Manual de Buenas Prácticas de Ciberseguridad para PYMES del Sector Turístico

ÍNDICE

1. MANUAL DE BUENAS PRÁCTICAS DE CIBERSEGURIDAD PARA PYMES DEL SECTOR TURÍSTICO

Antes de entrar en materia, conviene familiarizarse con los términos más habituales en ciberseguridad. No es necesario ser un experto en informática para entender estos conceptos: a continuación los explicamos de forma sencilla, con ejemplos cercanos al día a día de un negocio turístico.

1.1. GLOSARIO DE TERMINOLOGÍA RELACIONADA CON LA CIBERSEGURIDAD

En la siguiente tabla encontrarás los términos clave que aparecen a lo largo de este manual, explicados en un lenguaje pensado para que cualquier persona pueda comprenderlos, independientemente de su nivel técnico.

Término	Definición
Autenticación Multifactor (MFA)	Es como tener dos cerraduras en la puerta en vez de una. Para entrar en un sistema no basta con la contraseña: también se necesita un segundo paso, como un código que llega al móvil o una huella dactilar. Así, aunque alguien descubra tu contraseña, no podrá acceder sin ese segundo factor.
Cifrado	Imagina que envías una carta, pero en vez de escribirla en español la escribes en un código secreto que solo el destinatario puede descifrar. Eso es el cifrado: convierte la información en un formato ilegible para cualquiera que no tenga la clave correcta. Se usa tanto para proteger datos guardados en un ordenador como para los que viajan por internet (por ejemplo, cuando un cliente introduce su tarjeta en tu web).
Firewall	Es como el portero de un edificio: controla quién entra y quién sale de tu red. Un firewall revisa todo el tráfico de datos y bloquea aquello que no cumple las reglas de seguridad que hayas establecido. Puede ser un programa instalado en el ordenador o un dispositivo físico que protege toda la red del negocio.
Malware	Es el nombre genérico para cualquier programa malintencionado: virus, gusanos, troyanos, programas espía, etc. Puede llegar a través de un correo electrónico sospechoso, una descarga de internet o incluso un USB que alguien conecta al ordenador. Una vez dentro, puede robar datos, bloquear el sistema o espiar lo que haces.
Phishing	Es un engaño digital. Los atacantes envían correos, mensajes o crean páginas web que imitan a empresas reales (un banco, una plataforma de reservas, una aerolínea) para que introduzcas tu contraseña, tu número de tarjeta u otros datos sensibles. En el sector turístico es muy habitual recibir correos falsos que simulan ser de Booking, Airbnb o de un proveedor.
Ransomware	Es un tipo de malware que secuestra tus datos: los cifra para que no puedas acceder a ellos y te pide un rescate económico (normalmente en criptomonedas) para devolvértelos. Para un hotel o restaurante, esto puede significar perder el acceso a reservas, datos de clientes y facturación durante días.
VPN (Red Privada Virtual)	Es como un túnel privado dentro de internet. Cuando te conectas a una VPN, toda la información que envías y recibes va cifrada, de forma que nadie puede espiarla

	aunque estés usando una red Wi-Fi pública. Es especialmente útil para empleados que trabajan fuera del establecimiento o acceden a los sistemas desde casa.
Punto de Acceso Inalámbrico	Es el dispositivo que emite la señal Wi-Fi a la que se conectan móviles, portátiles y otros aparatos. En un hotel o restaurante puede haber varios repartidos por las instalaciones. Si no se configuran correctamente, cualquiera podría conectarse a la red interna del negocio.
Ingeniería Social	Son trucos psicológicos que usan los atacantes para manipular a las personas y conseguir información o acceso. No se aprovechan de fallos técnicos, sino de la confianza humana. Puede ser una llamada de alguien que se hace pasar por el soporte técnico, un SMS urgente que pide hacer clic en un enlace, o incluso alguien que se presenta físicamente en recepción haciéndose pasar por un proveedor.
Gestión de Parches	Los parches son como las reparaciones que se hacen en una carretera: corrigen fallos o agujeros de seguridad que se descubren en los programas que usas. Mantener los sistemas actualizados con los últimos parches es una de las formas más sencillas y eficaces de protegerse contra ataques.
Copia de Seguridad (Backup)	Es hacer una copia de tus datos importantes y guardarla en un lugar seguro y separado. Si un día sufres un ataque, un fallo del disco duro o un accidente, podrás recuperar toda la información desde esa copia. La regla de oro es tener al menos tres copias, en dos soportes diferentes, con una de ellas fuera del local (por ejemplo, en la nube).
Certificado SSL/TLS	Es lo que hace que una página web muestre el candado y el “https” en la barra del navegador. Significa que la comunicación entre el cliente y tu web está cifrada: los datos de reserva, contraseñas y pagos viajan protegidos. Sin este certificado, cualquiera podría interceptar esa información.
DDoS	Es como si miles de personas intentasen entrar a la vez por la puerta de tu local: el sistema se satura y deja de funcionar. Los atacantes envían un volumen enorme de tráfico falso a tu web o servidor para dejarlo fuera de servicio. En temporada alta, un ataque así puede dejar tu plataforma de reservas inaccesible justo cuando más la necesitas.
SIEM	Es un sistema que funciona como un centro de vigilancia: recoge información de seguridad de todos tus equipos y programas, la analiza en tiempo real y te avisa cuando detecta algo sospechoso. Es como tener un guardia de seguridad digital que vigila todo a la vez.
Segmentación de Red	Consiste en dividir tu red en partes separadas, como si en un hotel separases la Wi-Fi de los huéspedes de la red interna del personal. De esta forma, si un atacante consigue acceder a una parte, no puede moverse libremente al resto. Es una medida sencilla que limita mucho el daño en caso de intrusión.
Zero Trust	Es una filosofía de seguridad que dice: “no te fíes de nadie por defecto”. Da igual que un dispositivo esté conectado desde dentro de la oficina o que un empleado lleve años en la empresa; cada vez que alguien intenta acceder a algo, el sistema verifica que realmente tiene permiso. Es como pedir el DNI en cada puerta, no solo en la entrada principal.

