

Seguridad Digital para Restaurantes y Bares

Una guía práctica para proteger tu negocio de hostelería en la era digital

 **por Gestion Implantaciones Empresas**



Activos digitales a proteger



TPVs y pagos

Terminales de venta
vulnerables a ataques



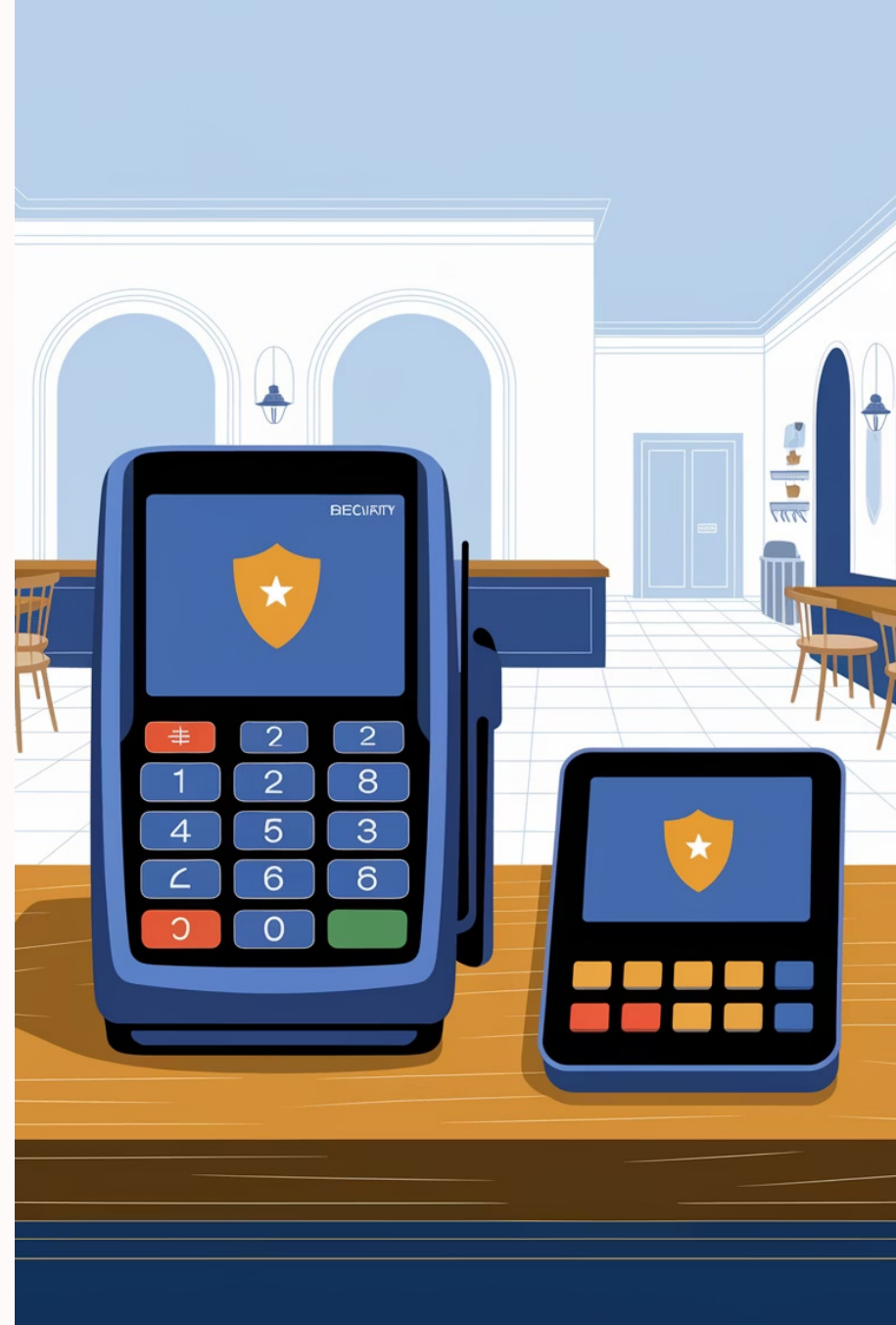
Sistema de reservas

Datos de clientes en
riesgo



Redes WiFi

Acceso a sistemas
internos



Amenazas comunes



Malware

Software malicioso que compromete sistemas



Phishing

Suplantación para robar credenciales



Robo de datos

Información de clientes y pagos



Protección de TPVs



Actualizar software

Aplicar parches de seguridad regularmente



TPVs certificados

Cumplir estándares PCI-DSS



Acceso restringido

Limitar quién puede usar terminales



Seguridad en reservas online

Proveedores confiables

Elegir plataformas con certificaciones de seguridad

Datos mínimos

Recoger solo información esencial

Eliminar periódicamente

No almacenar datos antiguos innecesarios

Redes WiFi seguras

Red separada para clientes

Aislar del sistema principal del negocio

Contraseñas robustas

Cambiar claves mensualmente

Cifrado WPA3

Evitar redes abiertas sin protección



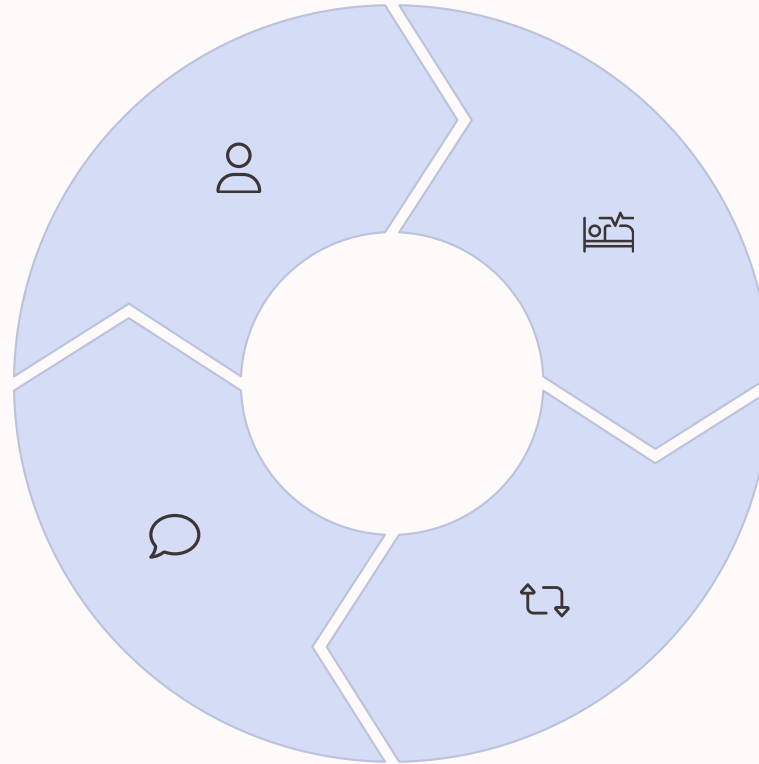
Formación del personal

Reconocer amenazas

Identificar intentos de phishing

Comunicación

Reportar incidentes sospechosos



Protocolos claros

Establecer procedimientos de seguridad

Actualización continua

Formación periódica sobre nuevas amenazas

Plan de acción inmediato

1

Auditoría

Evaluar vulnerabilidades actuales

2

Actualizar

Software y contraseñas

3

Formar

Capacitar al personal

[Descargar temario](#)

[Solicitar información](#)

