innovtourism

Guia Prático

Boas Práticas para a Cibersegurança no Turismo

Célia Rafael, João Costa, João Tiago Silva, Paulo Almeida

POLITÉCNICO DE LEIRIA
CiTUR Centro de Investigação, Desenvolvimento e Inovação em Turismo
PRR Plano de Recuperação e Resiliência
REPÚBLICA PORTUGUESA
Financiado pela União Europeia NextGenerationEU

Ficha Técnica

Título Guia Prático Boas Práticas para a Cibersegurança no Turismo

Equipa editorial

Paulo Almeida
ORCID: 0000-0002-4797-2128
CiTUR – Centro de Investigação Desenvolvimento e Inovação para o Turismo, Instituto Politécnico de Leiria

Célia Rafael
ORCID: 0000-0001-7388-129X
CiTUR – Centro de Investigação Desenvolvimento e Inovação para o Turismo, Instituto Politécnico de Leiria

João Costa
ORCID: 0000-0003-2359-0296
CiTUR – Centro de Investigação Desenvolvimento e Inovação para o Turismo, Instituto Politécnico de Leiria

João Tiago Silva
ORCID: 0009-0003-8784-6868
CiTUR – Centro de Investigação Desenvolvimento e Inovação para o Turismo, Instituto Politécnico de Leiria

Autores

Sérgio Cláudio Fontes
ORCID: 0000-0003-3264-4997
Escola Superior de Turismo e Tecnologia do Mar, Instituto Politécnico de Leiria

Alexandru Bertea,
LCG Consulting

Ronen Lago
LCG Consulting

Eran Fine
LCG Consulting

Jorge Páramos
LCG Consulting

Edição Instituto Politécnico de Leiria

ISBN 978-989-96501-6-9

DOI https://doi.org/10.25766/726f-cb14

Data Junho 2026

Para informação complementar https://innovtourism.pt/

Projeto DIH InnovTourism financiado por PRR Plano de Recuperação e Resiliência, Instituto Politécnico de Leiria

Guia Prático

Boas Práticas para a Cibersegurança no Turismo

Célia Rafael, João Costa, João Tiago Silva, Paulo Almeida

Equipa editorial

Célia Rafael, João Costa, João Tiago Silva e Paulo Almeida
CiTUR – Centro de Investigação Desenvolvimento e Inovação para o Turismo, Instituto Politécnico de Leiria

Autores

Sérgio Cláudio Fontes
Escola Superior de Turismo e Tecnologia do Mar, Instituto Politécnico de Leiria

Alexandru Bertea, Ronen Lago, Eran Fine e Jorge Páramos
Empresa LCG

Financiado pela União Europeia NextGenerationEU

Parceiro

InnovTourism

O InnovTourism, polo de inovação digital para o Turismo, é uma iniciativa estratégica orientada para acelerar a transformação digital do setor, promovendo a inovação, a competitividade e a sustentabilidade das empresas e destinos turísticos. O projeto apoia PME, start-ups e entidades públicas do setor turístico na adoção de soluções digitais, nomeadamente nas áreas da inteligência artificial, análise de dados, capacitação e desenvolvimento de serviços inovadores.

O Instituto Politécnico de Leiria assume um papel relevante neste ecossistema, através da Escola Superior de Turismo e Tecnologia do Mar (ESTM) e do CiTUR – Centro de Investigação, Desenvolvimento e Inovação em Turismo, contribuindo com conhecimento científico, investigação aplicada, formação especializada e forte ligação ao território.

CiTUR

O CiTUR Leiria, polo de referência da rede CiTUR, dedica-se ao avanço do conhecimento científico na área do turismo. Alinhado com o compromisso do Politécnico de Leiria com a investigação e a inovação, reúne uma equipa multidisciplinar de 70 investigadores, a maioria doutorados.

O centro aposta na investigação aplicada, na produção científica de elevado impacto e na colaboração internacional, apoiando-se em infraestruturas modernas que possibilitam a realização de estudos experimentais e o desenvolvimento de parcerias à escala global.

As suas instalações incluem laboratórios especializados nas áreas do turismo, multimédia e neurociência, bem como espaços destinados à formação profissional e à promoção do turismo sustentável.

Ao fomentar a colaboração e reforçar as parcerias de investigação, o CiTUR Leiria contribui para a resposta aos desafios atuais e futuros do setor do turismo.

Introdução

O presente documento organiza, em formato de guia, os conteúdos-base disponibilizados no âmbito do projeto InnovTourism. A estrutura foi definida para que a Parte I funcione como enquadramento introdutório e conceptual, preparando a leitura da Parte II, de natureza mais setorial e aplicada ao contexto da hotelaria e da inteligência artificial.

Parte I - Fundamentos de cibersegurança e boas práticas. Autoria: Sérgio Cláudio Fontes, Escola Superior de Turismo e Tecnologia do Mar do Politécnico de Leiria.

Parte II - Ciber-segurança na indústria hoteleira: ameaças e defesa na era da IA. Autoria: Alexandru Bertea, Ronen Lago, Eran Fine e Jorge Páramos, LCG Consulting.

Na presente versão, a Parte I foi expandida em registo editorial contínuo, incorporando frameworks de referência e elementos visuais de apoio à leitura. A Parte II mantém o texto-base da LCG Consulting, de modo a salvaguardar a integridade do conteúdo original.

Índice

Parte I

Fundamentos de cibersegurança e boas práticas 10

Parte II

Ciber-segurança na indústria hoteleira: ameaças e defesa na era da IA 24

Parte I

Fundamentos de cibersegurança e boas práticas

Autoria:

Sérgio Cláudio Fontes

Escola Superior de Turismo e Tecnologia do Mar do Politécnico de Leiria.

Esta primeira parte adapta e desenvolve o conteúdo do webinar para um formato de leitura contínua, com o objetivo de oferecer um enquadramento claro, rigoroso e operacional para profissionais e organizações do turismo.

1. Cibersegurança, confiança e continuidade no turismo

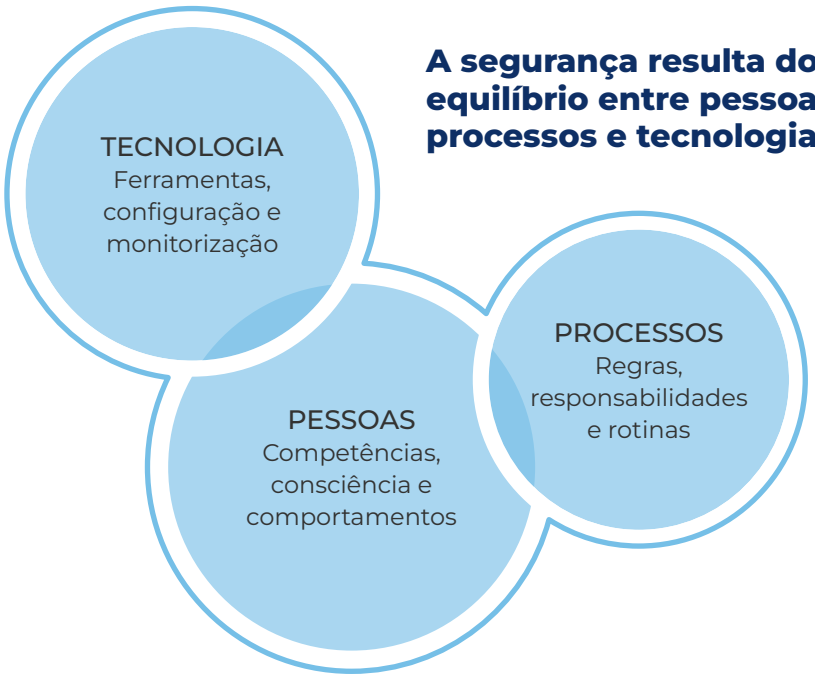
A cibersegurança deixou de ser um tema circunscrito ao domínio técnico para passar a integrar o núcleo da gestão organizacional. No turismo, esta realidade é particularmente evidente: hotéis, restaurantes, agências de viagens, plataformas de reservas e entidades de animação dependem de sistemas digitais para vender, comunicar, processar pagamentos, gerir operações e prestar serviço ao cliente. Sempre que um desses sistemas falha, não está apenas em causa um problema informático; pode estar em causa a continuidade da atividade, a confiança do cliente e a reputação acumulada pela organização.

A especificidade do setor agrava esta exposição. O turismo trabalha com fluxos intensivos de dados, muitos deles pessoais e financeiros; depende de redes de parceiros e plataformas externas; opera frequentemente vinte e quatro horas por dia; e mantém equipas heterogéneas, com diferentes níveis de literacia digital. Por isso, a cibersegurança deve ser compreendida como um fator de qualidade do serviço e de resiliência do negócio. Proteger sistemas e dados significa, em última instância, proteger a experiência do hóspede, a capacidade de resposta da organização e a credibilidade da marca.

A mensagem essencial é simples: segurança não se resume a instalar ferramentas. Resulta da articulação entre pessoas, processos e tecnologia. Quando um destes três pilares falha, a organização perde consistência; quando os três se reforçam mutuamente, a postura de segurança torna-se mais robusta e sustentável.

Figura 1

A SEGURANÇA DA INFORMAÇÃO ASSENTA NO EQUILÍBRIO ENTRE PESSOAS, PROCESSOS E TECNOLOGIA.



BOA PRÁTICA

Atribua a um responsável a coordenação das questões de segurança digital, mesmo que não exista uma equipa dedicada.

ERRO FREQUENTE

Considerar a cibersegurança apenas um assunto técnico e não uma responsabilidade da gestão.

RECOMENDAÇÃO

Inclua a segurança digital nas reuniões de gestão e nos processos de decisão da empresa.

CHECKLIST

- [ ] Existe um responsável pela segurança digital?
- [ ] A direção acompanha os riscos digitais?
- [ ] Existem regras básicas de utilização dos sistemas?
- [ ] Os colaboradores conhecem essas regras?

2. O que está em causa: ativos, informação e risco

Antes de discutir ameaças e controlos, importa perceber o que exatamente se pretende proteger. Numa organização turística, os ativos críticos incluem sistemas de reservas, *websites*, contas de *email*, dados de hóspedes e clientes, plataformas de pagamento, infraestruturas de rede, dispositivos móveis, equipamentos de ponto de venda, credenciais de acesso e conhecimento operacional. Em muitos casos, estes ativos não são detidos exclusivamente pela organização; estão distribuídos por serviços *cloud*, fornecedores tecnológicos, OTAs, *gateways* de pagamento ou aplicações SaaS. Este facto aumenta a superfície de exposição e obriga a uma leitura alargada do risco.

A segurança da informação pode ser lida através de três objetivos clássicos: confidencialidade, integridade e disponibilidade. A confidencialidade protege o acesso indevido a informação sensível; a integridade assegura que os dados e registos se mantêm corretos e fiéis; e a disponibilidade garante que sistemas e serviços podem ser utilizados quando necessários. No turismo, estes três objetivos têm tradução muito concreta. Uma fuga de dados compromete a confidencialidade; uma alteração indevida de tarifas, reservas ou faturas compromete a integridade; e uma indisponibilidade do motor de reservas ou do PMS compromete a disponibilidade, com impacto direto na operação e na receita.