Política de Contraseñas	Son las normas que estableces en tu empresa sobre cómo deben ser las contraseñas: que sean largas (mínimo 12 caracteres), que mezclen letras, números y símbolos, que no se repitan entre servicios y que se cambien periódicamente. Son reglas básicas pero que muchas veces no se aplican.
SOC (Centro de Operaciones de Seguridad)	Es un equipo (o un servicio contratado) que vigila la seguridad informática de forma continua, 24 horas al día, 7 días a la semana. Detecta amenazas, responde a incidentes y coordina la recuperación. Para una PYME, esto suele contratarse como servicio externo.

2. CIBERSEGURIDAD APLICADA AL SECTOR TURÍSTICO

La ciberseguridad puede sonar a algo que solo afecta a grandes empresas tecnológicas, pero nada más lejos de la realidad. Si tienes un hotel, un restaurante, una casa rural o una agencia de viajes, manejas a diario datos que los ciberdelincuentes buscan activamente: nombres, DNI, números de tarjeta, direcciones de correo y hábitos de consumo de tus clientes. Proteger esa información no es solo una obligación legal, sino una cuestión de confianza y supervivencia del negocio.

2.1. IMPORTANCIA DE LA CIBERSEGURIDAD EN EL SECTOR TURÍSTICO

El sector turístico se ha digitalizado a gran velocidad. Hoy en día, la mayoría de las reservas se realizan por internet, los pagos se procesan electrónicamente, los programas de fidelización almacenan datos personales y las opiniones de los clientes en plataformas online pueden determinar el éxito o el fracaso de un negocio. Toda esta digitalización aporta enormes ventajas, pero también abre la puerta a riesgos que antes no existían.

Piensa en toda la información que maneja tu negocio a lo largo de un solo día: datos de reservas con nombres y documentos de identidad, números de tarjetas de crédito, direcciones de correo electrónico, preferencias de viaje, registros de entrada y salida, datos de facturación. Toda esa información tiene un valor enorme en el mercado negro digital.

Un incidente de ciberseguridad no es solo un problema técnico. Sus consecuencias pueden afectar directamente a la viabilidad de tu negocio:

Pérdida de confianza

Si los datos de tus clientes se ven comprometidos, la reputación de tu negocio puede tardar años en recuperarse. Un huésped cuya tarjeta ha sido utilizada fraudulentamente tras alojarse en tu hotel probablemente no volverá.

Sanciones económicas

El incumplimiento de la normativa de protección de datos (RGPD) puede conllevar multas de hasta el 4% de la facturación anual o 20 millones de euros, la cantidad que sea mayor.

Paralización de la actividad

Un ataque de ransomware puede dejarte sin acceso a tu sistema de reservas, a los datos de clientes o incluso al control de las cerraduras electrónicas del hotel durante días o semanas.

Costes de recuperación

Más allá del propio rescate (que nunca se recomienda pagar), restaurar los sistemas, contratar especialistas forenses, comunicar la brecha a los afectados y a las autoridades tiene un coste elevado.

Responsabilidad legal de los administradores

Los directivos y administradores de la empresa pueden responder personalmente por negligencia en la protección de datos. Si se demuestra que no se adoptaron medidas razonables de seguridad, las sanciones pueden ir más allá de la empresa y afectar al patrimonio personal de quien la dirige.

Daño reputacional en plataformas online

Tras un incidente de seguridad, las reseñas negativas se propagan rápidamente por TripAdvisor, Google, Booking y redes sociales. Un solo comentario de un cliente afectado puede disuadir a cientos de potenciales visitantes. En el sector turístico, donde la reputación online es decisiva, este daño puede ser más costoso que la propia multa.

Pérdida de acuerdos con touroperadores y plataformas

Las grandes plataformas de reservas y los touroperadores exigen a sus colaboradores unos mínimos de seguridad. Si tu negocio sufre un incidente grave, pueden suspender tu cuenta o rescindir el contrato, dejándote sin uno de tus principales canales de venta precisamente cuando más lo necesitas.

Efecto multiplicador en temporada alta

Si el ataque ocurre en temporada alta (verano, Semana Santa, puentes festivos), las pérdidas se multiplican exponencialmente. Un hotel que no puede gestionar reservas durante una semana de agosto puede perder los ingresos equivalentes a varios meses de temporada baja. Los ciberdelincuentes lo saben y tienden a atacar justo en estos momentos de máxima actividad.

Obligación de notificación pública

El RGPD obliga a comunicar las brechas de seguridad a la Agencia Española de Protección de Datos en un plazo máximo de 72 horas, y en muchos casos también a todos los clientes afectados individualmente. Esta notificación genera un daño reputacional adicional y un coste operativo importante: hay que identificar a los afectados, redactar las comunicaciones, atender las reclamaciones y gestionar la crisis mediática.

Pérdida de datos irrecuperables

Sin copias de seguridad adecuadas, ciertos datos pueden perderse para siempre: el histórico de clientes, la contabilidad de años anteriores, las reservas futuras, las configuraciones de los sistemas. Reconstruir esta información, cuando es posible, requiere semanas de trabajo y nunca se recupera al completo.

Incremento de primas de seguros

Tras un incidente de ciberseguridad, el coste de los seguros de ciberriesgo puede aumentar significativamente, o incluso la aseguradora puede negarse a renovar la póliza. Y si no tenías seguro, contratarlo después de un incidente será mucho más caro.

