Alineada ENISA

ENISA (Agencia de la Unión Europea para la Ciberseguridad) taxonomía de dispositivos IoT para hogares

|  |  |
| --- | --- |
| **Categoría** | **Ejemplos de dispositivos** |
| Seguridad | Cámaras de seguridad  Sistemas de alarma  Sensores de movimiento  Sensores de presencia  Detectores de humo  Detectores de monóxido de carbono  Cerraduras |
| Entretenimiento | Altavoces inteligentes  Sistemas de cine en casa  Televisores inteligentes  Consolas de videojuegos  Streaming de contenido en línea  Reproductores de medios |
| Iluminación | Bombillas  Sistemas de iluminación conectados  Interruptores de luz  Luces de seguridad exteriores |
| Climatización | Termostatos  Ventiladores  Aires acondicionados  Sistemas de calefacción |
| Electrodomésticos inteligentes | Frigoríficos  Hornos  Cafeteras  Básculas de cocina |
| Limpieza y mantenimiento | Aspiradoras robóticas  Lavadoras  Secadoras  Sistemas de purificación de aire |
| Salud y cuidado personal | Monitores de actividad física  Medidores de glucosa en sangre  Monitores de presión arterial  Monitores de sueño  Básculas |
| Dispositivos de cómputo y comunicación | Tabletas  Teléfonos  Relojes  Ordenadores portátiles  Routers |

Características buenas para la seguridad

1. Autenticación fuerte de usuario: Requerir una autenticación sólida, como la autenticación de dos factores, para acceder al dispositivo.
2. Actualizaciones regulares de firmware: Actualizaciones regulares para corregir vulnerabilidades de seguridad y problemas conocidos.
3. Cifrado de datos: La encriptación de datos transmitidos y almacenados, lo que dificulta su acceso no autorizado.
4. Control de acceso basado en roles: Un sistema de control de acceso que limita la capacidad de cada usuario para acceder y controlar el dispositivo.
5. Notificaciones de seguridad en tiempo real: Alertas en tiempo real de cualquier actividad sospechosa o comportamiento anormal del dispositivo.
6. Monitoreo de integridad del sistema: Supervisión continua de la salud y el rendimiento del sistema para detectar y solucionar problemas de seguridad.
7. Detección de intrusiones: La capacidad de detectar y responder a intentos de intrusión y ataques maliciosos.
8. Compatibilidad con protocolos de seguridad estándar: Soporte de protocolos de seguridad estándar, como SSL/TLS y AES, para proteger la comunicación de red.
9. Desactivación de funciones innecesarias: Desactivar todas las funciones que no sean necesarias para minimizar el riesgo de ataques a través de estas funciones.
10. Registro de auditoría: Mantener un registro detallado de las actividades del dispositivo para ayudar a detectar y solucionar problemas de seguridad.

Características malas para la seguridad

1. Contraseñas predeterminadas débiles: Contraseñas que son fáciles de adivinar o que no se pueden cambiar fácilmente.
2. Comunicaciones no cifradas: La falta de encriptación de los datos transmitidos entre el dispositivo y otros dispositivos o servidores.
3. Vulnerabilidades conocidas no corregidas: No solucionar vulnerabilidades de seguridad conocidas en el firmware del dispositivo.
4. Permisos de usuario inadecuados: No tener un control de acceso adecuado que limite el acceso y control del dispositivo según el rol del usuario.
5. Falta de actualizaciones de seguridad: No proporcionar actualizaciones regulares para corregir vulnerabilidades de seguridad y problemas conocidos.
6. Exposición de información personal del usuario: La falta de protección de los datos personales del usuario almacenados en el dispositivo o transmitidos a través de él.
7. Puntos de entrada no seguros: Puntos de entrada al sistema que son vulnerables a ataques maliciosos, como puertos abiertos o interfaces web mal protegidas.
8. Falta de autenticación de usuario: Permitir que cualquier persona pueda acceder y controlar el dispositivo sin autenticación adecuada.
9. Aplicaciones de terceros inseguras: La falta de seguridad en las aplicaciones de terceros que se utilizan en conjunción con el dispositivo.
10. Configuraciones inseguras: La configuración incorrecta del dispositivo o de su software, que puede exponerlo a vulnerabilidades y ataques maliciosos.

Características buenas para la sostenibilidad:

1. Eficiencia energética: Los dispositivos IoT que son energéticamente eficientes pueden ayudar a reducir el consumo de energía y, por lo tanto, reducir la huella de carbono.
2. Diseño modular: Los dispositivos IoT que están diseñados con módulos intercambiables y actualizables pueden extender su vida útil y reducir la cantidad de residuos electrónicos.
3. Reciclabilidad: Los dispositivos IoT que son reciclables o están diseñados para su desmontaje y reciclaje pueden ayudar a reducir la cantidad de residuos electrónicos.
4. Uso de materiales sostenibles: Los dispositivos IoT que utilizan materiales sostenibles, como plásticos reciclados o materiales de origen biológico, pueden reducir su impacto ambiental.
5. Monitoreo ambiental: Los dispositivos IoT que monitorean el medio ambiente pueden ayudar a identificar y abordar problemas ambientales.
6. Tecnologías de bajo consumo: Las tecnologías de bajo consumo, como Bluetooth de baja energía (BLE) o Zigbee, pueden ayudar a reducir el consumo de energía de los dispositivos IoT.
7. Compatibilidad con energías renovables: Los dispositivos IoT que pueden funcionar con energías renovables, como la energía solar o eólica, pueden ayudar a reducir la huella de carbono.
8. Ciclo de vida prolongado: Los dispositivos IoT que están diseñados para durar más tiempo pueden reducir la cantidad de residuos electrónicos y la necesidad de fabricar nuevos dispositivos con frecuencia.

Características malas para la sostenibilidad:

1. Uso de materiales tóxicos: Los dispositivos IoT que utilizan materiales tóxicos, como mercurio o plomo, pueden causar daños ambientales y de salud.
2. Consumo energético elevado: Los dispositivos IoT que consumen mucha energía pueden contribuir a un mayor uso de combustibles fósiles y, por lo tanto, aumentar la huella de carbono.
3. Desperdicio de energía: Los dispositivos IoT que no tienen un modo de suspensión o que no pueden apagarse pueden desperdiciar energía innecesariamente.
4. Vida útil corta: Los dispositivos IoT que están diseñados para durar poco tiempo pueden aumentar la cantidad de residuos electrónicos.
5. Materiales no reciclables: Los dispositivos IoT que utilizan materiales no reciclables pueden contribuir a la acumulación de residuos electrónicos.
6. Monitoreo invasivo: Los dispositivos IoT que monitorean la privacidad del usuario o recopilan datos innecesarios pueden ser perjudiciales para la privacidad y la seguridad del usuario.
7. Compatibilidad limitada con energías renovables: Los dispositivos IoT que solo pueden funcionar con energías no renovables pueden ser perjudiciales para el medio ambiente.
8. Falta de transparencia en la cadena de suministro: La falta de transparencia en la cadena de suministro puede dificultar la evaluación de la sostenibilidad de los dispositivos IoT.

Ejemplos