É também importante distinguir ameaça, vulnerabilidade e impacto. A ameaça corresponde ao agente ou evento potencialmente danoso; a vulnerabilidade é a fragilidade que pode ser explorada; e o impacto traduz as consequências no negócio. Esta distinção permite às organizações passar de uma lógica reativa para uma lógica de gestão de risco: identificar onde estão as fragilidades mais relevantes, perceber como podem ser exploradas e priorizar medidas de mitigação de acordo com o efeito provável na operação.

BOA PRÁTICA

Mantenha um inventário atualizado dos sistemas, aplicações, equipamentos e dados críticos.

ERRO FREQUENTE

Desconhecer todos os dispositivos e aplicações ligados à rede da organização.

RECOMENDAÇÃO

Classifique os ativos de acordo com a sua importância para a operação turística.

CHECKLIST

- [ ] Existe inventário de equipamentos?
- [ ] Os sistemas críticos estão identificados?
- [ ] Os responsáveis pelos ativos são conhecidos?
- [ ] O inventário é atualizado regularmente?

3. Panorama de ameaças no setor do turismo

Entre as ameaças mais frequentes continuam a destacar-se o *phishing*, o *ransomware*, o roubo de credenciais, a engenharia social, as falhas de configuração, o abuso de privilégios e os incidentes originados em fornecedores ou integrações. Em muitos casos, o ponto de entrada não é sofisticado: um *link* clicado sem validação, uma *password* reutilizada, um dispositivo desatualizado, uma conta esquecida ou um colaborador pressionado por urgência aparente. A relevância da cibersegurança está precisamente no facto de pequenos erros, acumulados, poderem produzir consequências desproporcionadas.

O setor do turismo apresenta vulnerabilidades próprias. A pressão comercial para responder rapidamente, a sazonalidade, a rotatividade de equipas, o recurso a colaboradores temporários e a dependência de serviços externos podem reduzir o espaço para rotinas formais de controlo. Ao mesmo tempo, os atacantes sabem que organizações orientadas para o serviço tendem a privilegiar rapidez e conveniência, o que favorece esquemas de personificação, pedidos urgentes de pagamento, falsas reservas, alteração fraudulenta de IBAN ou mensagens que simulam parceiros legítimos.

Deve ainda notar-se que muitas ameaças já não se apresentam apenas sob a forma clássica de *malware* ou fraude direta. Hoje coexistem campanhas altamente personalizadas, tentativas de exploração de aplicações *web*, abuso de APIs, acessos indevidos via parceiros e uso malicioso de ferramentas automatizadas. Esta evolução torna ainda mais necessária uma abordagem estruturada e não apenas pontual à segurança.

4. Frameworks para organizar a segurança

Para evitar que a cibersegurança seja tratada como um conjunto disperso de boas intenções, é útil recorrer a frameworks de referência. Um dos quadros mais claros e adaptáveis para PME é o NIST *Cybersecurity Framework*, que organiza a segurança em cinco funções: identificar, proteger, detetar, responder e recuperar. A utilidade deste modelo está em transformar a segurança num ciclo de gestão e melhoria contínua, em vez de uma sucessão de medidas isoladas.

Identificar implica conhecer ativos, dependências, processos críticos e riscos. Proteger significa implementar controlos proporcionais: autenticação forte, gestão de acessos, atualização de sistemas, formação e segmentação. Detetar exige visibilidade: *logs*, alertas, revisão de eventos e capacidade mínima de monitorização. Responder implica saber quem decide, quem comunica e que passos são dados quando ocorre um incidente. Recuperar significa restaurar serviços, aprender com o sucedido e atualizar práticas e procedimentos.

Esta lógica é especialmente adequada ao turismo porque permite transformar a segurança em linguagem de gestão. Um gestor não precisa de dominar todos os detalhes técnicos para perceber se a organização conhece os seus ativos críticos, se protege os acessos, se consegue detetar comportamentos anómalos e se tem um plano claro para recuperar em caso de incidente.

BOA PRÁTICA

Promova ações regulares de sensibilização sobre phishing e engenharia social.

ERRO FREQUENTE

Abrir anexos ou clicar em links sem validar a origem da mensagem.

RECOMENDAÇÃO

Crie um procedimento simples para reportar emails suspeitos.

CHECKLIST

- [ ] Os colaboradores sabem identificar phishing?
- [ ] Existe canal para reportar incidentes?
- [ ] São realizadas ações de sensibilização?
- [ ] Existem exemplos de fraudes conhecidos pela equipa?

Figura 2

O NIST CSF OFERECE UMA ESTRUTURA CLARA PARA ORGANIZAR A CIBERSEGURANÇA NAS ORGANIZAÇÕES

Framework de referência para organizar a cibersegurança nas PME do turismo

PRIORIDADES OPERACIONAIS PARA PME DO TURISMO

HORIZONTE	OBJETIVO	EXEMPLOS DE AÇÃO
Imediato	Reduzir exposição básica	Ativar MFA nas contas críticas, rever passwords, atualizar sistemas e confirmar backups existentes.
Curto prazo	Organizar controlo interno	Mapear acessos, formalizar responsabilidades, definir procedimento de reporte e validar parceiros críticos.
Médio prazo	Ganhar visibilidade e resiliência	Melhorar monitorização, testar recuperação, realizar exercícios de incidente e rever políticas de retenção e proteção de dados.

BOA PRÁTICA

Defina políticas simples de segurança adaptadas à dimensão da empresa.

ERRO FREQUENTE

Depender apenas do conhecimento informal dos colaboradores.

RECOMENDAÇÃO

Documente os procedimentos essenciais relacionados com segurança digital.

CHECKLIST

- [ ] Existe política de palavras-passe?
- [ ] Existem regras para acesso remoto?
- [ ] Existem procedimentos documentados?
- [ ] Os colaboradores conhecem essas regras?

5. Aplicações, websites e o quadro OWASP Top 10

Uma parte importante do risco digital atual reside nas aplicações e serviços *web* que suportam a operação das organizações. *Websites* institucionais, formulários de contacto, motores de reserva, backoffices, extranets de parceiros e integrações por API são hoje peças centrais da cadeia de valor no turismo. Para compreender as fragilidades recorrentes neste domínio, o OWASP Top 10 oferece um quadro de referência particularmente útil.

O valor do OWASP não está apenas em nomear vulnerabilidades técnicas; está em tornar visíveis padrões de falha que têm consequências de negócio. Problemas de controlo de acessos podem expor reservas ou dados de clientes a utilizadores indevidos. Más configurações de segurança podem deixar serviços abertos com definições por omissão. Falhas de autenticação podem permitir o comprometimento de contas internas. Problemas criptográficos podem expor dados sensíveis. Falhas na cadeia de fornecimento de *software* tornam-se relevantes quando a organização depende de *plugins*, módulos, bibliotecas ou serviços de terceiros sem avaliação adequada.

Para as organizações do turismo, a principal lição é esta: as vulnerabilidades de aplicação não são um tema abstrato reservado aos programadores. Afetam diretamente a confiança do cliente, a proteção de dados, a continuidade do serviço e a exposição regulatória. Uma boa prática passa por exigir testes de segurança, revisão periódica de configurações, atualização de componentes, segregação de acessos administrativos e validação técnica de fornecedores que desenvolvem ou mantêm sistemas críticos.

Em termos pedagógicos, o OWASP ajuda também a recentrar a atenção na prevenção estrutural. Em vez de perguntar apenas se a organização tem antivírus, importa perguntar se os seus canais digitais foram desenhados e mantidos com critérios de segurança suficientes para suportar o negócio.

BOA PRÁTICA

Mantenha CMS, plugins e aplicações sempre atualizados.

ERRO FREQUENTE

Utilizar plugins desatualizados ou sem manutenção.

RECOMENDAÇÃO

Reveja trimestralmente os acessos administrativos do website.

CHECKLIST

- [ ] O website utiliza HTTPS?
- [ ] Os plugins estão atualizados?
- [ ] Existem cópias de segurança?
- [ ] Os acessos administrativos foram revistos?

6. Identidade, acessos e boas práticas dos utilizadores

A experiência demonstra que uma parte significativa dos incidentes começa com credenciais comprometidas ou com comportamentos inseguros de utilizadores. Por isso, a gestão de identidades e acessos deve ser vista como um dos eixos centrais da segurança. Utilizar *passwords* longas e únicas, apoiadas por um gestor de *passwords* sempre que possível, continua a ser uma prática essencial. A autenticação multifator deve ser ativada nas contas mais críticas: *email* institucional, sistemas de reservas, plataformas de faturação, acessos administrativos e serviços *cloud*.

No entanto, a segurança não depende apenas da robustez técnica das credenciais. Depende igualmente da capacidade dos utilizadores para reconhecer sinais de fraude. Mensagens com urgência artificial, pedidos de alteração de dados bancários, anexos inesperados, *links* abreviados ou domínios ligeiramente alterados são indicadores clássicos de risco. Numa cultura de segurança madura, os colaboradores sentem-se autorizados a interromper, confirmar e reportar sem receio de parecer excessivamente cautelosos.

Esta dimensão cultural é crucial no turismo. Em ambientes de *front office*, reservas, operações ou apoio ao cliente, a pressão para responder depressa é grande. Precisamente por isso, devem existir regras simples, conhecidas e repetidas: confirmar pedidos sensíveis por um segundo canal; não partilhar acessos; bloquear sessão quando se abandona o posto; evitar redes *Wi-Fi* inseguras para operações críticas; e restringir a partilha de ficheiros e dados apenas ao estritamente necessário.

BOA PRÁTICA

Implemente autenticação multifator (MFA) em contas críticas.

ERRO FREQUENTE

Partilhar contas entre vários colaboradores.

RECOMENDAÇÃO

Utilize um gestor de palavras-passe para armazenar credenciais.

CHECKLIST

- [ ] MFA ativo nas contas críticas?
- [ ] Contas individuais para cada colaborador?
- [ ] Palavras-passe fortes?
- [ ] Contas inativas removidas?

7. Administração, monitorização e gestão operacional da segurança

As boas práticas individuais só se tornam efetivas quando enquadradas por uma gestão operacional consistente. Isso implica políticas internas proporcionais, atribuição clara de responsabilidades, revisão periódica de acessos e algum nível de monitorização. O princípio do menor privilégio é aqui determinante: cada colaborador deve ter acesso apenas ao que é necessário para a sua função e durante o tempo em que dele necessita. Contas antigas, perfis genéricos ou permissões acumuladas ao longo do tempo constituem fontes clássicas de risco.

A monitorização não tem de começar por soluções complexas. O mais importante é garantir visibilidade mínima sobre eventos relevantes: tentativas de *login* falhadas, alterações de privilégios, acessos administrativos, execução de tarefas críticas, falhas anómalas de serviços e movimentos de dados não usuais. Sem registo e sem capacidade de observação, a organização fica dependente do acaso para descobrir que algo está a correr mal.