Impacto psicológico y desgaste del equipo

Un ciberataque no solo afecta a los sistemas: genera estrés, incertidumbre y desmotivación entre los empleados. El personal de recepción que tiene que gestionar las quejas de los clientes afectados, el gerente que debe tomar decisiones de emergencia sin información completa, el equipo técnico que trabaja contrarreloj para restaurar los sistemas... El desgaste humano es real y puede provocar bajas laborales y rotación de personal.

Pérdida de ventaja competitiva

Mientras tu negocio está paralizado intentando recuperarse de un ataque, tu competencia sigue operando con normalidad y captando a los clientes que tú no puedes atender. En un sector tan competitivo como el turístico, perder visibilidad y operatividad durante días o semanas puede suponer ceder cuota de mercado que luego es muy difícil de recuperar.

Interrupción de la cadena de pagos

Un ataque puede bloquear tu capacidad de cobrar a los clientes y de pagar a tus proveedores. Si no puedes procesar pagos con tarjeta, emitir facturas o acceder a tu banca online, la cadena financiera del negocio se rompe. Esto puede generar impagos a proveedores, recargos bancarios y problemas de liquidez que agraven aún más la situación.

Las PYMES turísticas son un objetivo especialmente atractivo para los ciberdelincuentes porque, por lo general, manejan muchos datos sensibles pero disponen de menos recursos técnicos y humanos

para protegerlos que una gran cadena hotelera. Sin embargo, la buena noticia es que la mayoría de los ataques se pueden prevenir con medidas básicas que no requieren grandes inversiones.

2.2. DESAFÍOS ESPECÍFICOS DEL SECTOR

El sector turístico presenta una serie de particularidades que lo hacen especialmente sensible a las amenazas cibernéticas:

Gran Dependencia de las Reservas Online

La mayoría de tus ingresos probablemente pasan por plataformas digitales: tu propia web, Booking, Expedia, Google Hotels, TheFork, etc. Si un atacante compromete tu cuenta en una de estas plataformas o tu pasarela de pago, las consecuencias son inmediatas. Un ejemplo habitual: un correo falso que simula ser de Booking te pide que "verifiques" tus credenciales, y al introducirlas, el atacante toma el control de tu cuenta.

Uso Extensivo de Dispositivos Móviles

Tus empleados probablemente usan móviles o tablets para gestionar reservas, comunicarse con proveedores o acceder al correo. Muchas veces son sus propios dispositivos personales (lo que se conoce como BYOD). Si uno de esos móviles se infecta con malware o se pierde sin protección, los datos de tu negocio quedan expuestos.

Interconexión de Sistemas

El sistema de gestión del hotel (PMS), la plataforma de reservas, el TPV (terminal de punto de venta), las cerraduras electrónicas, los sensores de climatización... todo está conectado. Si un atacante consigue entrar por uno de estos puntos, puede moverse lateralmente hasta alcanzar los datos más sensibles.

Estacionalidad y Rotación de Personal

En temporada alta contratas personal temporal que quizá no ha recibido ninguna formación en seguridad. Estas personas manejan igualmente datos de clientes, acceden a los sistemas de reserva y utilizan dispositivos del negocio. La falta de formación incrementa enormemente el riesgo de que alguien caiga en un engaño de phishing o cometa un error de seguridad.

Diversidad de Proveedores y Terceros

Tu negocio probablemente trabaja con varios proveedores tecnológicos: la empresa que gestiona tu web, la pasarela de pago, el proveedor del sistema de reservas, la empresa de mantenimiento informático, el servicio de contabilidad en la nube, etc. Cada uno de ellos es un posible punto de entrada si no cumple con unos mínimos de seguridad.

Presencia en Múltiples Ubicaciones

Si gestionas varios establecimientos (una cadena de apartamentos, varios restaurantes, oficinas de información turística), aplicar las mismas medidas de seguridad de forma uniforme es un reto. Cada local puede tener su propia red, sus propios equipos y su propio personal.

Atención al cliente 24/7

Un hotel opera las 24 horas del día. Eso significa que los sistemas deben estar disponibles permanentemente, lo que deja menos margen para realizar mantenimientos, aplicar actualizaciones o desconectar equipos para revisar incidentes sin afectar al servicio.

2.3. NORMATIVAS Y REGULACIONES

Cumplir con la legislación no es opcional: hay normativas europeas y nacionales que establecen obligaciones muy concretas para cualquier empresa que maneje datos personales. A continuación, las más relevantes para tu negocio, explicadas de forma práctica:

Reglamento General de Protección de Datos (RGPD)	Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD)
Es la normativa europea de referencia en protección de datos personales. Afecta a cualquier empresa que trate datos de ciudadanos de la UE, independientemente de su tamaño. En la práctica, te obliga a: obtener el consentimiento explícito de los clientes antes de tratar sus datos; informarles de qué datos recoges y para qué; permitirles acceder, rectificar o borrar sus datos si lo solicitan; y notificar cualquier brecha de seguridad a la Agencia Española de Protección de Datos en un plazo máximo de 72 horas. Las sanciones por incumplimiento pueden alcanzar los 20 millones de euros o el 4% de la facturación anual global.	Es la ley española que complementa al RGPD y lo adapta al marco jurídico nacional. Establece obligaciones adicionales, como la designación de un Delegado de Protección de Datos en determinados casos, y regula aspectos específicos como el derecho al olvido en internet o la protección de datos de menores. Si tu negocio opera en España, debes cumplir tanto con el RGPD como con esta ley.
Directiva NIS2	**Estándar PCI DSS**
Es una normativa europea relativamente reciente que amplía las obligaciones de ciberseguridad a más sectores económicos. Aunque está pensada principalmente para empresas medianas y grandes o aquellas que gestionan infraestructuras críticas, marca la dirección en la que va la regulación: cada vez se exigirá más a todas las empresas en materia de seguridad digital. Es importante estar al tanto de su evolución.	Si tu negocio acepta pagos con tarjeta (y es muy probable que lo haga), debes cumplir con esta norma. No es una ley en sí, sino un estándar de la industria de medios de pago que establece requisitos técnicos para proteger los datos de las tarjetas de tus clientes. Su incumplimiento puede acarrear multas por parte de las entidades bancarias e incluso la retirada del servicio de cobro con tarjeta.

