Aprendiendo Arduino

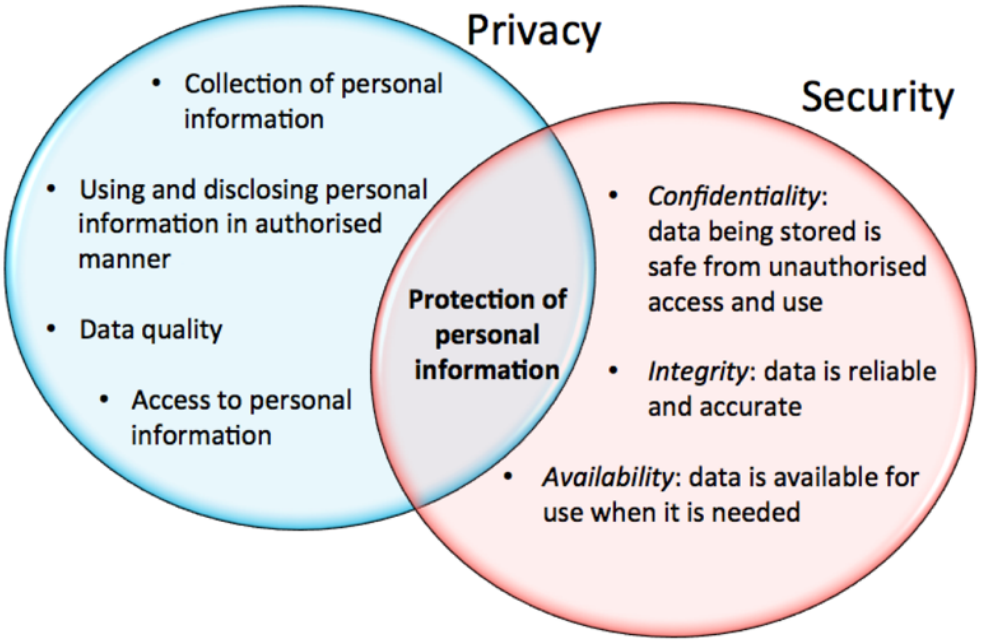
Aprendiendo a manejar Arduino en profundidad

Conceptos Básicos de Ciberseguridad

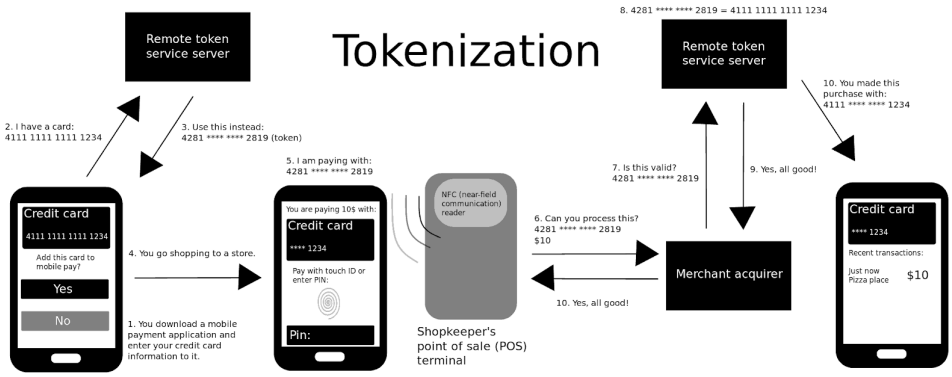
La seguridad y la privacidad de los datos son los conceptos principales de la protección de datos.

La **seguridad de los datos** es la prevención de accesos no autorizados a conjuntos de datos. Dichos accesos son los que desembocan en vulneraciones o ataques, Para lograr la seguridad, las organizaciones utilizan herramientas y soluciones tecnológicas como firewalls, autenticación de usuarios, limitaciones en la red y prácticas de seguridad adaptadas a cada entorno u organización. También pueden incluirse los procesos de encriptación y tokenización de manera a que no pueda ser posible la lectura de los datos en fases clave del tránsito de los mismos, por parte de los cibercriminales.

