



INTERNET DE LAS COSAS

RIESGOS DE EXPOSICIÓN DE DATOS EN IOT

RIESGOS DE EXPOSICIÓN DE DATOS EN IOT

Los riesgos de exposición de datos en ecosistemas IoT tienen características particulares debido al volumen masivo de información personal u operacional que estos sistemas recolectan, procesan y transmiten de forma continua. Los dispositivos IoT recopilan datos altamente sensibles como:

- Información biométrica.
- Patrones de comportamiento.
- Ubicación geográfica precisa.
- Actividades personales y profesionales.

Estos datos son especialmente vulnerables por factores como:

- Controles de privacidad inadecuados.
- Cifrado débil o inexistente.
- Políticas de retención de datos inadecuadas.

Arquitectura distribuida y puntos de vulnerabilidad

La arquitectura distribuida de sistemas IoT amplifica los riesgos al crear múltiples puntos de exposición a lo largo del flujo de datos, desde la captura hasta el análisis. Según Llanea González (2018), los datos transitan por:

Tabla 1. Riesgos de exposición de datos en la arquitectura IoT

Componente	Riesgo
Dispositivos de borde	Recolección sin cifrado o autenticación
Pasarelas y redes	Transmisión insegura de datos sensibles
Plataformas en la nube	Acceso indebido por falta de segmentación de permisos
Sistemas de análisis	Almacenamiento y correlación sin anonimización efectiva

La falta de cifrado extremo a extremo y políticas de acceso inconsistentes entre componentes facilitan accesos no autorizados. Además, la participación de múltiples organizaciones diluye la responsabilidad, creando vacíos de supervisión en la protección de los datos.

Consideraciones regulatorias y técnicas

En el desarrollo de aplicaciones IoT, se deben tener en cuenta normativas como el GDPR y leyes locales de protección de datos. Para cumplir con estas exigencias legales y éticas, se recomienda:

- Privacidad por diseño
 - Minimización de datos

- Seudonimización
- Consentimiento segmentado
- Técnicas avanzadas
 - Anonimización de datos
 - Privacidad diferencial (para evitar reidentificación mediante correlaciones)

Estas medidas son esenciales, ya que incluso datos aparentemente anónimos pueden ser reidentificados al correlacionarse con otras fuentes públicas.

Impacto en ingeniería de software

Los riesgos de exposición de datos influyen significativamente en el diseño de sistemas que manejan información sensible. Un caso crítico se presenta en sistemas de hogar inteligente, donde dispositivos como cámaras, asistentes de voz y sensores de ocupación recolectan información sobre:

- Rutinas familiares
- Conversaciones privadas
- Patrones de actividad

Una exposición no autorizada podría derivar en:

- Robo físico (identificación de periodos de ausencia)
- Chantaje (acceso a conversaciones privadas)
- Acecho (seguimiento de movimientos)

Esto demuestra que los riesgos de datos en IoT trascienden la privacidad digital, generando consecuencias físicas y personales reales.

Aplicación práctica


Para evaluar estos riesgos, se realiza un análisis exhaustivo del flujo de datos:

Tabla 2. Técnicas para evaluación de riesgos de exposición de datos en IoT

Elemento	Descripción
Mapeo de flujo de datos sensibles	Identificación de puntos de captura, almacenamiento, transmisión y análisis de datos confidenciales
Análisis de APIs web	<ul style="list-style-type: none"> ● Herramienta: OWASP ZAP ● Comando: <code>zap-baseline.py -t https://iot-api.ejemplo.com</code> - Objetivo: detectar puntos finales sin autenticación adecuada
Monitoreo de tráfico de red	<ul style="list-style-type: none"> ● Herramienta: tcpdump ● Comando: <code>`tcpdump -i any -A 'port 80 or port 8080'</code>
Prevención de pérdida de datos	Aplicación de expresiones regulares para identificar patrones sensibles en registros y transmisiones

El resultado esperado incluye identificación de APIs que exponen información personal identificable sin protección, comunicaciones que transmiten datos sensibles en claro, y sistemas de registro que inadvertidamente capturan información confidencial, proporcionando una línea base para implementar controles de protección de datos apropiados.

Bibliografía

-  Llanea González, P. (2018). Seguridad y responsabilidad en la internet de las cosas (IoT): (ed.). LA LEY Soluciones Legales S.A.
<https://elibro.net/es/ereader/tecnologicadeloriente/58379?page=1>