El incumplimiento de estas normativas no solo conlleva sanciones económicas. Puede generar responsabilidades legales personales para los administradores de la empresa y un daño a la imagen del negocio que resulta muy difícil de reparar. Además, en caso de reclamación de un cliente afectado, la empresa deberá demostrar que había adoptado medidas adecuadas para proteger sus datos.

2.4. ¿POR QUÉ DEBERÍA PREOCUPARME SI SOY UNA PYME?

Es habitual pensar que los ciberataques solo afectan a grandes empresas, pero la realidad es muy diferente. Las PYMES son, de hecho, uno de los objetivos preferidos de los ciberdelincuentes, precisamente porque suelen tener menos defensas. Algunos datos que ayudan a entender la dimensión del problema:

- La mayoría de los ciberataques tienen como objetivo pequeñas y medianas empresas, no grandes corporaciones.

- El coste medio de un incidente de ciberseguridad para una PYME se estima en varias decenas de miles de euros, considerando la interrupción de la actividad, la pérdida de datos y los costes de recuperación.
- Muchas PYMES que sufren un ciberataque grave no consiguen recuperarse completamente y algunas se ven obligadas a cerrar.
- En el sector turístico, los ataques se intensifican en temporada alta, justo cuando el negocio es más vulnerable porque opera a máxima capacidad y con personal temporal.

La ciberseguridad no es un gasto, es una inversión en la continuidad de tu negocio. Y como veremos en las siguientes secciones, muchas de las medidas más efectivas son sencillas, asequibles y no requieren conocimientos técnicos avanzados.

3. PRINCIPALES AMENAZAS DE CIBERSEGURIDAD DESDE DIFERENTES DISPOSITIVOS

Para poder protegerte, primero necesitas saber de qué te estás protegiendo. Las amenazas de ciberseguridad no son abstractas: son situaciones muy concretas que pueden afectar a tu negocio cualquier día. A continuación las explicamos organizadas por el tipo de dispositivo al que afectan, con ejemplos prácticos del sector turístico.

3.1. AMENAZAS EN DISPOSITIVOS MÓVILES

Los teléfonos y tablets se han convertido en herramientas de trabajo imprescindibles en el sector turístico. Pero su uso constante, muchas veces en redes abiertas y con mezcla de uso personal y profesional, los convierte en un punto débil.

- **Malware Móvil:** Son aplicaciones maliciosas que se instalan en el teléfono y pueden robar datos, espiar lo que escribes o tomar el control del dispositivo. Suelen llegar a través de tiendas de apps no oficiales, enlaces en mensajes o correos electrónicos engañosos. Ejemplo: un empleado descarga una app “gratuita” de traducción desde una web desconocida, y esa app registra en segundo plano todo lo que escribe, incluyendo contraseñas.

- **Phishing Móvil (Smishing y Vishing):** Son estafas que llegan por SMS o por llamada telefónica. En el sector turístico es muy habitual recibir mensajes falsos que simulan ser confirmaciones de reserva, alertas de cancelación o avisos de plataformas como Booking o Airbnb. El mensaje incluye un enlace que lleva a una web falsa donde te piden tus credenciales.

- **Redes Wi-Fi Públicas:** Cuando un empleado se conecta al Wi-Fi de una cafetería, un aeropuerto o un espacio público, un atacante puede estar “escuchando” todo lo que envía y recibe (correos, contraseñas, datos de clientes). Esta técnica se llama “Man-in-the-Middle” y es más habitual de lo que parece.

- **Pérdida o Robo de Dispositivos:** Un móvil perdido o robado que no tiene PIN, cifrado ni borrado remoto activado puede dar acceso directo al correo corporativo, a la app de gestión de reservas, a las fotos de documentos de identidad de clientes y a cualquier otra información almacenada en el dispositivo.

- **Aplicaciones con Permisos Excesivos:** Muchas apps piden acceso a la cámara, micrófono, contactos o ubicación sin que sea necesario para su función. Si un empleado instala una app aparentemente inofensiva que tiene acceso a todo el teléfono, esa app puede estar recopilando información sin que nadie lo note.
- **Bluetooth y NFC desprotegidos:** Muchos empleados llevan el Bluetooth o el NFC del móvil activado permanentemente sin ser conscientes del riesgo. Un atacante cercano puede aprovechar estas conexiones para enviar archivos maliciosos, interceptar datos o incluso emparejar su dispositivo sin que el usuario lo note. En un hotel o restaurante, donde el personal está en contacto constante con decenas de desconocidos, esta exposición es especialmente peligrosa.