Outra dimensão frequentemente subestimada é a gestão do ciclo de vida dos colaboradores e prestadores. A entrada, mudança de função e saída de pessoas devem desencadear revisões de acessos. Nas PME, onde as equipas são mais pequenas e os papéis menos estanques, esta disciplina é ainda mais importante. Segurança operacional significa previsibilidade, rastreabilidade e capacidade de decisão informada.

BOA PRÁTICA

Ative registos de eventos (logs) nos sistemas mais críticos.

ERRO FREQUENTE

Só investigar problemas depois de ocorrer um incidente.

RECOMENDAÇÃO

Monitorize acessos, tentativas falhadas e atividades anómalas.

CHECKLIST

- [ ] Os logs estão ativos?
- [ ] Os eventos são analisados?
- [ ] Existem alertas automáticos?
- [ ] Há monitorização dos sistemas críticos?

8. Backup, recuperação, resposta a incidentes e continuidade

Uma organização verdadeiramente resiliente não se limita a tentar evitar incidentes; prepara-se também para recuperar quando eles acontecem. Neste domínio, o *backup* é um elemento essencial, mas deve ser entendido como parte de uma estratégia mais ampla de recuperação. A regra 3-2-1 continua a oferecer uma referência prática e facilmente comunicável: três cópias dos dados, em dois suportes ou meios diferentes, com uma cópia fora do ambiente principal. O objetivo não é apenas armazenar cópias; é garantir que existe capacidade real de restauro em tempo útil.

Por isso, *backup* sem teste é uma falsa sensação de segurança. É necessário saber se as cópias abrangem os sistemas realmente críticos, com que frequência são atualizadas, quanto tempo demora a recuperação e quem tem autoridade para desencadear esse processo. No turismo, onde a indisponibilidade de reservas, comunicações, faturação ou escalas afeta de imediato o serviço, os tempos de recuperação devem ser compatíveis com a realidade operacional.

A resposta a incidentes deve ser igualmente preparada com antecedência. Quando ocorre um problema, importa conter, comunicar, preservar evidências e decidir. Isolar sistemas afetados, registar logs e mensagens relevantes, ativar contactos internos e manter clareza sobre responsabilidades reduz a desorganização típica dos momentos de crise.

A continuidade de negócio entra precisamente aqui: como continuar a operar, mesmo que parcialmente, enquanto se avalia e mitiga o incidente? As organizações mais maduras fazem exercícios de mesa e simulações simples para testar decisões críticas. Este tipo de prática é valioso porque transforma o plano de resposta de um documento estático numa competência organizacional efetiva.

Figura 3

A REGRA 3-2-1 AJUDA A ESTRUTURAR A RECUPERAÇÃO E A REDUZIR O IMPACTO DE PERDA OU CORRUPÇÃO DE DADOS

Regra 3-2-1 para resiliência e recuperação

BOA PRÁTICA

Mantenha cópias de segurança em local separado da rede principal.

ERRO FREQUENTE

Assumir que o backup funciona sem o testar.

RECOMENDAÇÃO

Realize testes periódicos de recuperação de informação.

CHECKLIST

- [ ] Backups automáticos?
- [ ] Backups fora da rede principal?
- [ ] Testes de recuperação realizados?
- [ ] Plano de continuidade definido?

9. Governação, fornecedores, ISO 27001 e RGPD

À medida que a maturidade aumenta, a cibersegurança passa a ser enquadrada por práticas de governação e conformidade. A ISO 27001 é relevante porque propõe uma abordagem sistemática baseada em risco, melhoria contínua e controlo organizado da segurança da informação. Não se trata apenas de certificação; trata-se de uma forma estruturada de pensar responsabilidades, ativos, controlos, incidentes, fornecedores e revisão periódica.

No mesmo plano, o RGPD recorda que a proteção de dados pessoais é inseparável da segurança. Organizações turísticas tratam diariamente dados de identificação, contactos, preferências, transações e, em certos contextos, informação mais sensível. A conformidade exige conhecer os dados tratados, os fundamentos para o seu tratamento, os períodos de retenção, os acessos concedidos e as medidas técnicas e organizativas adotadas para os proteger.

A relação com fornecedores merece destaque particular. Grande parte da infraestrutura digital do turismo depende de terceiros: OTAs, PMS, *channel managers*, soluções de pagamentos, *marketing platforms*, IoT, serviços *cloud* e parceiros tecnológicos especializados. Cada ligação desta cadeia pode aumentar o risco. Assim, selecionar fornecedores, exigir garantias mínimas de segurança, definir acessos de forma restrita e rever integrações críticas não é um detalhe contratual; é parte integrante da postura de segurança da organização.

BOA PRÁTICA

Avalie os requisitos de segurança dos fornecedores antes da contratação.

ERRO FREQUENTE

Confiar totalmente nos fornecedores sem verificar os seus controlos de segurança.

RECOMENDAÇÃO

Inclua cláusulas de segurança e proteção de dados nos contratos.

CHECKLIST

- [ ] Os fornecedores críticos estão identificados?
- [ ] Existem cláusulas de segurança?
- [ ] Existe processo de avaliação?
- [ ] Há procedimentos para notificação de incidentes?

10. Síntese e ponte para a Parte II

Em síntese, a cibersegurança no turismo assenta em fundamentos claros: compreender os ativos críticos, gerir risco, envolver pessoas, organizar processos, proteger acessos, monitorizar, preparar a recuperação e enquadrar tudo isto numa lógica de governação. A ideia central não mudou: prevenir continua a ser mais barato e mais eficaz do que reagir; e a segurança continua a ser responsabilidade de todos.

Ao mesmo tempo, o contexto em que estes princípios são aplicados está a mudar rapidamente. A integração crescente de inteligência artificial, automação, sistemas conectados e decisões algorítmicas introduz novos cenários de risco, novas vulnerabilidades e novas exigências de supervisão. É precisamente nesse ponto que a análise setorial da LCG Consulting ganha relevância. A Parte II aprofunda a forma como estas transformações se manifestam no setor hoteleiro, preservando o seu conteúdo-base e ampliando a leitura deste guia para a era da IA.

Parte II

Ciber-segurança na indústria hoteleira: ameaças e defesa na era da IA

Autoria:

Alexandru Bertea

Ronen Lago

Eran Fine

Jorge Páramos

LCG Consulting

Nota editorial: o conteúdo-base da LCG Consulting é apresentado em seguida, preservando a integridade substantiva do texto original.


IOT
****
IA

Introdução

A indústria hoteleira está a entrar numa era em que a inteligência artificial (IA) e a automação estão a transformar as operações e a experiência do cliente – de algoritmos de preços dinâmicos a *chatbots* de atendimento – enquanto simultaneamente introduzem riscos cibernéticos sem precedentes. *Hackers* e criminosos estão a usar a IA para lançar ataques cibernéticos sofisticados em larga escala, aproveitando a vasta quantidade de dados sensíveis e sistemas interligados que caracterizam a hotelaria. Em paralelo, os sistemas autónomos de IA nos hotéis tomam decisões sem intervenção humana direta (sobre tarifas, reservas, interações com clientes), podendo falhar ou ser manipulados de formas inesperadas se não forem adequadamente supervisionados.

Embora recente, esta tecnologia já deu origem a incidentes de grande impacto – desde a polémica do sistema de preços dinâmicos da Delta Air Lines até ao fiasco do *chatbot* da Air Canada – ilustram as consequências reais quando algo corre mal. Estatísticas recentes reforçam a urgência de adaptar as estratégias de ciber-segurança dos hotéis a este novo paradigma dominado pela IA: como exemplo, desde 2022 houve um aumento de mais de 4000% nas tentativas de *phishing* assistidas por IA dirigidas a viajantes, e estudos estimam que 73% dos hotéis sofreram uma violação de dados em 2024.

Estes ataques não se limitam a causar prejuízos financeiros diretos (roubo de fundos, fraude, pagamentos de resgate); provocam também sanções regulatórias (por violações de proteção de dados, como o RGPD) e danos reputacionais num setor que vive da confiança do cliente. Como o negócio hoteleiro "vende" segurança e fiabilidade aos hóspedes, uma única falha de segurança pode minar a confiança construída ao longo de anos.

As estatísticas citadas destacam que tanto atacantes como vítimas dispõem agora de ferramentas de IA avançada. Nas secções a seguir, examinamos como a IA está a redefinir as ameaças cibernéticas na hotelaria, com exemplos concretos de falhas e ataques reais, identificamos as vulnerabilidades específicas dos sistemas hoteleiros e apresentamos um conjunto de recomendações práticas – incluindo auditorias de IA, conformidade regulatória, supervisão humana, verificação de identidade, *red teaming* e segurança da cadeia de fornecedores – para orientar os gestores de TI hoteleiros na fortalecimento das defesas e na proteção das operações e da confiança dos hóspedes nesta nova era.

1. Panorama em Evolução das Ameaças: Ataques Impulsionados por IA

O panorama de ameaças cibernéticas no setor do turismo evoluiu drasticamente nos últimos anos devido à rápida evolução da IA. Atacantes maliciosos utilizam agora a IA para automatizar e potenciar os seus ataques, aumentando a sua escala e sofisticação. Uma linha temporal da evolução do *phishing* e de outras técnicas de ataque ilustra esta transformação:

O que impulsiona esta mudança? Em suma, a IA tornou-se um multiplicador de força para os criminosos cibernéticos. Modelos de IA conseguem gerar *phishing* personalizado, *malware* mutante e até vozes *deepfake* em meros segundos – tarefas que antes demoravam dias a *hackers* humanos. Como resultado, assistimos a um aumento exponencial tanto no volume como na eficácia dos ataques contra empresas de viagens e hotéis. Desde 2022, por exemplo, registou-se um crescimento de mais de 4000% nas tentativas de *phishing* assistidas por IA. E esta ameaça não é teórica: ataques cibernéticos baseados em IA estão a ocorrer, neste momento, em hotéis e agências de viagem em todo o mundo.

O setor do turismo e hotelaria é particularmente visado por várias razões. Em primeiro lugar, os hotéis lidam com dados altamente sensíveis e valiosos – informação pessoal e financeira de milhões de hóspedes (números de passaporte, detalhes de cartões de crédito, contactos, preferências de viagem) – convertendo-se em alvos atrativos para roubo de identidade e fraude financeira. Em segundo lugar, a operação hoteleira depende de uma tecnologia fortemente interconectada: sistemas de reservas online, gestores de canais, portais de *booking*, *gateways* de pagamento, *apps* de fidelização e outros serviços de terceiros (agências de viagem online, sistemas de gestão de propriedades). Tudo isto está ligado por APIs, partilhando dados constantemente. Uma falha de segurança em qualquer ponto desta cadeia pode ser explorada e permitir acesso indevido aos sistemas do hotel.

