

GUIA TÉCNICO GRATUITO

Checklist de Cibersegurança para Hotéis **guia completo**

25 controles de identidade, rede, fornecedores e conformidade, com o porquê de cada um, como avaliar sua operação e o passo a passo para resolver.

25

controles

4

áreas

2026

edição

hotelti.com.br

Como usar este guia

Hotéis conectam PMS, terminais POS, Wi-Fi de hóspedes, fechaduras eletrônicas e sistemas de fornecedores numa única rede operacional. Cada categoria abaixo é um ponto de entrada ou caminho de movimento lateral já confirmado em incidentes reais do setor hoteleiro, e os 25 controles deste guia tratam das falhas que se repetem nesses incidentes.

01

Identidade e acesso

02

Rede e infraestrutura

03

Fornecedores e integrações

04

Conformidade e resposta a incidentes

Como percorrer o checklist

1. **Avalie item por item:** cada um traz uma pergunta objetiva para confirmar se o controle já existe na sua operação.
2. **Use o selo de complexidade** para priorizar: comece pelos itens rápidos, que costumam ser configuração interna sem custo adicional.
3. **Trate os itens de projeto como plano, não como pendência de uma tarde:** eles geralmente exigem orçamento, um fornecedor ou uma mudança de processo.
4. **Revise o guia a cada 6 a 12 meses,** ou sempre que trocar de PMS, motor de reservas ou fornecedor de pagamento.

● Rápido: ajuste de configuração interna ● Médio: envolve fornecedor ou processo novo

● Projeto: requer orçamento e planejamento

01 Identidade e acesso

Quem consegue entrar nos seus sistemas, com qual credencial, e por quanto tempo depois de deixar de precisar.

1. Autenticação multifator (MFA) ativa no PMS, e-mail corporativo e painéis administrativos

RÁPIDO

POR QUE IMPORTA

Login e senha sozinhos são a causa mais comum de acesso indevido. Um segundo fator torna uma senha vazada, sozinha, insuficiente para um invasor.

COMO AVALIAR

Pergunte: se eu soubesse a senha de um funcionário agora, conseguiria entrar no PMS sem mais nada?

COMO RESOLVER

- Ative MFA na configuração do PMS, e-mail e VPN/acesso remoto. Não deixe como opcional
- Priorize contas com acesso administrativo ou financeiro primeiro
- Use um app autenticador em vez de SMS sempre que o sistema permitir

2. Nenhum login compartilhado entre funcionários em sistemas de PMS ou POS

RÁPIDO

POR QUE IMPORTA

Login compartilhado impede saber quem fez o quê e torna impossível revogar o acesso de uma pessoa sem afetar todo o turno.

COMO AVALIAR

Verifique quantos funcionários conseguem citar de cor a senha genérica de recepção ou caixa.

COMO RESOLVER

- Crie um usuário individual por funcionário no PMS e no POS
- Desative contas genéricas do tipo "recepção" ou "caixa1"
- Ative o log de auditoria por usuário, se o sistema oferecer

3. Acessos de ex-funcionários revogados no mesmo dia do desligamento

MÉDIO

POR QUE IMPORTA

Setores com alta rotatividade, como recepção e temporada, são onde esse controle mais falha, e onde mais fica um acesso esquecido ativo por meses.

COMO AVALIAR

Peça a lista de usuários ativos no PMS e compare com a folha de pagamento atual.

COMO RESOLVER

- Crie um checklist de desligamento cobrindo PMS, e-mail, Wi-Fi, VPN e sistemas de fornecedores
- Torne a revogação de acesso parte formal do processo de RH, não uma tarefa avulsa de TI
- Audite trimestralmente usuários ativos versus funcionários atuais

4. Monitoramento de credenciais vazadas ou expostas na dark web

MÉDIO

POR QUE IMPORTA

Boa parte das senhas corporativas circula em vazamentos de outros serviços muito antes de serem usadas contra o hotel.

COMO AVALIAR

Pergunte se alguém já checkou os e-mails corporativos em um serviço de verificação de vazamentos nos últimos 6 meses.

COMO RESOLVER

- Contrate ou ative um serviço de monitoramento de credenciais vazadas para os domínios da empresa
- Defina um processo automático de troca de senha quando uma credencial for sinalizada

5. Acesso a PMS e POS restrito por função, sem permissões administrativas por padrão

MÉDIO

POR QUE IMPORTA

Quanto mais gente com acesso administrativo, maior a superfície de erro e de ataque. A maioria das funções não precisa desse nível de permissão.