- **Códigos QR maliciosos:** En el sector turístico se usan cada vez más los códigos QR: para ver la carta del restaurante, acceder a información turística, conectarse al Wi-Fi o dejar una reseña. Un atacante puede sustituir un QR legítimo por uno falso (pegando una pegatina encima, por ejemplo) que dirija al empleado o al cliente a una web maliciosa que roba credenciales o instala malware en el dispositivo.
- **Copias de seguridad automáticas en la nube sin control:** Muchos móviles suben automáticamente fotos, documentos y datos a servicios en la nube (Google Drive, iCloud) vinculados a la cuenta personal del empleado. Si un trabajador fotografía el DNI de un cliente para el registro y esa imagen se sube automáticamente a su nube personal, los datos del cliente quedan fuera del control de la empresa y en un entorno que probablemente no cumple con el RGPD.
- **Mensajería instantánea como canal de trabajo:** Es muy habitual que los equipos de trabajo se comuniquen por WhatsApp o Telegram para coordinarse: turnos, incidencias, datos de reservas, incluso fotos de pasaportes de clientes. Estas aplicaciones no están pensadas para gestionar información sensible, no ofrecen control empresarial sobre los datos y, si un empleado pierde el móvil o deja la empresa, toda esa información se va con él.
- **Dispositivos sin cifrar:** Muchos móviles y tablets, especialmente los Android más antiguos o los que se compran como dispositivos "de trabajo baratos", no tienen activado el cifrado del almacenamiento. Esto significa que si alguien accede físicamente al dispositivo (un robo, una pérdida, incluso un técnico de reparación), puede extraer toda la información almacenada sin necesidad de conocer el PIN o la contraseña.
- **Actualizaciones del sistema operativo ignoradas:** Los empleados tienden a posponer las actualizaciones del móvil porque tardan, consumen batería o cambian la interfaz. Pero cada actualización que se ignora deja abiertas vulnerabilidades de seguridad que los atacantes conocen y explotan activamente. Un móvil con un sistema operativo desactualizado es una puerta abierta.

3.2. AMENAZAS EN COMPUTADORAS Y SERVIDORES

Amenaza	Explicación	Ejemplo / impacto
Ransomware	Es una de las amenazas más graves y frecuentes. Un programa malicioso cifra todos los archivos de tu ordenador o servidor y muestra un mensaje pidiendo un rescate, normalmente entre miles y decenas de miles de euros en criptomonedas, para darte la clave que los descifra.	Una mañana enciendes el ordenador de recepción y aparece un mensaje en rojo diciendo que todos tus datos están bloqueados. No puedes acceder a las reservas, ni a la facturación, ni al historial de clientes.
Ataques de fuerza bruta	Son intentos automáticos y masivos de adivinar contraseñas. Un programa prueba miles de combinaciones por segundo hasta dar con la correcta.	Afectan especialmente a paneles de administración web, correos electrónicos y accesos remotos que usan contraseñas débiles como “123456”, “admin” o el nombre del hotel.

Spyware	Es un programa espía que se instala sin que lo sepas y monitoriza todo lo que haces: qué páginas visitas, qué datos introduces y qué correos envías.	Captura contraseñas, datos bancarios y otra información sensible, y la envía a terceros.
Explotación de vulnerabilidades en software desactualizado	Si tu web está hecha con WordPress, Joomla u otro gestor de contenido y no lo actualizas regularmente, los atacantes pueden aprovechar fallos de seguridad conocidos para tomar el control de la página.	Lo mismo ocurre con sistemas operativos y programas que no reciben actualizaciones.
Ataques a la cadena de suministro	Los atacantes no siempre van directamente a por ti: a veces comprometen un software o servicio que tú utilizas.	Un plugin de reservas instalado en tu web tiene una vulnerabilidad y los atacantes la aprovechan para interceptar los datos de pago que introducen tus clientes al reservar.
Correo electrónico corporativo comprometido (BEC)	Los atacantes investigan cómo funciona tu negocio, quién es el gerente y quién se encarga de los pagos. Después envían un correo que parece venir de un jefe o proveedor real, pidiendo una transferencia urgente o un cambio de cuenta bancaria.	No es un correo masivo genérico: está personalizado y redactado para parecer completamente legítimo. En el sector turístico, donde se manejan pagos constantes a proveedores, este tipo de ataque es cada vez más frecuente.
Uso de software pirata o sin licencia	Para ahorrar costes, algunas empresas instalan programas sin licencia o descargados de fuentes no oficiales. Estos programas suelen venir con malware integrado que pasa desapercibido durante meses.	Puede recopilar información, contraseñas y datos bancarios. Además, al no tener licencia, no recibe actualizaciones de seguridad, lo que lo hace doblemente vulnerable.
Acceso remoto mal configurado	Desde la pandemia, muchos negocios habilitaron accesos remotos como Escritorio Remoto, TeamViewer o AnyDesk para que los empleados pudieran trabajar desde casa.	Si estos accesos siguen activos con contraseñas débiles, sin MFA o expuestos directamente a internet, son una de las vías de entrada más utilizadas por los atacantes para instalar ransomware.
Amenazas internas	No todas las amenazas vienen de fuera. También pueden venir de empleados descontentos o negligentes.	Un empleado que se marcha enfadado puede llevarse una copia de la base de datos de clientes en un USB, o un trabajador puede compartir su contraseña con un compañero por comodidad. La falta de control de accesos y de registros de actividad facilita que estos incidentes pasen desapercibidos.
Robo de credenciales por filtraciones previas	Cuando un servicio externo sufre una brecha de datos, como LinkedIn, Adobe u otros, las contraseñas de los usuarios pueden quedar expuestas en internet.	Si un empleado usaba la misma contraseña para ese servicio y para el correo corporativo o el sistema de reservas, los atacantes la probarán automáticamente en miles de sitios. Este

		ataque se llama credential stuffing y es extremadamente habitual.
Macros y archivos adjuntos maliciosos	Los atacantes envían documentos de Word o Excel con macros ocultas que, al activarse, descargan e instalan malware en el ordenador.	Suelen disfrazarse como facturas, presupuestos o confirmaciones de reserva. Basta con que un empleado abra el archivo y haga clic en "Habilitar contenido" para que el ataque se ejecute.
Minería de criptomonedas oculta — cryptojacking	Los atacantes instalan programas que utilizan la capacidad de procesamiento de tus ordenadores o servidores para minar criptomonedas sin que lo sepas.	No roban datos directamente, pero ralentizan los equipos, aumentan el consumo eléctrico y acortan la vida útil del hardware. Muchos negocios lo sufren durante meses sin darse cuenta, atribuyendo la lentitud a que "los ordenadores son viejos".

