autenticação de dois fatores
Ative a autenticação de dois fatores (2FA) em todas as suas contas e serviços críticos para adicionar uma camada extra de segurança.

Redundância dos backups
Recomendamos fortemente armazenar os seus backups em vários locais diferentes para reduzir os riscos de perda de dados em caso de sinistro.

Evolução para um EDR
Substitua ou complemente o seu antivírus tradicional com uma solução EDR (Endpoint Detection and Response), capaz de detectar comportamentos maliciosos e isolar computadores comprometidos diante de ataques modernos, como os ransomwares.

Centralização dos logs
Centralize os logs dos seus servidores e equipamentos críticos em um espaço de armazenamento dedicado e guarde-os por vários meses (de 6 a 12 meses recomendados). Assim, é possível detectar e analisar incidentes mesmo que o invasor apague os rastros locais.

Mapeamento dos ativos internos
Atualize e complete regularmente o mapeamento dos seus ativos internos para melhorar a gestão da segurança.

Segmentação da rede Wi-Fi
Implemente várias redes Wi-Fi para separar os acessos públicos e internos, reforçando a segurança e oferecendo ao mesmo tempo um Wi-Fi público apenas para acesso à internet.

Implantação de uma política de atualização externa
Adote uma política rigorosa de atualização para todos os seus ativos externos, a fim de minimizar os riscos ligados às vulnerabilidades.

Implantação de uma política de uso de TI
Garanta que todos os colaboradores assinem uma política de uso de TI que defina as regras e boas práticas de segurança, com ênfase na proteção dos dados pessoais para atender às exigências do RGPD.

Simulações de phishing regulares
Organize campanhas de simulação de phishing pelo menos uma vez por ano para medir os reflexos dos seus colaboradores em condições reais e direcionar a conscientização para os pontos fracos identificados.

Controle dos acessos de prestadores
Controle os acessos dos seus prestadores de serviço: contas nominais dedicadas, direitos limitados ao estritamente necessário, desativação sistemática ao fim da intervenção ou do contrato e rastreabilidade das conexões.

Controle de acesso à sala de servidores
Implemente um controle rigoroso de acesso à sala de servidores para evitar manipulações não autorizadas.

Implantação de um procedimento de entrada e saída
Defina um procedimento claro para a entrada e a saída de colaboradores, incluindo a exclusão das contas e dos acessos, para proteger a empresa contra riscos de segurança.

Legenda:

INFORMAÇÃO

Risco global nulo, trata-se apenas de observações levantadas durante a auditoria.

MENOR

Risco global baixo, que não exige ações significativas.

MODERADO

Risco global moderado, que exige ações a médio prazo.

MAIOR

Risco global alto, que exige ações a curto prazo.

CRÍTICO

Risco global crítico, que exige ações imediatas.