Una vez más, el **eslabón más débil** de esta cadena vuelve a ser el **factor humano** por su **escasa concienciación** y su **exceso de confianza** a la hora de emplear estas redes.

En general, los **riesgos** asociados a las redes sociales son los mismos que los del resto de actividades y/o servicios en Internet: grandes [1]**dificultades** para **eliminar** la **información subida**, el [2]**acceso futuro** por **terceros** (el derecho a cambiar de opinión es nulo y será muy difícil borrar cualquier opinión, fotografía o vídeo subido a la red) y la [3]**dificultad** de **discernir** entre **información veraz** y **propaganda** o **manipulación**.

A continuación, se indican los principales **consejos** que se pueden dar como buenas prácticas en el **uso** de **redes sociales**:

- **Creación cuidadosa** del **perfil** y la **configuración** de **privacidad**. No basarse en la configuración por defecto que proporcionan las plataformas.
- **Reflexión** sobre todo **lo que se publica** y **emplear** un **pseudónimo**. Dar por sentado que todo lo que se sube en una red social es **permanente**, aunque se elimine la cuenta.
- **Escoger cuidadosamente** a nuestros **amigos**.
- Para **evitar revelar** las direcciones de **correo** de sus **amigos**, **no permita** que los **servicios de redes sociales examinen** su **libreta** de direcciones de **correo**.
- **Prestar atención** a los **servicios** basados en la **localización** y la **información** del **teléfono móvil**.
- **Precaución** con los **enlaces**. **Evitar** hacer clic en **hipervínculos** o **enlaces** de procedencia **dudosa**.
- **Escribir directamente** la **dirección** de su **sitio** de **redes sociales** en el **navegador** para evitar que un sitio falso pueda robar su información personal.
- **Tener precaución** al **instalar elementos adicionales** en su sitio ya que, en ocasiones, se usan estas aplicaciones para robar información personal.
- **Revisar** la **información publicada**. **Eludir dar excesiva información** sobre **uno mismo** entre otras cosas para evitar que puedan entrar en su cuenta al responder a preguntas del tipo su cumpleaños, su ciudad natal, clase del instituto, etc.
- **Seguridad** de las contraseñas, **utilice contraseñas complejas** que incluyan **números**, **símbolos** y **signos de puntuación**. Es importante no compartir la misma contraseña para todas las redes sociales ni para el resto de servicios que se utilizan en Internet.
- **Incrementar** la **seguridad** en el **acceso** a la **cuenta añadiendo** un **segundo factor** de **autenticación** (2FA) que impida a un potencial atacante que se haya hecho con la contraseña acceder al servicio.

Internet de las cosas IoT (Nº 13)

En esencia, **IOT** (Internet of Things) se refiere a **redes** de **objetos físicos**, **artefactos**, **vehículos**, **edificios**, **electrodomésticos**, **atuendos**, **implantes**, etc. que **llevan** en su seno **componentes electrónicos**, **software**, **sensores con conectividad** en red que les **permite recolectar información** para lograr una contextualización de la situación **mediante técnicas** de **Big Data*** imposible de realizar por otros medios.

Se trata de una **red** que **interconecta** miles de **objetos físicos ofreciendo datos** en **tiempo real**, convirtiéndose en los sensores del mundo físico. En este punto hay que considerar el **cambio cultural** que suponen ya que la tecnología **influye** en nuestra **forma** de **tomar** las **decisiones** y ello **afecta** a la **capacidad de acción**, **privacidad** y **autonomía** de las personas.

La **Iot** es la **primera evolución real** de **Internet**, un salto que podría llevar a **aplicaciones revolucionarias** con capacidad para **modificar** de forma dramática **la forma** en la que **vivimos, aprendemos**, **trabajamos** y nos **entretenemos** o **relacionamos socialmente**.