3.3. AMENAZAS EN REDES Y DISPOSITIVOS DE IOT

Los dispositivos IoT (Internet de las Cosas) son todos aquellos aparatos conectados a internet que no son ordenadores ni móviles: cámaras de seguridad, cerraduras inteligentes, termostatos, sensores de humo, sistemas de iluminación automatizada, terminales de punto de venta (TPV), etc. Son cada vez más habituales en hoteles y restaurantes, pero a menudo se instalan sin prestar atención a su seguridad.

- **Accesos No Autorizados:** Muchos dispositivos IoT se instalan con el usuario y contraseña de fábrica ("admin/admin" o "admin/1234") y nadie los cambia. Un atacante que conozca estas credenciales por defecto puede acceder a tus cámaras de seguridad, abrir cerraduras inteligentes o entrar en tu red a través de cualquier dispositivo conectado.

- **Ataques de Denegación de Servicio (DDoS):** Los dispositivos IoT mal protegidos pueden ser "secuestrados" por atacantes para formar parte de redes de miles de dispositivos (llamadas "botnets") que se utilizan para lanzar ataques masivos contra otros objetivos. Además, tu propia red puede ser víctima de este tipo de ataques, dejando sin servicio tu Wi-Fi, tu web o tus sistemas de reservas.

- **Inseguridad en el Firmware:** El firmware es el software interno que hace funcionar un dispositivo IoT. Muchos fabricantes, especialmente de gama baja, no publican actualizaciones de seguridad o dejan de dar soporte al producto al poco tiempo. Si el firmware de tus cámaras o sensores tiene un fallo de seguridad conocido y no hay actualización disponible, esos dispositivos se convierten en un punto de entrada permanente para los atacantes.

- **Interceptación de Comunicaciones:** Algunos dispositivos IoT transmiten datos sin cifrar. Esto significa que un atacante podría interceptar la información que envían: datos de los sensores, registros de quién abre qué puerta, patrones de ocupación del establecimiento, etc.

- **Amenazas Físicas a Dispositivos Expuestos:** A diferencia de un servidor guardado en una sala cerrada, muchos dispositivos IoT están instalados en zonas accesibles al público:

cámaras en el vestíbulo, sensores en la terraza, terminales en la barra. Un atacante con acceso físico podría manipularlos, resetearlos o extraer información directamente.

- **Dispositivos IoT abandonados en la red:** Con el tiempo, es habitual que se instalen dispositivos nuevos sin retirar los antiguos. Una cámara vieja que ya no se usa pero sigue conectada a la red, un sensor de temperatura que se desconectó pero nunca se eliminó del sistema, un router antiguo que se dejó enchufado en un armario. Estos dispositivos olvidados siguen siendo accesibles para los atacantes y, al no recibir ningún tipo de mantenimiento, se convierten en puntos de entrada silenciosos.

- **Redes de invitados sin aislamiento real:** Muchos negocios creen que tienen la red de clientes separada de la interna, pero en realidad ambas comparten el mismo router o punto de acceso sin una segmentación efectiva. Un atacante conectado a la "red de invitados" puede, en estos casos, alcanzar los sistemas internos del negocio. La separación debe ser real a nivel de configuración del router, no basta con crear dos nombres de Wi-Fi diferentes.

- **Ataques a sistemas de climatización y domótica:** Los sistemas de climatización inteligente, persianas automatizadas, iluminación conectada y otros elementos de domótica que se instalan en hoteles y restaurantes modernos funcionan a través de la red. Si un atacante accede a estos sistemas, puede manipular la temperatura de las habitaciones, activar alarmas, apagar luces o causar molestias que afecten directamente a la experiencia del cliente y a la operativa del negocio.

- **Suplantación de puntos de acceso Wi-Fi (Evil Twin):** Un atacante puede crear una red Wi-Fi con el mismo nombre que la de tu establecimiento (por ejemplo, "Hotel_Playa_WiFi"). Los huéspedes y empleados se conectan creyendo que es la red legítima, y todo lo que envían y reciben pasa por el dispositivo del atacante: correos, contraseñas, datos de tarjetas. Esta técnica es especialmente efectiva en hoteles y espacios públicos donde los usuarios esperan encontrar Wi-Fi abierta.

- **Vulnerabilidades en TPVs (Terminales de Punto de Venta):** Los datáfonos y terminales de cobro también son dispositivos conectados que pueden ser atacados. Si el software del TPV no está actualizado o si el dispositivo se conecta a una red insegura, un atacante puede interceptar los datos de las tarjetas que pasan por él. En restaurantes y hoteles, donde se procesan decenas o cientos de transacciones al día, el impacto puede ser masivo.

- **Escuchas a través de dispositivos con micrófono:** Asistentes de voz, altavoces inteligentes, intercomunicadores y algunos sistemas de videoconferencia instalados en salas de reuniones o zonas comunes tienen micrófonos permanentemente activos. Si estos dispositivos están comprometidos o mal configurados, pueden utilizarse para espiar conversaciones privadas, negociaciones comerciales o datos sensibles que se comenten en voz alta.