Além disso, as campanhas de ataque suportadas por IA são extremamente velozes e adaptáveis, escapando com facilidade aos mecanismos tradicionais de defesa. Se os ataques convencionais muitas vezes podiam ser detetados por padrões repetitivos ou por assinaturas conhecidas, o *malware* e *phishing* atuais não só são altamente personalizados, como mudam de forma para evitar a deteção. Com efeito, o *malware* polimórfico alimentado por IA reescreve repetidamente o seu próprio código, levando as taxas de deteção a caírem de ~90% (para *malware* tradicional) para menos de 15% nas variantes geradas por IA. Alguns códigos maliciosos aprendem mesmo com as tentativas de bloqueio: cada vez que são detetados, regressam mais furtivamente, criando uma espécie de ciclo evolutivo de *software* malicioso.

Esta convergência de fatores significa que uma violação não envolve apenas perdas financeiras diretas ou interrupções operacionais, mas pode também desencadear sanções regulatórias (por incumprimento do RGPD, PCI-DSS, etc.) e danos à reputação da marca. Importa relembrar que a indústria hoteleira vende essencialmente segurança e confiança aos seus clientes. Um ciberincidente grave – como a divulgação de dados de hóspedes ou um ataque que cause indisponibilidade prolongada de serviços – pode afastar os clientes e corroer a credibilidade de uma marca outrora respeitável.

Por este motivo, a ciber-segurança alimentada por IA deixou de ser apenas uma preocupação de "*backoffice*" para se tornar um assunto estratégico para a gestão de topo. Nas próximas secções, exploraremos as implicações desta nova realidade para as operações hoteleiras.

2. Automação por IA nas Operações Hoteleiras: Oportunidades e Riscos

Os hotéis têm adotado amplamente a IA para melhorar a eficiência e o serviço ao cliente – mas estas mesmas tecnologias podem introduzir novas vulnerabilidades se não forem geridas cuidadosamente. Abaixo, examinamos como a automação suportada por IA e sistemas "agentes" (IA com autonomia de decisão) estão a transformar as operações hoteleiras e porque é que a supervisão humana continua a ser imprescindível.

IA NAS OPERAÇÕES HOTELEIRAS. EXEMPLOS DE APLICAÇÕES DE IA EM AMBIENTES HOTELEIROS INCLUEM:

1. **Preços Dinâmicos & *Revenue Management*:** Muitos hotéis utilizam modelos de *machine learning* para ajustar, em tempo real, os preços dos quartos com base na procura, concorrência, segmentação de clientes e outros fatores. Se bem que esta tarifação dinâmica possa maximizar receitas, existem riscos de comportamento inesperado ou perceções de injustiça.

2. ***Chatbots* e Assistentes Virtuais:** Um número crescente de hotéis implementa *chatbots* em *websites* e aplicações de mensagens para lidar com reservas, pedidos de informação e serviços de *concierge* digital. Estas AIs de atendimento ao cliente aliviam as equipas humanas e oferecem respostas imediatas 24/7. Contudo, sem o devido controlo, *chatbots* podem enganar ou frustrar os hóspedes.
   Esta situação serve de alerta: os hotéis devem assegurar que os seus *chatbots* são exaustivamente testados e periodicamente monitorizados por humanos, de forma a evitar alucinações da IA que induzam clientes em erro e resultem em litígios ou danos reputacionais.

3. **Sistemas de Recomendação & Vendas Assistidas:** Plataformas de reservas e OTAs (agências de viagens *online*) recorrem a IA para personalizar sugestões – indicando hotéis, upgrades ou serviços suplementares com base no perfil do cliente. Sem supervisão, estes algoritmos podem desenvolver viés ou estratégias de otimização contrárias à ética e aos interesses de negócio. Assim, um sistema não auditado pode decidir mostrar tarifas mais elevadas a clientes específicos com base no seu histórico ou dispositivo (um padrão observado em alguns sítios de viagens). Tais práticas de discriminação oculta não só *afetam negativamente a experiência dos hóspedes*, como podem levar a ações judiciais e sanções se violarem normas de proteção ao consumidor.
   Da perspetiva do hotel, os sistemas algorítmicos das plataformas parceiras também representam risco: se o motor de recomendação de uma OTA "desfavorece" injustamente o seu hotel – por razões desconhecidas devido à natureza *black-box* do algoritmo – as suas vendas podem cair sem que perceba o porquê. Auditar e exigir transparência nos sistemas de recomendação tornou-se, portanto, um imperativo para garantir práticas de negócio justas e defender a reputação.

4. **Operações Internas e IoT Inteligentes:** Os hotéis adotam IA em diversas áreas operacionais: controlo energético inteligente, *smart rooms*, sistemas de *check-in* automatizado com reconhecimento facial, robôs de entrega de serviço de quartos, entre outros. A nova fronteira são os sistemas agentes: IAs com autonomia para tomar medidas sem validação humana imediata. De facto, observa-se em 2026 uma transição "de ferramentas para agentes", onde *softwares* de IA podem executar tarefas em tempo real, como aprovar transações, reatribuir quartos ou reordenar *stocks*, sem intervenção humana: tal acarreta uma agilidade operacional nunca antes vista, mas também o risco da "autonomia descontrolada". Diferente de algoritmos estáticos, estes agentes continuam a aprender e a alterar o seu comportamento após entrarem em produção, podendo tomar decisões inesperadas.

Sem um contrapeso humano (e.g., um gerente a monitorizar ou validar ações críticas), um agente mal configurado pode causar danos antes que alguém se aperceba. Por exemplo, um assistente de reservas totalmente autónomo poderia, em resposta a um *input* malicioso ou a um erro de *software*, cancelar uma série de reservas legítimas ou emitir reembolsos indevidos. Para prevenir tais cenários, estratégias de *human-in-the-loop* (HITL) – que garantem que um humano valida ou acompanha as decisões mais sensíveis da IA – são essenciais para evitar que a automação se torne sinónimo de perda de controlo.

Em suma, a hotelaria combina um contexto de alta exposição a ataques com dependência crescente de sistemas de IA críticos, tornando os riscos especialmente altos. As operações em tempo real dos hotéis significam que erros mínimos podem rapidamente escalar em grandes disrupções: uma tarifa mal calculada ou uma resposta errada de um *chatbot* pode propagar-se a centenas de clientes antes de ser corrigida. A automação sem supervisão adequada pode assim causar estragos – e cada ocorrência tem o potencial de se tornar viral ou levar a escrutínio público e jurídico, dado o impacto direto nos consumidores.

No próximo capítulo, analisamos alguns casos reais que exemplificam estes perigos e as suas consequências, preparando o terreno para a identificação das vulnerabilidades específicas dos sistemas hoteleiros.

3. Casos Reais de Incidentes Envolvendo IA e Hotelaria

EXAMINEMOS ALGUNS INCIDENTES NOTÁVEIS DOS ÚLTIMOS ANOS, LIGADOS A IA OU AUTOMAÇÃO, QUE AFETARAM EMPRESAS DE VIAGENS E HOTELARIA – REVELANDO LIÇÕES VALIOSAS:

1. **Delta Air Lines e a Controvérsia dos Preços Dinâmicos (2025) – *Confiança & Justiça Algorítmica***
   Em julho de 2025, a Delta Air Lines foi alvo de escrutínio intensivo após adotar um sistema de preços de bilhetes orientado por IA. Desenvolvido em parceria com a *startup* Fetcherr, o algoritmo prometia "revolucionar" a tarifação aérea, personalizando preços em função da procura e possivelmente do perfil do cliente.
   A novidade suscitou receios públicos e políticos de que a Delta pudesse estar a aplicar preços discriminatórios, explorando dados pessoais para cobrar mais de certos passageiros (por exemplo, se estivesse a viajar por um motivo urgente). Três senadores norte-americanos enviaram uma carta ao CEO da Delta, Ed Bastian, questionando se a companhia utilizaria a IA para "cobrar o que acha que cada cliente está disposto a pagar" e pedindo esclarecimentos sobre como dados pessoais seriam usados. A notícia desta investigação do Senado gerou indignação nas redes sociais e na imprensa, com muitos clientes a temer estar a ser alvo de "precificação individual" e manipulação algorítmica. Pressionada, a Delta emitiu comunicados públicos afirmando que não estava a definir tarifas de forma individualizada e que todos os passageiros continuariam a ver as mesmas tarifas base. No entanto, o episódio alimentou o debate sobre a necessidade de maior transparência e regulação da IA em sectores de consumo sensíveis. Para os hotéis, o caso Delta serve de alerta: se um algoritmo de preços for percebido como injusto ou opaco, os danos para a confiança do cliente podem ser imediatos e significativos, além de atrair fiscalização governamental.

2. **Case do *Chatbot* da Air Canada (2022–2024) – *Desinformação & Responsabilidade Legal***
   Em 2022, um cliente da Air Canada perguntou ao *chatbot* da empresa sobre reembolsos de bilhetes sob tarifa de emergência por falecimento de familiar. O assistente virtual de IA forneceu uma explicação aparentemente confiante – mas errada – instruindo o cliente a comprar um bilhete normal e solicitar o reembolso no prazo de 90 dias.

Na realidade, a política oficial da Air Canada (numa página distinta do *site*) não permitia tal reembolso. Quando o cliente seguiu as orientações do *chatbot* e descobriu posteriormente que não tinha direito à devolução, recorreu aos tribunais. Em 2024, um tribunal canadiano emitiu uma decisão histórica responsabilizando a Air Canada pelas informações erróneas dadas pelo seu *chatbot*, recusando o argumento de que "o *chatbot* é uma entidade separada" e afirmando que a empresa responde pelos atos e declarações dos seus sistemas de IA.
A Air Canada foi condenada a compensar o cliente e a interromper o uso do *chatbot* até garantir a sua fiabilidade. Esta decisão criou um precedente legal importante: as empresas podem ser legalmente responsáveis pelos erros das suas IAs, especialmente em matéria de direitos do consumidor. Para hotéis, isto enfatiza a importância de monitorizar e validar continuamente as respostas de *chatbots* e assistentes inteligentes, garantindo que não fornecem informações incorretas sobre políticas de reservas, tarifas, requisitos de viagem ou outros assuntos críticos.

3. **"Alucinação" de IA Causa Perda de Voo (2025) – *Experiência do Cliente & Risco Reputacional***
No verão de 2025, um casal de influentes *bloggers* de viagens espanhóis perdeu um voo para Porto Rico por confiar em conselhos de um *chatbot*. Ao planear a viagem, eles perguntaram a uma IA (*ChatGPT*) se precisavam de visto. A IA respondeu (incorretamente) que, não sendo necessário visto, poderiam embarcar sem preocupações.
Na realidade, embora cidadãos espanhóis não precisem de visto para Porto Rico, precisam de uma Autorização Eletrónica de Viagem (ESTA), por se tratar de um território dos EUA. Barrados no aeroporto, o casal relatou a história emocionada nas redes sociais, tornando-se viral e sendo amplamente coberta pela imprensa espanhola.
Este caso, apesar de não envolver uma empresa hoteleira diretamente, serve de lição: modelos de linguagem de IA têm propensão a "inventar" respostas falsas (conhecidas como *alucinações*), e quando os clientes confiam cegamente nessas respostas em contextos de viagem, os resultados podem ser desastrosos. As empresas de turismo que utilizam *chatbots* ou assistentes virtuais devem, portanto, implementar mecanismos de verificação e validação de conteúdo, especialmente para informações críticas (documentação de viagem, políticas de cancelamento, regulamentos sanitários, etc.), de forma a evitar equívocos custosos e salvaguardar a confiança do cliente.

