

Activos Críticos

Activo	Clasificación
Servidor de base de datos	Crítico (Contiene datos de clientes y tarjetas de crédito)
Sistema de pagos en línea	Crítico (Permite procesar transacciones económicas)
Copias de seguridad (Backups)	Crítico (Aseguran recuperación ante incidentes)

Amenazas Relevantes

Tipo de Amenaza	Descripción
Cibernética	Intentos de acceso no autorizado (phishing, fuerza bruta, malware)
Física	Robo o daño a servidores en las instalaciones físicas

Vulnerabilidades Potenciales

- Contraseñas débiles o compartidas entre usuarios.
- Servidor sin actualizaciones de seguridad críticas.

Controles de Seguridad Propuestos

Tipo de Control	Descripción
Técnico	Configuración de firewall y uso de autenticación multifactor (MFA)
Administrativo	Política de contraseñas robustas y capacitación en seguridad para empleados

Relación con los Principios de la CIA

Principio	Relación con amenazas y controles
Confidencialidad	Las amenazas cibernéticas como el phishing comprometen la confidencialidad; MFA y firewall la protegen.
Integridad	Alteraciones malintencionadas en datos podrían ocurrir si hay vulnerabilidades; los backups y las políticas de cambio seguro preservan la integridad.
Disponibilidad	Una intrusión o daño físico puede dejar los sistemas fuera de servicio; los backups y medidas físicas (cerraduras, cámaras) aseguran la disponibilidad.