- **Falta de segmentación entre dispositivos IoT:** Incluso cuando la red de invitados está separada, es frecuente que todos los dispositivos IoT (cámaras, cerraduras, sensores, TVs inteligentes) compartan la misma red entre sí y con los ordenadores de gestión. Si un atacante compromete una Smart TV del vestíbulo, puede saltar desde ahí a las cámaras de seguridad o al sistema de cerraduras electrónicas. Cada tipo de dispositivo debería estar en su propia subred aislada.

4. MEDIDAS DE CIBERSEGURIDAD APLICABLES A DIFERENTES DISPOSITIVOS

Ahora que conoces las principales amenazas, veamos qué puedes hacer para proteger tu negocio. Las medidas que se detallan a continuación están pensadas para ser aplicables por cualquier PYME del sector turístico, sin necesidad de ser un experto en tecnología. Muchas de ellas son sencillas, gratuitas o de bajo coste, y pueden marcar la diferencia entre ser víctima de un ataque o evitarlo.

4.1. DISPOSITIVOS MÓVILES

Los móviles y tablets que usas en tu negocio necesitan una protección específica. Estas son las medidas más importantes:

Medida	Descripción
Actualización regular	Mantén el sistema operativo (Android o iOS) y todas las aplicaciones siempre actualizadas. Las actualizaciones corrigen fallos de seguridad que los atacantes aprovechan. Activa las actualizaciones automáticas para no tener que acordarte. Comprueba periódicamente que todos los dispositivos de la empresa están al día.
Uso de aplicaciones seguras	Descarga aplicaciones únicamente desde Google Play Store o Apple App Store. Nunca instales apps desde enlaces que te lleguen por correo, SMS o WhatsApp. Antes de instalar una app, revisa los permisos que pide: si una app de linterna te pide acceso a tus contactos y al micrófono, desconfía.
VPN obligatoria	Cuando un empleado se conecte a una red Wi-Fi que no sea la del establecimiento (por ejemplo, en un desplazamiento o desde casa), debe usar siempre una VPN. La VPN cifra toda la comunicación, impidiendo que alguien pueda espiar los datos que se envían y reciben. Existen soluciones VPN sencillas y económicas para empresas.
Gestión centralizada (MDM)	Si tu empresa proporciona móviles a los empleados, plantéate usar un sistema de gestión de dispositivos móviles (MDM). Permite aplicar normas de seguridad desde un único punto: forzar el uso de PIN, cifrar el dispositivo, bloquear apps no autorizadas y, lo más importante, borrar el dispositivo a distancia si se pierde o lo roban.
Separación de datos personales y corporativos	Si los empleados usan sus propios móviles para trabajar, lo ideal es que los datos de la empresa estén en un "contenedor" separado dentro del teléfono. Así, la información corporativa queda protegida incluso si el empleado instala apps personales poco seguras o pierde el dispositivo
Bloqueo automático de pantalla	Configura todos los dispositivos para que se bloqueen automáticamente tras un máximo de 2 minutos sin uso, y que requieran PIN, huella dactilar o reconocimiento facial para desbloquearse. Es una medida muy simple que evita que alguien pueda acceder al móvil si se deja olvidado en una mesa.

4.2. COMPUTADORAS Y SERVIDORES

Los ordenadores y servidores son el núcleo de la operativa. Protegerlos adecuadamente es fundamental:

Medida	Descripción
Software antimalware	Instala un programa antimalware (antivirus) de calidad en todos los ordenadores y mantenlo actualizado. Debe tener protección en tiempo real (que detecte amenazas al momento, no solo cuando tú lanzas un análisis). Existen opciones gratuitas aceptables, pero para un negocio se recomienda una solución profesional.
Copias de seguridad regulares	Haz copias de seguridad de todos los datos importantes con regularidad. La regla de oro es la regla 3-2-1: tres copias de tus datos, en dos soportes diferentes (por ejemplo, un disco externo y la nube), con una copia fuera del local. Y lo más importante: comprueba periódicamente que las copias funcionan y que puedes restaurar los datos a partir de ellas..
Actualizaciones y parches	Mantén actualizados todos los programas: el sistema operativo (Windows, macOS, Linux), los navegadores, el programa de gestión, el antivirus, etc. Cada actualización corrige fallos de seguridad. Establece un día a la semana o al mes para revisar que todo está al día. Si usas sistemas antiguos que ya no reciben actualizaciones, plantéate seriamente reemplazarlos.
Control de acceso basado en roles	No todos los empleados necesitan acceder a toda la información. El recepcionista necesita acceder a las reservas, pero no a la contabilidad completa. Configura los permisos de cada usuario para que solo pueda ver y modificar lo que necesita para su trabajo. Y cuando un empleado deja la empresa, revoca sus accesos inmediatamente.
Cifrado de discos y datos sensibles	Activa el cifrado del disco duro en todos los portátiles (BitLocker en Windows, FileVault en macOS). De esta forma, si un portátil se pierde o lo roban, los datos que contiene serán ilegibles para quien no tenga la contraseña. Para datos especialmente sensibles (base de datos de clientes, información financiera), usa cifrado adicional.
Monitorización y registro de actividad	Activa los registros (logs) de acceso en tus sistemas: quién se conectó, cuándo, desde dónde y qué hizo. No hace falta revisarlos cada día, pero si alguna vez ocurre un incidente, estos registros serán imprescindibles para entender qué pasó y cómo solucionarlo. Muchos sistemas de gestión traen esta funcionalidad integrada.