4. **Intrusão através da Cadeia de Fornecimento (2024) – *A Fraqueza do Elo Mais Fraco***
Um incidente em 2024 evidenciou como vulnerabilidades em sistemas de parceiros podem comprometer hotéis. Piratas informáticos exploraram uma falha de segurança na API de uma agência de viagens online (OTA), utilizando-a como vetor para penetrar nos sistemas de reservas de vários hotéis interligados. Esse ataque de cadeia de abastecimento envolveu a injeção de consultas maliciosas através da integração legítima OTA–hotel e permitiu que os atacantes extraíssem informações confidenciais de hóspedes e dados de pagamento de 380 hotéis europeus, afetando 4,2 milhões de registos de clientes. Mais alarmante foi a deteção de "portas dos fundos" instaladas nas redes dos hotéis durante o ataque, facilitando futuras intrusões sem detecção.
Como resultado de todo este incidente, os hotéis impactados enfrentaram a tarefa árdua de notificar clientes e autoridades (conforme os requisitos do RGPD), além de terem de suportar os custos de investigações forenses, reparações de sistemas e potenciais multas. Este incidente realça que a segurança de um hotel é tão forte quanto a do seu parceiro mais fraco. Muitas vezes, os hotéis não têm visibilidade total sobre as práticas de segurança dos seus fornecedores tecnológicos, embora as suas redes estejam interligadas.
Este caso enfatiza a necessidade de diligência constante na seleção e monitorização de parceiros e da implementação de controlos técnicos (como segmentação de redes e políticas de acesso restrito para integrações) para minimizar o risco de contágio cibernético via terceiros.

5. **Ataque *AI-in-the-Middle* a Executivo Financeiro (2026) – *Fraude Financeira & Quebra de Autenticação***
   Os avanços recentes permitem a criminosos contornar até mecanismos de segurança outrora robustos. Um exemplo paradigmático em Portugal envolveu um diretor financeiro de um grupo hoteleiro, cujo login no portal bancário foi interceptado por um ataque *AI-in-the-Middle (AiTM)* durante um processo de autenticação de dois fatores. Os atacantes puseram uma IA a atuar como proxy entre o CFO e o banco, clonando em tempo real a página do *homebanking* e colhendo simultaneamente as credenciais de acesso e o código de uso único (OTP) do telemóvel. Conseguiram assim assumir a sessão bancária e ordenar uma transferência fraudulenta de 127.000 €, tudo numa questão de minutos. Este ataque contornou completamente a dupla autenticação tradicional – provando que MFA baseada em SMS/app pode ser insuficiente contra adversários com IA.
   Como desfecho do ataque, o hotel registou uma perda financeira significativa, tendo de reforçar urgentemente os seus sistemas de autenticação e alertar o banco e reguladores. A lição desta história é clara: mecanismos de autenticação "antigos" devem ser atualizados para métodos à prova de *phishing* (por exemplo, chaves de segurança *FIDO2*), e é crucial implementar sistemas de deteção de anomalias nas transações que alertem para movimentações atípicas, mesmo quando as credenciais pareçam legítimas.

Estes casos ilustram de forma tangível os desafios e consequências do uso da IA – tanto das suas falhas como das ameaças que potencia – e reforçam a premente necessidade de se adotar práticas de ciber-segurança adaptadas à era da IA. Na secção seguinte, sistematizamos as vulnerabilidades comuns nos ambientes tecnológicos hoteleiros que propiciam estes incidentes, preparando a base para as medidas de mitigação adiante discutidas.

4. Vulnerabilidades Comuns nos Sistemas Hoteleiros

VÁRIAS VULNERABILIDADES TÍPICAS TORNAM OS HOTÉIS PARTICULARMENTE EXPOSTOS A ATAQUES CIBERNÉTICOS – RISCOS QUE SE AMPLIFICAM COM A ADOÇÃO GENERALIZADA DE IA. OS PONTOS FRÁGEIS MAIS FREQUENTES INCLUEM:

1. **Algoritmos de Preços Dinâmicos:** Sistemas de *revenue management* que ajustam tarifas de forma autónoma podem comportar-se de maneira errática se mal calibrados. Sem restrições definidas, um algoritmo de preços pode gerar tarifas exorbitantes ou incongruentes (prejudicando a experiência do cliente) ou até incorporar viés de discriminação, cobrando involuntariamente mais de certos grupos de hóspedes.
   Além disso, atacantes podem explorar estas ferramentas – por exemplo, enviando um volume massivo de pedidos falsos de reserva para manipular os preços ou induzir o sistema a exibir *sobre-lotação* falsa (um tipo de ataque discutido adiante, conhecido como *"bloqueio de inventário"*). Este tipo de ataque não só prejudica as receitas, mas também mina a confiança dos clientes.

2. ***Chatbots* e Interfaces de Atendimento Automático:** *Chatbots*, assistentes de voz e *concierges* virtuais, se não forem robustos, podem ser alvo de manipulação. Técnicas de injeção de *prompts* permitem que atacantes ocultem comandos maliciosos em conteúdos gerados pelos utilizadores (por exemplo, críticas ou mensagens), levando um *chatbot* desprevenido a quebrar as suas regras e divulgar informações confidenciais ou tomar ações não autorizadas.
   Um cenário conhecido como *"concierge fantasma"* explora essa técnica para que o *chatbot* de um hotel acabe por fornecer, por exemplo, detalhes de clientes VIP ou processar reembolsos indevidos sob influência de instruções ocultas deixadas em textos aparentemente inofensivos. Mesmo sem interferência externa, *chatbots* podem fornecer respostas incorretas ou enganosas (como o caso Air Canada demonstrou), causando confusão e potenciais problemas legais.
   Deste modo, é essencial implementar fortes filtros de conteúdo e limites para *chatbots*, monitorizando o seu desempenho e estabelecendo intervenção humana quando surgirem perguntas complexas ou situações anómalas.

3. **Sistemas de Reservas e *Booking*:** O coração digital de um hotel é frequentemente um mosaico de sistemas integrados: sites de reservas, motores de busca de disponibilidade, PMS (sistema de gestão de propriedade), *gateways* de pagamento, ligações a GDS (sistemas globais de distribuição) e APIs de terceiros (por exemplo, *Expedia*, *Booking.com*, *Metasearch*). Esta interligação cria múltiplos pontos de entrada potenciais para atacantes.
   Como visto na violação da OTA em 2024, um único ponto fraco num parceiro pode abrir as portas a milhares de dados de hóspedes e cartões de crédito. Além disso, os sistemas de reservas enfrentam ameaças de *bots* automatizados: redes de *bots* podem tentar "sitiar" o inventário do hotel, simulando reservas massivas para esgotar temporariamente a disponibilidade. No assim chamado cenário de *"Enxame"*, microagentes de IA conseguem reservar milhares de quartos quase em simultâneo durante um período de pico, fazendo com que o seu site indique *lotação esgotada* e desviando potenciais clientes para concorrentes. No último momento os *bots* cancelam as reservas, deixando o hotel com quartos vazios e perda de receita. Este tipo de ataque aproveita a natureza automática e reativa dos sistemas de *booking* modernos, evidenciando a necessidade de mecanismos de detecção de *bots* e limites de transação por utilizador para proteger a disponibilidade do inventário.

4. **Dependência de Fornecedores e Integrações de Terceiros:** A digitalização hoteleira baseia-se numa complexa cadeia de fornecedores – desde sistemas de POS e controlos de acesso até serviços de *marketing* e CRMs na nuvem. Cada integração externa é uma nova superfície de ataque potencial, muitas vezes fora do controlo direto da equipa de TI do hotel. Se uma aplicação de *check-in* ou um sistema de contabilidade *cloud* de um fornecedor tiver uma vulnerabilidade, isso pode ser explorado para penetrar a rede do hotel.
   O desafio reside na baixa visibilidade que os hotéis têm sobre a segurança dos seus fornecedores. Também há o risco de compromisso de atualizações de *software*: um *hacker* que infiltre a infraestrutura de um fornecedor pode adulterar uma atualização legítima, distribuindo *malware* para todos os clientes daquele fornecedor de uma só vez.
   Para mitigar estes riscos, os hotéis devem adotar abordagens de zero trust com fornecedores – restringindo as permissões de integração ao mínimo necessário (p.ex., uma OTA só deveria ver e editar o que seja imprescindível para a reserva) – e realizar avaliações de segurança e *compliance* antes de contratar ou renovar contratos de *software* e serviços externos.

5. **Deficiências de Autenticação e Controlo de Acessos:** Apesar do elevado valor dos dados e transações em jogo, muitos hotéis ainda dependem de credenciais fracas ou facilmente subvertíveis. A reutilização de senhas por parte de funcionários e clientes, combinada com vazamentos massivos de dados noutras plataformas, leva a ataques de *credential stuffing* (tentativas automatizadas de usar credenciais roubadas noutros sites) que podem ter sucesso se não houver MFA robusto.
   Embora a autenticação multifator (MFA) se tenha tornado mais comum, os métodos baseados em SMS ou *apps* continuam vulneráveis a roubo em tempo real por IA (tal como visto no ataque ao CFO do hotel). Por outro lado, contas internas privilegiadas (como administradores de sistemas) muitas vezes não têm segregação de funções ou são partilhadas entre vários funcionários – o que, em caso de comprometimento, dá ao atacante acesso livre a vastas porções da rede. Além disso, o ser humano permanece um elo fraco: engenharia social sofisticada, potenciada por IA, consegue enganar funcionários a partilhar senhas ou aprovar ações maliciosas. Vozes *deepfake* de executivos a dar instruções de pagamento urgente ou e-mails forjados (mas gramaticalmente perfeitos) de parceiros a solicitar mudanças bancárias são cada vez mais usados para enganar até funcionários experientes. Estes cenários mostram que reforçar a segurança de identidade e acesso – com MFA de próxima geração (ex.: biometria ou chaves físicas), revisão periódica de permissões de utilizadores e treino *anti-phishing* – não é apenas boa prática, mas uma necessidade urgente.