COMO AVALIAR

Liste quantos usuários têm permissão de administrador no PMS hoje e quantos realmente precisam dela no dia a dia.

COMO RESOLVER

- Aplique o princípio do menor privilégio: cada função vê e altera só o necessário
- Documente exceções administrativas com justificativa e data de revisão

6. Contas de extranet de OTAs (Booking.com, Expedia e similares) protegidas com MFA e equipe treinada contra phishing direcionado

MÉDIO

POR QUE IMPORTA

Campanhas recentes comprometem contas de extranet para enviar mensagens falsas de "reconfirmação de reserva" a hóspedes, e algumas induzem a equipe a rodar comandos maliciosos no computador (técnica conhecida como ClickFix).

COMO AVALIAR

Confirme se a extranet de cada OTA usada pelo hotel tem autenticação em duas etapas ativa, e não apenas senha.

COMO RESOLVER

- Ative a autenticação em duas etapas oferecida pela própria plataforma da OTA
- Oriente a equipe a nunca copiar e executar comandos ou scripts recebidos por e-mail, chat ou mensagem de hóspede
- Revise periodicamente quem na equipe tem acesso à extranet

02 Rede e infraestrutura

Como PMS, POS, Wi-Fi de hóspedes e dispositivos de quarto se comunicam entre si, e o que os separa de um invasor.

7. Wi-Fi de hóspedes segmentado e isolado da rede operacional e do PMS

PROJETO

POR QUE IMPORTA

Sem segmentação, um dispositivo comprometido na rede de hóspedes consegue, em teoria, "enxergar" o PMS e os terminais de pagamento.

COMO AVALIAR

Peça ao seu provedor de TI o diagrama de rede atual e confirme se hóspedes, operação e dispositivos de quarto estão em VLANs separadas.

COMO RESOLVER

- Configure VLANs distintas para hóspedes, operação e dispositivos de quarto
- Bloqueie por padrão o tráfego entre VLANs, liberando só o estritamente necessário

8. Rede de terminais POS isolada, dentro do escopo definido para o PCI DSS

PROJETO

POR QUE IMPORTA

Terminais com P2PE (criptografia ponto a ponto) cifram o dado do cartão já na leitura, para que o número completo nunca circule desprotegido pela rede do hotel.

COMO AVALIAR

Pergunte ao seu adquirente ou fornecedor de POS se os terminais atuais são certificados P2PE.

COMO RESOLVER

- Isole a rede de POS em uma VLAN própria dentro do escopo do PCI DSS
- Priorize a troca por terminais com P2PE certificado na próxima renovação de contrato

9. Credenciais padrão trocadas em TVs, fechaduras e dispositivos de quartos inteligentes

RÁPIDO

POR QUE IMPORTA

Todo equipamento de IoT sai de fábrica com usuário e senha padrão, muitas vezes públicos em manuais disponíveis on-line.

COMO AVALIAR

Teste o login padrão de fábrica em um dispositivo de amostra. Se funcionar, o problema é real.

COMO RESOLVER

- Troque todas as credenciais padrão antes ou imediatamente após a instalação
- Documente onde cada credencial fica registrada, com acesso restrito a essa lista

10. Varredura ativa de vulnerabilidades além de firewall e antivírus padrão

MÉDIO

POR QUE IMPORTA

Firewall e antivírus são a base, não o teto. Eles não avisam sobre um sistema desatualizado ou mal configurado antes que alguém o explore.

COMO AVALIAR

Pergunte quando foi a última varredura de vulnerabilidades feita na sua rede. Se não souber responder, provavelmente nunca foi feita.

COMO RESOLVER

- Contrate varreduras periódicas, internas e externas
- Trate as descobertas como plano de correção com prazo, não como relatório arquivado

11. Backups testados periodicamente, com cópia offline ou isolada da rede principal

MÉDIO

POR QUE IMPORTA

Um backup que nunca foi restaurado é uma suposição, não uma garantia. Um backup só conectado à rede principal também é alvo do mesmo ransomware.

COMO AVALIAR

Pergunte quando foi a última vez que alguém restaurou um backup de teste, não apenas confirmou que ele "rodou".

COMO RESOLVER

- Teste a restauração completa pelo menos uma vez por trimestre
- Mantenha ao menos uma cópia offline ou isolada da rede principal

12. Detecção e resposta em endpoints (EDR) nos computadores de recepção, back-office e financeiro

MÉDIO

POR QUE IMPORTA

Antivírus tradicional reconhece ameaças já catalogadas; EDR observa comportamento e consegue conter um ataque em andamento, hoje uma exigência comum de seguradoras de cibersegurança.