4.3. REDES Y DISPOSITIVOS DE IOT

La red es la columna vertebral de tu infraestructura digital, y los dispositivos IoT son cada vez más habituales. Protegerlos correctamente es esencial:

Medida	Descripción
Red Wi-Fi segura	Configura tu Wi-Fi con el cifrado más fuerte disponible (WPA3, o al menos WPA2). Cambia la contraseña que viene de fábrica en el router y en todos los puntos de acceso. Para la red interna (la que usa el personal), oculta el nombre de la red (SSID) para que no sea visible públicamente. Desactiva cualquier función de administración remota que no necesites.
Monitoreo de tráfico	Usa un firewall para controlar qué entra y sale de tu red. Los firewalls modernos (llamados NGFW) son capaces de detectar patrones sospechosos en tiempo real. Si tu proveedor de internet o tu empresa de mantenimiento informático ofrece este servicio, es una inversión que merece la pena.
Separar redes	Esta es una de las medidas más efectivas y no tiene por qué ser complicada. Crea al menos dos redes separadas: una para el personal (donde están los sistemas de gestión, la facturación, los datos de clientes) y otra para los clientes (la Wi-Fi del hotel o restaurante). Así, aunque un huésped conecte un dispositivo infectado a tu Wi-Fi, no podrá acceder a tus sistemas internos. Si además tienes dispositivos IoT (cámaras, sensores), ponlos en una tercera red separada.
Inventario y control de dispositivos IoT	Haz una lista de todos los dispositivos conectados a tu red: ordenadores, móviles, impresoras, cámaras, sensores, cerraduras, TPVs, etc. Anota para cada uno su ubicación, modelo, y quién es responsable de mantenerlo. Si hay algún dispositivo que ya no recibe actualizaciones del fabricante, valora desconectarlo o sustituirlo: es un riesgo permanente.
Cambio de credenciales por defecto	Antes de conectar cualquier dispositivo nuevo a la red (router, cámara, TPV, cerradura inteligente), cambia el usuario y contraseña que trae de fábrica. Usa contraseñas diferentes para cada dispositivo. Las credenciales por defecto de la mayoría de dispositivos son públicas y cualquier atacante las conoce.
Actualizaciones de firmware	El firmware es el software interno de los dispositivos IoT. Igual que actualizas el sistema operativo de tu ordenador, revisa periódicamente si hay actualizaciones disponibles para tus cámaras, routers, cerraduras inteligentes, etc. Si el fabricante deja de publicar actualizaciones, plantéate sustituir el dispositivo por uno que sí las reciba.

4.4. POLÍTICAS GENERALES DE SEGURIDAD

Más allá de las medidas técnicas, hay una serie de normas y prácticas organizativas que toda empresa del sector turístico debería implantar. No requieren grandes inversiones, pero sí compromiso y constancia:

Políticas generales de seguridad
Medidas transversales aplicables a toda la organización

Contraseñas fuertes

Establece normas claras sobre contraseñas en tu empresa. Una buena contraseña debe tener al menos 12 caracteres y mezclar letras mayúsculas, minúsculas, números y símbolos. Nunca debe usarse la misma contraseña en dos servicios diferentes, ni basarse en información fácil de adivinar (nombre del hotel, fecha de inauguración, "123456"). Lo ideal es usar un gestor de contraseñas: es una aplicación que genera contraseñas seguras y las guarda cifradas, de forma que solo tienes que recordar una contraseña maestra.

Autenticación multifactor (MFA)

Activa la verificación en dos pasos en todos los servicios que lo permitan: correo electrónico, plataformas de reservas, cuentas bancarias online, panel de administración de la web, redes sociales del negocio. En la práctica, esto significa que además de la contraseña, necesitarás un código que llega a tu móvil o que se genera en una app como Google Authenticator o Microsoft Authenticator. Es uno de los pasos más efectivos que puedes dar para proteger tus cuentas.

Concienciación y formación

El eslabón más débil de la cadena de seguridad suele ser la persona, no la tecnología. Forma a todos tus empleados (incluido el personal temporal de temporada) en los conceptos básicos de ciberseguridad: cómo identificar un correo de phishing, por qué no deben instalar apps de fuentes desconocidas, qué hacer si sospechan que algo no va bien, a quién deben avisar. No hace falta que sean sesiones largas ni técnicas: una charla práctica de 30 minutos con ejemplos reales puede marcar la diferencia. Realiza estas sesiones al menos una vez al año, y siempre que se incorpore personal nuevo.

Plan de respuesta ante incidentes

Ten preparado un plan para saber qué hacer si ocurre un incidente de seguridad. No tiene que ser un documento técnico complejo: lo esencial es que defina quién hace qué, en qué orden y a quién se avisa. Por ejemplo: si un empleado detecta un correo sospechoso, ¿a quién informa? Si el sistema de reservas se bloquea de repente, ¿cuál es el primer paso? ¿Quién contacta con la empresa de mantenimiento informático? ¿Quién notifica a la Agencia de Protección de Datos si hay una brecha? Tener esto definido de antemano ahorra tiempo y reduce el impacto del incidente.

Política de uso aceptable

Define por escrito las normas de uso de los dispositivos y sistemas del negocio: qué se puede y qué no se puede hacer con los ordenadores de la empresa, si se permite el uso personal del correo corporativo, si se pueden instalar programas sin autorización, cuáles son las normas sobre el uso de USB, qué ocurre si un empleado no cumple estas normas. Que todo el personal lo conozca y lo firme al incorporarse.

Gestión de proveedores y terceros

Si contratas servicios tecnológicos (mantenimiento informático, diseño web, pasarela de pago, software de gestión), asegúrate de que tus proveedores también cuidan la seguridad. Incluye cláusulas de seguridad y protección de datos en los contratos. Pregunta qué medidas aplican para proteger tus datos. Si un proveedor sufre un ataque y tus datos se ven afectados, la responsabilidad ante tus clientes sigue siendo tuya.