La **privacidad de los datos** se encarga de asegurar que los datos; ya sean procesados, almacenados o transmitidos sean consumidos de acuerdo a las regulaciones y normas. Así también, que estos datos puedan ser manipulados bajo el consentimiento de quien sea dueño de los mismos.



Tokenización: https://en.wikipedia.org/wiki/Tokenization_(data_security)



Los pilares de la seguridad son:

- **Confidencialidad**
- **Integridad**
- **Disponibilidad**

Confidencialidad: Cualidad de la información para no ser divulgada a personas o sistemas no autorizados. Se trata básicamente de la propiedad por la que esa información sólo resultará accesible con la debida y comprobada autorización.

El objetivo de la confidencialidad es, prevenir la divulgación no autorizada de la información sobre nuestra organización.

Integridad: Cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros. Esta integridad se pierde cuando la información se modifica o cuando parte de ella se elimina. Una garantía para mantenerla intacta es la firma digital.

El objetivo de la integridad es prevenir modificaciones no autorizadas de la información.

Disponibilidad: Aquella información a la que podemos acceder cuando la necesitamos a través de los canales adecuados siguiendo los procesos correctos.

El objetivo de la disponibilidad es prevenir interrupciones no autorizadas de los recursos informáticos.

Más información:

- https://www.redeszone.net/tutoriales/dominios/proteger-dns-teletrabajo-seguridad/
- https://blogs.deusto.es/master-informatica/privacidad-vs-seguridad/
- https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

Mejorar seguridad en entornos IoT: https://www.arsys.es/blog/seguridad-entornos-iot/

Guia seguridad IoT INCIBE:

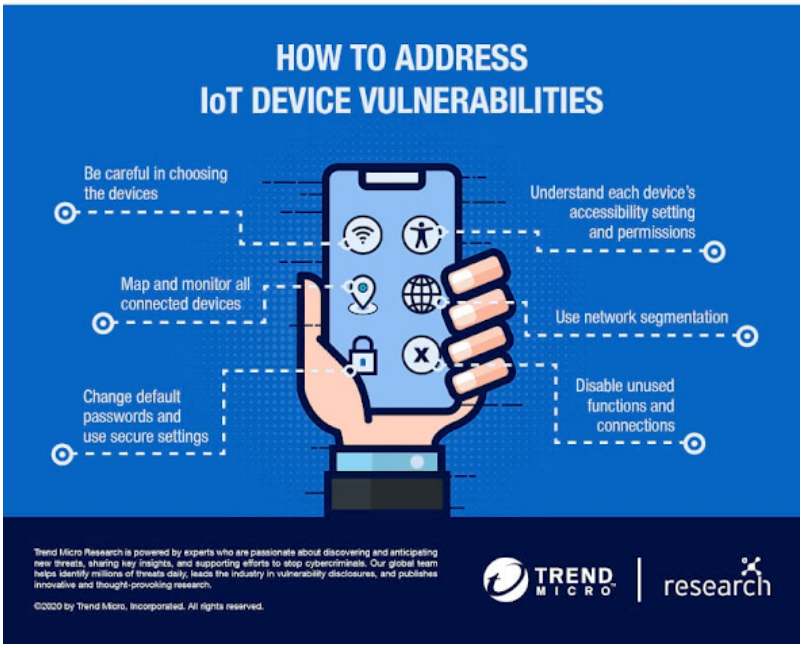
- **https://www.incibe.es/protege-tu-empresa/blog/seguridad-instalacion-y-uso-dispositivos-iot-guia-aproximacion-el-empresario**
- **https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-de-seguridad-iot.pdf**

Otros artículos interesantes:

- https://www.ikusi.es/consideraciones-basicas-de-seguridad-en-el-iot/
- https://www.incibe-cert.es/blog/riesgos-y-retos-ciberseguridad-y-privacidad-iot
- https://ciberseguridad.blog/recomendaciones-de-ciberseguridad-en-iot/
- https://www.kaspersky.es/resource-center/preemptive-safety/best-practices-for-iot-security