5. **Fator Humano e Engenharia Social:** A natureza acolhedora e orientada para serviço dos hotéis pode ser explorada por criminosos. Os colaboradores são treinados para ser solícitos e resolver problemas dos hóspedes rapidamente, o que pode *facilitá-los* a contornar procedimentos de segurança se acreditarem estar a ajudar alguém.
   A IA agrava este risco ao produzir chamarizes de engenharia social quase infalíveis: por exemplo, documentos de identidade falsos e realistas que passam nos controlos de *check-in*, ou centenas de comentários negativos falsos produzidos por IA que arruínam a reputação *online* de um hotel numa única noite. De igual modo, um *phishing* direcionado a partir de um endereço e com um estilo de escrita praticamente indistinguíveis de um *e-mail* genuíno de um gestor ou parceiro do hotel pode levar funcionários a clicar em *links* maliciosos ou partilhar informação sensível. Como exemplo, em 2024 foi reportado que criminosos utilizaram a voz clonada por IA de um CEO para enganar um funcionário de um grupo hoteleiro, conseguindo que este transferisse uma grande soma de dinheiro para uma conta fraudulenta. Tal demonstra que, perante a IA, a "cadeia humana" de segurança requer reforço: formar equipas para verificar identidades de forma independente (por ex., retornar a chamada para um número oficial conhecido antes de cumprir pedidos financeiros por telefone), e instituir políticas onde nenhuma transação sensível seja efetuada apenas com base em instruções digitais.

EM TERMOS GERAIS, A ADOÇÃO MASSIVA DE IA NOS HOTÉIS SIGNIFICA QUE CADA SISTEMA E PROCESSO PODE SER REPENSADO EM TERMOS DE CIBERSEGURANÇA. A TABELA A SEGUIR RESUME AS PRINCIPAIS CATEGORIAS DE RISCO DE CIBER-SEGURANÇA NA ERA DA IA, INCLUINDO UMA BREVE DESCRIÇÃO E EXEMPLOS REAIS OU IMPACTOS POTENCIAIS:

CATEGORIA DE RISCO	DESCRIÇÃO
Preços Dinâmicos Descontrolados	Algoritmos de tarifas que resultam em preços injustos, voláteis ou discriminatórios se não forem bem calibrados ou auditados.
Chatbots e Assistentes Virtuais	*Chatbots* ou concierges digitais que podem fornecer informações incorretas, ou ser manipulados por utilizadores maliciosos através de injeções de *prompt*.
Integrações com Terceiros	APIs e sistemas de fornecedores externos (OTAs, sistemas de pagamento, *smart locks*, etc.) podem servir de porta de entrada se possuírem vulnerabilidades.
Engenharia Social Avançada	Tentativas de fraude e *phishing* sofisticado amplificadas por IA, incluindo e-mails perfeitos, *deepfakes* de voz/vídeo e outros esquemas multi-canal.
Malware Polimórfico por IA	*Malware* gerado por IA que se reescreve constantemente, evitando assinaturas de antivírus tradicionais e adaptando-se a cada tentativa de bloqueio.
Fraude de Identidade Sintética	Uso de IA para criar identidades e perfis falsos extremamente convincentes e contornar verificações ID ou esquemas de fidelidade dos hotéis.
Ataques *AI-in-the-Middle* (AiTM)	AI atua como intermediário invisível para roubar credenciais e sessões, quebrando mesmo MFA convencional.
"Shadow AI" / Uso Não-Autorizado	Colaboradores usam ferramentas de IA não-sancionadas (e.g. *ChatGPT*) nos fluxos de trabalho, expondo inadvertidamente dados internos a plataformas externas.
Ataques à Reputação Online	Uso de IA para gerar e disseminar conteúdo negativo falso em massa (comentários, críticas, *posts* nas redes sociais) com o propósito de prejudicar a imagem do hotel.
Bloqueio de Inventário "Enxame"	Enxames de *bots* de IA fazem reservas e cancelamentos em massa para esgotar temporariamente os quartos disponíveis.

Como se vê, o leque de riscos vai desde as armas cibernéticas potentes nas mãos de atacantes até as falhas e vulnerabilidades involuntárias nos sistemas de IA dos próprios hotéis. Tendo identificado estes perigos, importa perceber como lidar com eles: uma peça-chave dessa resposta está em garantir a responsabilidade e transparência das IAs – e é precisamente por isso que a auditoria de IA e o cumprimento dos regulamentos emergentes (como o AI *Act* da UE) assumem enorme relevância para o setor.

5. Auditoria de IA e Conformidade Regulatória no Setor Hoteleiro

À medida que a IA se integra cada vez mais nas operações hoteleiras, torna-se crucial estabelecer práticas de auditoria e conformidade legal específicas para esses sistemas. Três fatores principais impulsionam esta necessidade: manutenção da confiança e equidade, mitigação de riscos cibernéticos e cumprimento das novas regulações (sobretudo o *Regulamento Europeu de IA* e o RGPD).

O QUE É UMA AUDITORIA DE IA? EM TERMOS PRÁTICOS, PODE-SE IMAGINAR UMA AUDITORIA DE IA COMO UMA ESPÉCIE DE "INSPEÇÃO TÉCNICA REGULAR" AOS SISTEMAS INTELIGENTES. NÃO SE TRATA APENAS DE VERIFICAR SE A TECNOLOGIA ESTÁ FUNCIONAL – VAI MUITO ALÉM DISSO. UMA AUDITORIA DE IA AVALIA SE UM SISTEMA INTELIGENTE É:

- **Justo:** Trata todos os clientes e colaboradores de forma equitativa, evitando vieses indevidos? (Ex.: verificar se um algoritmo de recomendação não está a discriminar certos hotéis ou hóspedes sem motivo legítimo).
- **Seguro:** Protege os dados pessoais e transações dos hóspedes contra acessos indevidos ou fugas? (Ex.: garantir que um *chatbot* não expõe dados sensíveis e que os modelos respeitam normas de privacidade como o RGPD).
- **Explicável:** Oferece transparência nas suas decisões e ações? (Ex.: se um sistema de IA recusar uma reserva suspeita ou propor uma tarifa incomumente alta, consegue-se entender porquê? A lógica é passível de explicação e justificação?).
- **Legalmente Conformado:** Cumpre as leis aplicáveis (RGPD, AI *Act* etc.) e não infringe direitos do consumidor ou normativos setoriais?

PORQUÊ AUDITAR IAS NO SETOR DO TURISMO? EXPERIÊNCIAS RECENTES LEVANTAM VÁRIOS MOTIVOS:

1. **Salvaguardar Confiança & Reputação:** Em turismo, confiança é fundamental: um único escândalo tecnológico – seja um *pricing* abusivo, um *chatbot* mentiroso ou uma fuga de dados – pode destruir a reputação de um hotel num instante. Auditar regularmente as IAs contribui para evitar esses escândalos, detetando eventuais falhas ou injustiças *antes* que se tornem públicas. Assim, a auditoria de IA é uma nova forma de gestão de risco reputacional, que ajuda a manter a imagem de segurança e fiabilidade da marca.

2. **Exigências Legais Emergentes:** O Regulamento Europeu de IA (AI Act), que deverá entrar em vigor em 2026, classifica certos sistemas de IA como "alto risco" e vai exigir avaliações de conformidade e possivelmente auditorias externas para estas aplicações críticas (por exemplo, IAs usadas em segurança hoteleira, decisões de crédito, recrutamento de pessoal, etc.). O AI Act também obrigará à transparência: sempre que um cliente interaja com um sistema de IA (por exemplo, um *chatbot*), deve ser informado de que não está a falar com um humano. Além disso, o RGPD já impõe fortes obrigações de proteção de dados pessoais, que se aplicam integralmente aos sistemas de IA. Isso inclui a necessidade de evitar decisões totalmente automatizadas sem intervenção humana em certos contextos (artigo 22.º do RGPD), justificar como os dados dos clientes são utilizados e mantê-los seguros. A não conformidade com esses regulamentos pode resultar em multas multimilionárias e sanções severas.
   Portanto, a auditoria de IA também serve para assegurar e demonstrar às autoridades que o hotel está em cumprimento – por exemplo, documentando que o seu *chatbot* não retém dados pessoais sem consentimento ou que o seu algoritmo de preços foi testado quanto à equidade de género e não pratica discriminação injustificada.

3. **Melhoria de Desempenho & Eficiência:** Auditar não é apenas "procurar problemas" – também promove a excelência operacional. Modelos de IA sujeitos a revisão periódica tendem a ter maior exatidão e confiabilidade. A auditoria pode revelar, por exemplo, que um algoritmo de *upselling* está a recomendar insistentemente um serviço que clientes nunca compram, permitindo reprogramá-lo para sugerir algo mais relevante. Pode também descobrir que um *chatbot* tem dificuldades com certo idioma ou dialeto, possibilitando um *upgrade* de idioma antes que isso se torne um problema de serviço ao cliente.
   Em suma, as auditorias ajudam a manter as IAs alinhadas com os objetivos de negócio e a corrigir derivações ou bugs que comprometeriam a eficiência. Num setor onde margens são apertadas, evitar desperdícios e otimizar processos via IA fiável é uma vantagem estratégica.

IA Sem Auditoria vs IA Auditada – Em que Difere? Visualizemos como um sistema de IA não auditado contrasta com um sistema auditado, no contexto hoteleiro:

CRITÉRIO	IA NÃO AUDITADA (RISCOS)	IA AUDITADA (BENEFÍCIOS)
Precisão & Fiabilidade	Maior probabilidade de erros e "alucinações", já que o sistema não é periodicamente verificado. Pode fornecer recomendações ou decisões incorretas com confiança, confundindo tanto clientes como gestores.	Calibrada e verificada regularmente, o que resulta em menos falhas e informação mais precisa disponível para colaboradores e hóspedes.
Equidade & Viés	Suscetível a desenvolver viés injusto sem vigilância adequada – por exemplo, pode favorecer certos perfis de hóspedes ou tipos de reservas (*output* não equitativo). Pode levar a reclamações de clientes e danos de imagem.	Testada quanto a viés e correção de modo contínuo. Uma IA auditada promove resultados mais justos e imparciais, tratando todos os utilizadores de forma equitativa e reforçando a confiança do cliente na marca.
Conformidade Legal	Alto risco de infração de leis como o RGPD e o AI Act – por exemplo, recolha indevida de dados pessoais ou falta de transparência. Isto pode resultar em multas e ações legais severas.	Cumprimento assegurado através de controlos apropriados. A auditoria regular verifica e documenta que a IA está em linha com o RGPD (minimizando dados, respeitando direitos) e com os requisitos do AI Act, provando diligência em caso de inspeções.
Transparência & Confiança	Opera como uma "caixa negra": as razões das suas ações são opacas e desconhecidas até mesmo para a gestão do hotel. Essa falta de transparência mina a confiança de clientes, colaboradores e dos próprios gestores e reguladores.	Decisões explicáveis e auditáveis. Os hotéis conseguem traçar por que razão a IA tomou determinada decisão (ex.: por que um pedido foi sinalizado como fraude), permitindo rapidez na resolução de problemas e proporcionando justificativas a clientes ou reguladores.

Em síntese, auditar a IA é agora parte integrante da boa gestão de riscos em hotelaria. A par das auditorias financeiras e de qualidade já habituais, as auditorias de IA verificam se a "mente" digital do hotel está a funcionar corretamente e de acordo com as regras éticas e legais. Ser líder em IA responsável e transparente não só evita multas e crises, como pode ser um diferenciador competitivo no mercado: hóspedes e parceiros começarão a valorizar organizações que garantem que os seus sistemas de IA são seguros, justos e confiáveis.