COMO AVALIAR

Confirme se a proteção instalada nos computadores é antivírus tradicional ou uma solução de EDR com monitoramento ativo.

COMO RESOLVER

- Substitua o antivírus tradicional por uma solução de EDR nos computadores de maior exposição
- Garanta que os alertas gerados sejam efetivamente monitorados, não só coletados

13. Firmware de fechaduras eletrônicas e outros dispositivos de IoT mantido atualizado

MÉDIO

POR QUE IMPORTA

Vulnerabilidades como a que afetou milhões de fechaduras eletrônicas no mundo todo, permitindo abrir qualquer porta com um cartão clonado, só são corrigidas por atualização de firmware.

COMO AVALIAR

Pergunte ao fabricante da sua fechadura qual a versão de firmware instalada e se há atualizações de segurança pendentes.

COMO RESOLVER

- Acompanhe os boletins de segurança do fabricante das fechaduras e dispositivos de IoT
- Inclua a atualização de firmware como item recorrente de manutenção, não como evento único pós-instalação

03 Fornecedores e integrações

O hotel raramente é comprometido sozinho. O fornecedor com acesso mal controlado é um dos caminhos mais comuns.

14. Contratos de fornecedores com cláusulas claras de segurança e direito de auditoria

MÉDIO

POR QUE IMPORTA

Sem cláusulas específicas, o fornecedor não tem obrigação formal de segurança nem de responder a um incidente que afete o hotel.

COMO AVALIAR

Releia os contratos dos três fornecedores mais críticos (PMS, pagamento, Wi-Fi) e verifique se mencionam segurança da informação.

COMO RESOLVER

- Inclua cláusulas de segurança e direito de auditoria em contratos novos
- Negocie aditivos nos contratos vigentes mais críticos

15. Acesso de fornecedores a PMS e sistemas de fidelidade revisado periodicamente

RÁPIDO

POR QUE IMPORTA

Fornecedores mudam de equipe e de escopo de trabalho com o tempo, e o acesso concedido no início raramente é revisto depois.

COMO AVALIAR

Liste todos os fornecedores com acesso ativo hoje e confirme se ainda prestam o serviço que justificou o acesso.

COMO RESOLVER

- Revise o acesso de fornecedores trimestralmente
- Remova imediatamente o acesso de contratos encerrados

16. Integrações entre PMS, motor de reservas e canais de distribuição auditadas

MÉDIO

POR QUE IMPORTA

Cada integração é um canal de troca de dados, e integrações esquecidas ativas depois de uma troca de fornecedor são um risco comum e pouco visível.

COMO AVALIAR

Peça ao seu PMS a lista de integrações ativas e confirme se todas ainda estão em uso.

COMO RESOLVER

- Audite todas as integrações ativas e desative as que não são mais usadas
- Confirme que cada integração restante usa autenticação própria e criptografia

17. Prazos de notificação de incidente definidos em contrato com fornecedores críticos

MÉDIO

POR QUE IMPORTA

Se um fornecedor sofrer uma violação envolvendo dados dos seus hóspedes, você precisa saber a tempo de cumprir seus próprios prazos legais.

COMO AVALIAR

Verifique se os contratos dos fornecedores críticos definem um prazo objetivo para notificar o hotel em caso de incidente.

COMO RESOLVER

- Inclua prazo de notificação de incidente nos contratos com fornecedores críticos
- Alinhe esse prazo com o tempo que você precisa para cumprir suas próprias obrigações legais

18. Registro central de quais fornecedores têm acesso remoto aos sistemas do hotel

RÁPIDO

POR QUE IMPORTA

Sem esse registro, é praticamente impossível responder "quem mais tinha acesso" no meio de um incidente, exatamente quando a resposta rápida importa mais.

COMO AVALIAR

Tente montar essa lista agora: se levar mais que alguns minutos ou depender de perguntar a várias pessoas, o registro não existe de fato.

COMO RESOLVER

- Crie uma planilha ou registro único com fornecedor, sistema, data de concessão e motivo do acesso
- Atualize o registro a cada novo acesso concedido ou revogado

04 Conformidade e resposta a incidentes

O que fazer antes, e nos primeiros dias depois, de um incidente envolvendo dados de hóspedes.

19. Mapeamento atualizado de quais dados pessoais de hóspedes são coletados e onde ficam armazenados

MÉDIO

POR QUE IMPORTA

Sem esse mapeamento, é impossível responder a um pedido de titular ou avaliar o impacto real de um incidente com precisão.