Recomendaciones Seguridad IoT

Vulneravilidades comunes de los dispositivos IoT: https://www.infoplc.net/actualidad-industrial/item/108035-vulnerabilidades-dispositivos-iot



Recomendaciones:

- **No abrir puertos innecesariamente**. Si un servidor envía datos a un dispositivo IoT, este debe estar escuchando con un puerto abierto de entrada. Esto supone que el dispositivo tiene que estar escuchando en todo momento para que los datos sean enviados. Por esta razón, implementar protocolos **COAP, MQTT, WebSockets y HTTP2.0** son mejores prácticas para proteger una conexión, independiente del protocolo de red usado durante el intercambio de información.
- **Cifrado de extremo a extremo**. TLS / SSL protege el nivel superior del flujo de datos entre los dispositivos y cifra los datos mientras son transferidos. TLS / SSL es adecuado para la seguridad de la transmisión de datos, pero no los datos que residen en el dispositivo a menos que está encriptado. Para una verdadera seguridad de extremo a extremo, los datos deben cifrarse con Advanced Encryption Standard (AES).
- **Control de acceso basado en tokens**. Mientras AES y TLS / SSL se pueden utilizar para cifrar los datos a medida que se está transfiriendo, otro reto importante es definir el control de quién y qué puede transmitir y recibir datos. Dentro del paradigma de publicación / suscripción, un enfoque de control de acceso basado en token puede ser utilizado para distribuir señales a los dispositivos para permitir el acceso a los canales de datos específicos. En su defecto usar contraseñas seguras.
- **Interfaces web seguras y certificadas**. Uso de HTTPS para proteger la información transmitida con acceso mediante usuario y contraseña.
- **Autenticación y autorización**. No solo prestar atención a la autenticación, sino también a los datos o recursos a los que se puede acceder.

- **Prestar atención a la privacidad**. Determinar la cantidad de información personal recopilada y protegerlos adecuadamente, así como desidentificar o anonimizar.
- **Configuración de la seguridad**. Usar protocolos seguros y actualizados sin vulnerabilidades conocidas. Usar las soluciones de cifrado más potentes.
- **Usar software y firmware seguro**. Asegurarse de tener los dispositivos actualizados y con los parches de seguridad aplicados. No usar sistemas operativos obsoletos, ni librerías no mantenidas en el desarrollo de aplicaciones o firmware.
- **Deshabilitar funcionalidades no utilizadas**. No habilitar características no usadas, no conectar dispositivos si no es necesario o apagar cuando no se use, deshabilitar o proteger el acceso remoto a los dispositivos IoT.
- **Habilitar el uso de logs**. Guardar los eventos que se producen como accesos, cambios de contraseña, actualizaciones, etc..
- **Prestar atención a la seguridad física**. Limitar el acceso a puertos del dispositivo y ubicarlos en sitios seguros (p.e. vandalismo, acceso de terceros, pérdidas de energía).
- **Realizar auditorías de seguridad con regularidad**. Pentesting, comprobar visibilidad de los dispositivos en Internet (p.e. shodan), etc...
- **Pensar en la seguridad desde la fase de requisitos y diseño.**
- **Almacenamiento de datos seguro.** No exponer las bases de datos y usar procesos intermedios para insertar, modificar y acceder a los datos.
- **Gestionar y monitorizar los dispositivos IoT de forma centralizada**. Comprobar su correcto funcionamiento y que no se produzcan eventos que puedan afectar a su seguridad. Poder apagar dispositivos de forma remota en caso que sea comprometido.

Esta entrada se publicó en Ciberseguridad, IIoT, IoT, Seguridad y está etiquetada con Ciberseguridad, IIoT, IoT, Seguridad, Seguridad IoT en 6 marzo, 2021 [https://aprendiendoarduino.wordpress.com/2021/03/06/conceptos-basicos-de-ciberseguridad/] .

Un pensamiento en “Conceptos Básicos de Ciberseguridad”

Pingback: Saber Más Fundamentos IoT CEFIRE | Aprendiendo Arduino

Este sitio usa Akismet para reducir el spam. Aprende cómo se procesan los datos de tus comentarios .