6. Construir um *Framework* de Defesa: Recomendações para Equipas de TI

MITIGAR AS AMEAÇAS POTENCIALIZADAS PELA IA EXIGE UMA ESTRATÉGIA DE CIBER-SEGURANÇA MULTICAMADA. ABAIXO ESTÃO RECOMENDAÇÕES PRÁTICAS QUE AS EQUIPAS DE TI HOTELEIRAS DEVEM CONSIDERAR PARA REFORÇAR AS DEFESAS:

- **Supervisão Humana (*Human-in-the-Loop*) Obrigatória:** Em nenhum caso sistemas de IA com impacto crítico devem operar sem *checkpoints* de supervisão humana. É fundamental estabelecer pontos de controlo em fluxos automáticos de alta importância – por exemplo, um *bot* de reservas que aprove reembolsos ou atribuição de quartos caros deve requerer validação de um gestor antes de concluir a ação: deve por isso existir um "interruptor de emergência" (*kill switch*) que permita suspender imediatamente um sistema automatizado se este apresentar comportamento anómalo ou potencialmente prejudicial.
  Independentemente dos detalhes técnicos, a regra de ouro a adotar é que os humanos devem manter-se "no banco do condutor" quando a IA lida com transações financeiras, dados sensíveis ou decisões que impactam diretamente os hóspedes. Assim previnem-se cenários onde a IA, agindo sozinha, possa causar estragos descontrolados.

- **Reforçar a Segurança de Identidades e Acessos:** Proteja o hotel contra esquemas de roubo de credenciais e personificação, com medidas tais como:
  - **MFA Resistente a *Phishing*:** Evolua para métodos de autenticação robustos como chaves de segurança FIDO2/WebAuthn, autenticação biométrica ou *tokens* físicos, em substituição a OTPs via SMS ou *e-mail*. Estas abordagens baseadas em criptografia eliminam o risco de ataques *AI-in-the-Middle*, já que não há códigos intercetáveis.
  - **Verificação Comportamental:** Implemente sistemas de *login* que analisem o comportamento do utilizador como fator de autenticação. Por exemplo, padrões de digitação, horários usuais de acesso ou localização geográfica podem ajudar a detetar se é realmente o funcionário/hóspede legítimo em sessão. *Softwares* modernos utilizam IA para distinguir um utilizador verdadeiro de um *bot* ou impostor, mesmo se as credenciais corretas forem apresentadas.
  - **Gestão Restrita de Privilégios:** Aplique o princípio do privilégio mínimo. Garanta que cada colaborador tenha acesso apenas aos sistemas e dados indispensáveis para a sua função. Revise periodicamente os acessos e remova prontamente contas de ex-funcionários ou de serviços não utilizados. Desta forma, mesmo que uma conta seja comprometida, os danos potenciais ficam confinados. Em paralelo, a segmentação de rede é útil para isolar sistemas críticos (databases de hóspedes, servidores de pagamentos) das partes mais expostas (como serviços web ou integrações com terceiros).
  - **Verificação de Pedidos Sensíveis:** Estabeleça procedimentos de confirmação para quaisquer solicitações relacionadas com informações confidenciais ou transferências financeiras, especialmente quando recebidas por meios digitais. Por exemplo, se o departamento financeiro receber um e-mail alegadamente do diretor pedindo um pagamento urgente, exija que o colaborador confirme a ordem através de uma chamada telefónica ou vídeo para o próprio diretor, ou através de um segundo canal seguro conhecido. Esta regra de "dois fatores humanos" pode frustrar ataques de *phishing* mesmo quando e-mails ou telefonemas parecem legítimos (por exemplo, chamadas de voz *deepfake*).

- **Auditorias Regulares de IA & Testes de Intrusão:** Faça da auditoria e do *red teaming* parte da rotina de cibersegurança:
  - **Auditoria IAs periódicas:** Como detalhado anteriormente, realize auditorias de IA para todos os sistemas críticos: do motor de preços dinâmicos aos *chatbots*. Desenvolva *checklists* multidisciplinares que envolvam equipas de TI, análise de dados, legal e *compliance* para avaliar fatores como precisão, evolução de desempenho, viés e conformidade legal de cada IA. Corrija prontamente quaisquer desvios. Documente também os processos e resultados da auditoria – isso pode ser uma mais-valia em caso de inspeção ou questionamento, demonstrando que o hotel adota *governança* sobre as suas IAs.
  - **Preparação para Regulamentos:** Identifique desde já quais dos vossos sistemas de IA podem ser considerados de "alto risco" pelo AI *Act* (por exemplo, IAs usadas em segurança ou que afetem direitos dos colaboradores/hóspedes) e planeie tempo e recursos para certificações ou avaliações de conformidade externas exigidas por lei.
  - **Ao mesmo tempo, reforce os controlos RGPD:** minimize a retenção de dados pessoais nos modelos de IA e assegure que os hóspedes são informados quando interagem com IAs (transparência obrigatória no AI *Act*) — garantindo assim um melhor cumprimento deste importante regulamento legal, e reduzindo a exposição de dados a agentes maliciosos.
  - ***Red Teaming*:** Contrate ou treine profissionais de segurança para atuarem como "inimigos" e testarem ativamente os sistemas do hotel, tanto com ataques aos sistemas convencionais como a quaisquer ferramentas IA existentes: estes tentarão enganar o seu *chatbot* (teste de *prompt injection*), manipular o algoritmo de preços com dados maliciosos, ou simular um colaborador desonesto a extrair dados por meio da IA interna, entre outras medidas. Quanto mais brechas forem encontradas nesses ensaios controlados, mais preparadas as suas defesas estarão para um ataque real.
    Da mesma forma, realize simulações de *phishing* internas (inclusive com cenários de *deepfake* de voz e *e-mail*) para testar se os colaboradores seguem os protocolos de verificação estabelecidos. Use os resultados para reforçar a sensibilização e ajustar procedimentos conforme necessário.

- **Monitorização Ativa e Analítica Preditiva:** Aproveite também a IA do lado da defesa para detetar e responder a ameaças em tempo real:
  - **Ferramentas de Detecção Baseadas em IA:** Substitua ou complemente antivírus tradicionais por soluções de EDR/XDR (deteção e resposta a *endpoints*) de última geração que usam análises comportamentais e aprendizagem automática. Estas ferramentas monitorizam os dispositivos (computadores de hóspedes, terminais POS, servidores) em busca de atividades suspeitas – não apenas ficheiros maliciosos conhecidos. Quando um *ransomware* de IA começa a encriptar ficheiros em massa, ou quando um *script* tenta extrair dados, a EDR consegue detetá-lo pelo comportamento anómalo e isolar o processo antes que o dano se espalhe.
  - **Anomalias e SIEM Avançado:** Implemente sistemas de SIEM (*Security Information and Event Management*) com capacidades de deteção de anomalias. Estes sistemas centralizam *logs* e eventos de toda a infraestrutura (desde acessos a redes até interações do *chatbot*), e utilizam IA/ML para aprender qual é o padrão "normal" de atividade no seu hotel. Assim que algo foge do padrão – e.g. um pico repentino de falhas de *login* indicando um possível ataque de força bruta, ou um aumento anormal no volume de dados transferidos de um servidor sugerindo exfiltração – o sistema gera alertas.
    Com IA, estes alertas podem ser mais precisos, reduzindo *false positives* e priorizando as ameaças mais prováveis de serem reais. Este tipo de deteção proativa é crucial para travar ataques em curso, especialmente os que são executados em alta velocidade por sistemas automatizados.

- **Segurança de *Email* Reforçada:** O *phishing* continua a ser um vetor de ataque principal. Para complementar o treino dado aos funcionários, utilize ferramentas de segurança de e-mail com IA. Estas analisam o conteúdo, contexto e proveniência das mensagens recebidas em busca de sinais de *phishing* (uso de linguagem persuasiva, pequenos erros contextuais, URLs recém-criados ou ofuscados, etc.).
  Devem por isso ser implementadas políticas DMARC, SPF e DKIM para bloquear *e-mails* com remetentes forjados, e use *gateways* de *e-mail* que reescrevem URLs e testam anexos em ambientes *sandbox*, neutralizando ligações maliciosas ou *malware* antes que alguém clique.

- **Fortalecer a Cadeia de Fornecimento e Parceiros:** Uma estratégia de ciber-segurança abrangente deve tratar não apenas dos sistemas internos, mas também das ligações com o exterior:
  - **Cláusulas Contratuais de Segurança:** Ao contratar sistemas ou serviços de terceiros (p.ex., *software* de gestão de propriedade na nuvem, sistemas de *booking*, consultores TI), inclua cláusulas que obriguem o fornecedor a garantir práticas de segurança robustas e notificar prontamente qualquer incidente de segurança.
  - **Sempre que possível, solicite evidências de certificações de segurança (como ISO 27001 ou PCI DSS) ou relatórios de teste de intrusão do fornecedor, especialmente se este processar dados de cartão de crédito ou PII de hóspedes. Lembre-se:** dadas as estatísticas que indicam que cerca de 37% das violações de segurança poderão originar-se em ferramentas de IA de terceiros, a seleção criteriosa e a exigência de *compliance* por parte dos parceiros nunca foi tão importante.
  - **Controlo de Integridades e Acesso em APIs:** Tecnicamente, utilize *gateways* de API e *proxys* de serviço para gerir as integrações, impondo autenticação forte, limites de taxa (*rate limiting*) e monitorização em tempo real das chamadas de API. Por exemplo, se um parceiro externo começar subitamente a fazer muito mais chamadas que o normal ou a solicitar dados incomuns, isso deve gerar um alarme. Mantenha as integrações em redes segregadas (por exemplo, uma DMZ – zona desmilitarizada) para que um eventual comprometimento de uma API não dê acesso direto às suas bases de dados nucleares.
    Além disso, limite estritamente os privilégios das credenciais de API: se um parceiro não precisa de editar ou apagar dados, dê-lhe apenas acesso de leitura, restringindo o seu acesso apenas ao mínimo necessário para cumprimento dos seus objetivos e obrigações.
    Em resumo, como princípio deve lidar-se com cada integração com desconfiança (*"zero trust"*) — assumindo que pode ser comprometida, e planeando medidas para minimizar os danos caso isso aconteça.

