
Privacidad y Seguridad en el Edificio Inteligente

Dionisio Oliver Segura

Ingeniero de Telecomunicación

Miembro del GTEP del COIT



colegio oficial
ingenieros de telecomunicación

Congreso Edificios Inteligentes

25 de Octubre de 2018

DEFINICIONES

- Privacidad: habilidad para controlar a quién y en qué contexto se revela información acerca de nosotros.
 - Derecho esencial preservado por el artículo 18 de la Constitución / artículo 12 de la Declaración Universal de los Derechos Humanos.
- Seguridad: capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos (Directiva UE/2016/1148).
 - Esencial para actividades económicas y sociales en el Mercado interior de la UE.



MARCO DE LA PRIVACIDAD. RGPD

- Reglamento UE /2016/679.
- Aplica a los datos personales.
- Incluye las fases de recogida y transporte de la información.
- Impone la privacidad desde el diseño y por defecto.
- Extiende el concepto de dato personal a todos los posibles identificadores unívocos, directos o indirectos.
- Exige notificar las brechas de seguridad, por lo que se deberá extraer información constante sobre los intentos de intrusión.
- Cifrado de información obligatorio en ciertos casos de manejo de datos sensibles (hospitales, servicios domésticos de e-salud, despachos abogados, etc.).
- Obligaciones exógenas sobre conservación de datos e interceptación de comunicaciones que imponen cumplir con el RGPD (ej. Wi-fi publicas).

MARCO DE LA PRIVACIDAD. E-PRIVACY

- Propuesta Reglamento
- Aplica a las comunicaciones M2M para aplicaciones de IoT.
- Obliga a la confidencialidad de todas las comunicaciones electrónicas.
- Exige anonimizar los datos y metadatos cuando sea necesario guardarlos por razones legales o comerciales.
- Impone exigencias al SW comercializado para impedir a terceros almacenar o manipular la información de los equipos terminales de un usuario final.
- Establece que la prohibición de la interceptación de datos de comunicaciones ha de ser aplicable durante su fase de transporte.

MARCO DE LA CIBERSEGURIDAD

- Implantación sectorial de la Directiva NIS, transpuesta por Real Decreto-ley 12/2018.
- Propuesta de Reglamento sobre ciberseguridad por diseño y para un marco europeo de certificación.
- Propuesta de Reglamento y Directiva e-Evidence.
- Propuesta de Directiva para la lucha contra el fraude y la falsificación de medios de pago.
- Propuesta de Reglamento de un marco para la libre circulación de datos no personales en la Unión Europea.
- Propuesta de Directiva relativa al Código europeo de las comunicaciones electrónicas .
- Esquema nacional de seguridad.
- Ley de conservación de datos relativos a las comunicaciones electrónicas.
- Ley de interceptación de las comunicaciones electrónicas.

RESUMIENDO SUS NOVEDADES...

- ¿A qué afectan?
 - A las redes e infraestructuras de comunicaciones.
 - A los dispositivos conectados a las mismas.
 - A los servicios que se prestan a través de las mismas.
 - A los procesos de diseño e instalación de las mismas.
- ¿A quién afectan?
 - A las propietarios de las infraestructuras (redes y dispositivos).
 - A los prestadores de los servicios a través de las mismas.
 - A los diseñadores que ofrecen garantía de las mismas.
 - A los instaladores y mantenedores de las mismas.



RESUMIENDO SU IMPORTANCIA...

- Impacto en el negocio: Conciencia de sus carencias como un riesgo comercial y para la reputación empresarial.
- Valor añadido como imagen de marca: Garantizar la privacidad y la seguridad por diseño.
- Exigencia legal (sanciones): Vigilancia proactiva para detectar posibles vulnerabilidades es atenuante (aunque no eximente).

Principio rector de privacidad y seguridad desde el diseño y por defecto: Fundamental la labor a realizar por los ingenieros y arquitectos.