COMO AVALIAR

Pergunte: hoje, alguém consegue listar em uma hora todos os sistemas que armazenam dados de hóspedes?

COMO RESOLVER

- Mapeie todos os sistemas que coletam ou armazenam dados pessoais de hóspedes
- Atualize o mapeamento sempre que um novo sistema ou integração entrar em operação

20. Plano de resposta a incidentes documentado e testado, não apenas escrito

PROJETO

POR QUE IMPORTA

Um plano nunca simulado costuma falhar exatamente no momento em que é mais necessário.

COMO AVALIAR

Pergunte quando foi o último exercício de simulação de incidente feito com a equipe que de fato vai executar o plano.

COMO RESOLVER

- Documente papéis, responsáveis e passos do plano de resposta a incidentes
- Faça pelo menos um exercício de mesa por ano com as pessoas envolvidas

21. Escopo do PCI DSS definido, com SAQ ou avaliação QSA em dia

PROJETO

POR QUE IMPORTA

Escolher o tipo de SAQ errado é, em si, uma falha de conformidade. O escopo mal definido geralmente aparece só quando já é tarde.

COMO AVALIAR

Confirme se alguém já validou formalmente qual SAQ se aplica à forma como o hotel processa pagamentos hoje.

COMO RESOLVER

- Identifique corretamente o SAQ aplicável com apoio de um QSA ou especialista
- Mantenha a validação em dia e revise sempre que o fluxo de pagamento mudar

22. Procedimento pronto para notificar a ANPD dentro do prazo de 3 dias úteis exigido pela Resolução CD/ANPD Nº 15/2024

MÉDIO

POR QUE IMPORTA

O prazo é curto e conta a partir da ciência do incidente. Ter um modelo pronto e um responsável definido de antemão é o que torna esse prazo viável.

COMO AVALIAR

Pergunte quem, hoje, saberia exatamente o que fazer nas primeiras horas após identificar um incidente com dados de hóspedes.

COMO RESOLVER

- Prepare um modelo de notificação à ANPD com antecedência
- Defina formalmente quem é o responsável por decidir e enviar a notificação

23. Treinamento de phishing atualizado para reconhecer ataques gerados por IA

RÁPIDO

POR QUE IMPORTA

E-mails de phishing gerados por IA têm menos erros de português e imitam melhor o tom de fornecedores e OTAs reais. Exemplos antigos e óbvios não preparam mais a equipe.

COMO AVALIAR

Verifique a data do último treinamento de phishing da equipe e se os exemplos usados ainda são realistas.

COMO RESOLVER

- Atualize o material de treinamento com exemplos recentes, incluindo golpes de reserva/OTA
- Repita o treinamento periodicamente, não como evento único de integração

24. Autenticação de e-mail (SPF, DKIM e DMARC) configurada no domínio do hotel

MÉDIO

POR QUE IMPORTA

Sem esses registros, é mais fácil forjar e-mails que parecem vir do seu domínio para enganar hóspedes ou fornecedores.

COMO AVALIAR

Use uma ferramenta gratuita de verificação de DMARC com o domínio do hotel e confira se os três registros estão configurados.

COMO RESOLVER

- Configure SPF, DKIM e DMARC no domínio do hotel
- Evolua o DMARC gradualmente até o modo de aplicação (reject), não apenas monitoramento

25. Monitoramento de segurança com cobertura 24/7, não apenas alertas que ninguém revisa

PROJETO

POR QUE IMPORTA

Um alerta gerado às 2h de um sábado só tem valor se alguém o vir e agir antes da segunda-feira.

COMO AVALIAR

Pergunte quem, na prática, monitora alertas de segurança fora do horário comercial, e o que acontece se ninguém vir.

COMO RESOLVER

- Avalie um serviço de MDR (deteção e resposta gerenciada) com cobertura 24/7
- Defina um processo claro de escalonamento para alertas críticos fora do horário comercial

PRÓXIMO PASSO

Quer uma avaliação completa da sua operação, não só o checklist?

A HotelTI, especialista em tecnologia hoteleira, ajuda hotéis e redes a identificar os controles ausentes na sua operação e a resolvê-los sem parar a rotina do hotel.

Site: hotelti.com.br

E-mail: info@hotelti.com.br

Cibersegurança hoteleira: hotelti.com.br/ciberseguranca

Este guia tem caráter informativo geral e não substitui uma avaliação técnica da sua operação específica. Os prazos legais citados refletem a legislação vigente na data de publicação; consulte sempre a fonte oficial mais recente. © 2026 HotelTI.