- **Formação e Cultura de Segurança:** Apesar de toda a tecnologia, os colaboradores são a última linha (e muitas vezes a primeira) de defesa. Desenvolva um programa de formação contínua em ciber-segurança adaptado aos novos cenários de IA:
  - **Consciencialização sobre *Deepfakes* e Fraudes Automatizadas:** Mostre exemplos de voz/vídeo *deepfake* e *e-mails* gerados por IA, para que as equipas reconheçam sinais de alerta (p. ex., entoações ligeiramente robóticas, incoerências no contexto, pedidos de urgência injustificados). Estabeleça a cultura de "nunca validar transações financeiras ou divulgar dados sensíveis sem confirmação em segunda via", por mais legítima que a solicitação pareça. E encoraje os funcionários a reportar imediatamente quaisquer interações suspeitas, sem receio de retaliação ou ridículo.
  - **Sistemas de Recompensa e Simulações Internas:** Considere implementar testes surpresa – por exemplo, enviando periodicamente *e-mails* de *phishing* internos simulados para verificar se os colaboradores seguem as diretrizes (como não clicar em *links* duvidosos e reportar a tentativa). Recompense e reconheça os funcionários que demonstrem vigilância exemplar, para reforçar comportamentos seguros.

- **Protocolos Claros e Exercícios de Mesa:** Atualize os planos de resposta a incidentes com cenários de ataques de IA. Realize *drills* (exercícios de simulação) como, por exemplo, responder a uma situação em que o *website* do hotel é inundado por reservas falsas, ou gerir um *data leak* proveniente de um parceiro. Envolver diversos departamentos (TI, operações, comunicação, jurídico) nestes exercícios garante que todos sabem o seu papel se um incidente real ocorrer, e identifica lacunas no plano de resposta.

Combinando as medidas acima, os hotéis podem construir uma camada de defesa em profundidade adequada à era da IA. Não existe solução única eficaz em todos os cenários: a segurança resulta da sobreposição de camadas de tecnologia, processos e consciencialização humana. Em particular, a vigilância contínua é fundamental: se os atacantes adaptam as suas armas graças à IA, também as defesas devem evoluir dinamicamente, alimentadas por inteligência e atualizações frequentes.

7. Recomendações Práticas para Equipas de TI Hoteleiras

1. **Impor supervisão humana *(HITL)* em decisões críticas de IA:** Garantir que automatismos envolvendo finanças, dados pessoais ou serviço ao cliente tenham validação humana antes de concluir ações sensíveis.
2. **Implementar MFA *anti-phishing*:** Adotar métodos de autenticação robustos (ex.: *passkeys* FIDO2, chaves de segurança físicas) que não possam ser intercetados por *proxies* de IA.
3. **Monitorização comportamental e deteção de anomalias:** Usar IA para aprender os padrões de uso normais nos sistemas do hotel e detetar comportamentos fora do padrão (inícios de sessão, reservas, transferências), identificando intrusões automatizadas precocemente.
4. **Princípio do privilégio mínimo:** Restringir drasticamente acessos de funcionários e de sistemas aos dados e funções essenciais. Revogar prontamente acessos de ex-colaboradores e segmentar a rede para conter movimentos laterais de atacantes.
5. **Auditar todos os sistemas de IA regularmente:** Avaliar a precisão, equidade, transparência e *compliance* de algoritmos de preços, *chatbots*, sistemas de recomendação, etc. Corrigir desvios e documentar os resultados para efeito de conformidade regulatória.
6. **Testes de intrusão e *red teaming* focados em IA:** Simular ataques de agentes de IA contra os seus próprios sistemas (ex.: injeção de *prompt* em *chatbots*, manipulação de modelos) para identificar e corrigir vulnerabilidades antes que atacantes reais o façam.
7. **Ferramentas de segurança de próxima geração:** Implementar soluções de EDR/XDR e SIEM com análise comportamental e resposta automática para deter *malware* de IA e ataques em tempo real.
8. **Políticas rigorosas de verificação anti-fraude:** Exigir confirmações adicionais (via outros canais) para qualquer pedido de alteração de dados financeiros ou transferências de dinheiro, para deter fraudes multicanais com *deepfakes*.
9. **Fortalecer e auditar a cadeia de fornecedores:** Adotar cláusulas contratuais de segurança, exigir certificações e avaliações de segurança de parceiros tecnológicos, e monitorizar ativamente o tráfego e atualizações dos seus sistemas por potenciais sinais de comprometimento.
10. **Formar e sensibilizar a equipa para ameaças de IA:** Capacitar todos os funcionários – de rececionistas a gestores – para reconhecer e reportar *phishing* avançado, *deepfakes* e outras fraudes. Promover uma cultura de segurança onde toda a equipa entende que o *elo humano* deve ficar alerta e é crucial para complementar as defesas tecnológicas.

Implementando este conjunto de medidas, os hotéis estarão muito melhor posicionados para enfrentar as ciber-ameaças modernas: metaforicamente, governar a IA não é colocar um travão à transformação digital, mas sim garantir que esta está também equipada com um volante calibrado, para que possamos conduzir a inovação com segurança numa época de automação inteligente.

8. Conclusão

NO LIMIAR DE 2026, A CIBER-SEGURANÇA NA INDÚSTRIA HOTELEIRA DEVE SER RE-IMAGINADA SOB DUAS PERSPETIVAS COMPLEMENTARES:

1. A IA amplificou as ameaças clássicas – *phishing*, *malware*, fraude financeira – conferindo-lhes uma velocidade e escala sem precedentes. Os hotéis, com os seus vastos repositórios de dados e ecossistemas digitais complexos, tornaram-se alvos preferenciais e precisam de defesas igualmente modernizadas.
2. Os próprios hotéis estão a evoluir para serem organizações cada vez mais automatizadas e dependentes de IA, com riscos internos inerentes de falha de sistemas e consequências inesperadas de decisões algorítmicas.

Assim, proteger as operações hoteleiras hoje significa tanto bloquear agentes de IA maliciosos externos como garantir que as IAs internas são fiáveis, auditáveis e sob controlo humano.

Em última análise, a adoção bem-sucedida de IA na hotelaria passa por um equilíbrio entre aproveitar a automação e manter um forte controlo de segurança e ética. Os hotéis que investirem em ciber-segurança avançada – integrando ferramentas de IA defensiva, auditorias regulares e formação humana – estarão melhor equipados para preservar o ativo mais precioso do setor: a confiança dos hóspedes.

Num mundo inundado de *deepfakes* e agentes digitais maliciosos, a confiança e a segurança tornar-se-ão verdadeiros luxos – e os hotéis que as oferecerem consistentemente emergirão como líderes de mercado, provando que é possível inovar com IA sem abdicar da segurança e integridade do serviço prestado aos clientes.

Em suma: proteja a sua "citadela digital" para poder continuar a cultivar a confiança — que é, hoje como ontem e amanhã, a essência da hospitalidade.

Biografia da equipa editorial

CÉLIA RAFAEL

Professora Adjunta da Escola Superior de Turismo e Tecnologia do Mar do Politécnico de Leiria, é doutorada em Gestão de Empresas e Sociologia, pela Universidade de Extremadura, Espanha, com investigação centrada no impacto das experiências virtuais online na formação da imagem dos destinos turísticos. É mestre em Engenharia Eletrotécnica e de Computadores e licenciada em Informática de Gestão. Atualmente, coordena o curso de Tecnologias Digitais aplicadas ao Turismo.
É investigadora integrada do CiTUR – Centro de Investigação, Desenvolvimento e Inovação em Turismo, desenvolvendo atividades nas áreas das tecnologias digitais aplicadas ao turismo, transformação digital, marketing digital, inovação em destinos turísticos, experiências virtuais, inteligência artificial e tecnologias emergentes no setor do turismo. Como docente, leciona e tem desenvolvido atividade pedagógica e científica no âmbito do marketing digital no turismo, das tecnologias digitais aplicadas ao turismo e da inovação pedagógica no ensino superior. É Coordenadora Científica do Projeto DIH InnovTourism – PRR, no Politécnico de Leiria, Portugal, contribuindo para o desenvolvimento de soluções digitais, estratégias de inovação e capacitação das PME do setor do turismo.
ORCID: 0000-0001-7388-129X
E-mail: celia.rafael@ipleiria.pt

JOÃO COSTA

Professor Adjunto na Escola Superior de Turismo e Tecnologia do Mar do Instituto Politécnico de Leiria e doutorado em Engenharia Multimédia pela Universitat Politècnica de Catalunya. Docente nos 1.º e 2.º ciclos de estudos, lecionando unidades curriculares nas áreas dos Sistemas de Informação Geográfica, Imagem e Edição Gráfica e Marketing Digital. Integra o CiTUR – Centro de Investigação, Desenvolvimento e Inovação em Turismo, onde participa em projetos de investigação aplicada nas áreas do Turismo, financiados por programas nacionais e internacionais. A sua atividade científica centra-se no turismo digital, no turismo sustentável e na inovação tecnológica aplicada ao setor do turismo. Desempenha funções de Coordenador Científico do projeto DIH InnovTourism - PRR no Politécnico de Leiria, contribuindo para a promoção da inovação, da digitalização e da competitividade das empresas e organizações do setor turístico em Portugal.
ORCID: 0000-0003-2359-0296
E-mail: joao.costa@ipleiria.pt

JOÃO TIAGO SILVA

Licenciado em Turismo pela Escola Superior de Turismo e Tecnologia do Mar do Politécnico de Leiria. Atualmente, frequenta o Mestrado em Estudos e Gestão da Cultura no Iscte – Instituto Universitário de Lisboa, na Escola de Sociologia e Políticas Públicas.
É bolseiro de investigação do CiTUR, integrando o projeto InnovTourism - Digital Innovation Hub contribuindo para o desenvolvimento de soluções digitais, estratégias de inovação e capacitação das PME do setor do turismo.
ORCID: 0009-0003-8784-6868
E-mail: joaotiago.fm.silva03@gmail.com

PAULO ALMEIDA

Professor Coordenador Principal do Politécnico de Leiria, é Doutor em Marketing e Comércio Internacional, pela Universidade de Extremadura, Espanha. Mestre em Gestão e Desenvolvimento em Turismo, pela Universidade de Aveiro. Licenciado em Gestão Hoteleira, pela Universidade do Algarve. Foi Diretor da Escola Superior de Turismo e Tecnologia do Mar (ESTM). Foi Presidente da Comissão Executiva da RIPTUR – Rede de Escolas Superiores Politécnicas com Cursos de Turismo. É hoje Diretor Nacional do CiTUR - Centro de Investigação, Desenvolvimento e Inovação, sendo Executive Editor do EJTHR - European Journal of Tourism, Hospitality and Recreation. Como investigador tem apresentado diversas comunicações em congressos internacionais e publicado alguns trabalhos e artigos na área do Marketing Turístico e da Imagem dos Destinos Turísticos, procurando perceber a problemática integrada no desenvolvimento e promoção dos destinos turísticos. Como docente leciona e tem orientado diversas teses de Doutoramento e dissertações no Mestrado em Gestão e Direção Hoteleira e no Mestrado em Marketing e Promoção Turística. É hoje Investigador Responsável pelos Projetos FAST – Agenda ATT - PRR, e Projeto DIH InnovTourism - PRR, no Politécnico de Leiria, Portugal.
ORCID: 0000-0002-4797-2128

Parceiro


Financiado pela
União Europeia
NextGenerationEU


REPÚBLICA
PORTUGUESA


PRR
Plano de Recuperação
e Resiliência


CiTUR


POLITÉCNICO
DE LEIRIA