Los **artículos** de **uso diario** han **dejado de ser** elementos **aislados**, dispositivos que a su vez pueden estar conectados a otros dispositivos. La **pesadilla** de los **expertos** en **ciberseguridad** puede convertirse en **ejércitos** de "**botnets**" **utilizando** las **tostadoras inteligentes** para desarrollar **ataques DDoS*** o para **esconder información** y ejecutables lejos de la vista de los investigadores.

En la **Iot** hay que considerar **aspectos** de **vital importancia** como la **seguridad**, la **interoperabilidad** y **manejabilidad** de dichos **sistemas**:

- **Interfaz Web**.
- **Mecanismos** de **autenticación**.
- **Servicios** de **red**.
- **Transporte no cifrado**.
- **Protección** de la **intimidad**.
- **Configuración** de **seguridad**.
- **Integridad software/firmware**.
- **Seguridad física** de los **dispositivos**.
- El **reto** se reduce a establecer una base de **monitorización** y **control** para **reducir** la **exposición** al **riesgo** y **aplicar técnicas inteligentes** a la creciente población de dispositivos Iot.
- **Cambiar** las **contraseñas** por **defecto** de los dispositivos y **utilizar contraseñas** realmente **robustas**.
- **Mantener actualizados** los **dispositivos** con las **últimas versiones** disponibles de **software** y **firmware**.
- **Desactivar** toda **conectividad remota** (con Internet) de los dispositivos cuando no sea estrictamente necesaria.
- **Mantener abiertos** solo aquellos **puertos de comunicación** que sean realmente **necesarios** y **modificar** los **puertos de escucha** si es posible.
- Si los **dispositivos Iot no permiten** la **configuración** de su **seguridad**, **operar** con ellos siempre en una **red de área local** (**LAN**) detrás de un **dispositivo** (enrutador) correctamente configurado que **sí provea** esa **seguridad**.
- En la medida de lo posible, **asegurar** la **autenticidad**, **confidencialidad** e **integridad** en todas las **comunicaciones locales** (**LAN**), especialmente si estas se realizan por enlaces radio (WiFi, Bluetooth, etc.).
- **Comprobar** periódicamente la **configuración** de **seguridad** de todos los **elementos** de la arquitectura **Iot** y su **comunicación** con el **exterior**.
- **Mantener deshabilitados** los **componentes no necesarios** como pueden ser, según el caso, micrófonos, cámaras de vídeo, etc...
- **Comprobar** la **visibilidad** de los **dispositivos** propios en **buscadores** de **dispositivos Iot** como **Shodan**.

REAL DECRETO 4/2010, DE 8 DE ENERO, POR EL QUE SE REGULA EL ESQUEMA NACIONAL DE INTEROPERABILIDAD EN EL ÁMBITO DE LA ADMINISTRACIÓN ELECTRÓNICA.

DISPOSICIONES GENERALES (Cap. 1)

Objeto (Art. 1)

El presente **real decreto** tiene por objeto **regular** el **Esquema Nacional de Interoperabilidad** establecido en el artículo 42 de la Ley 11/2007, de 22 de junio.

El **Esquema Nacional de Interoperabilidad** comprenderá los **criterios** y **recomendaciones** de [1]**seguridad**, [2]**normalización** y [3]**conservación** de la **información**, de los **formatos** y de las **aplicaciones** que deberán ser tenidos en cuenta por las Administraciones públicas para **asegurar** un adecuado nivel de **interoperabilidad** **organizativa**, **semántica** y **técnica** de los **datos**, **informaciones** y **servicios** que gestionen en el ejercicio de sus competencias y para **evitar** la **discriminación** a los **ciudadanos** por razón de su elección tecnológica.

Ámbito de aplicación (Art. 3)

El **Esquema Nacional de Interoperabilidad** y sus normas de desarrollo, **prevalecerán** sobre cualquier **otro criterio** en materia de **política** de **interoperabilidad** en la utilización de medios electrónicos para el acceso de los ciudadanos a los servicios públicos.

PRINCIPIOS BÁSICOS (Cap. 2)

Principios básicos del Esquema Nacional de Interoperabilidad (Art. 4)

La **aplicación** del **Esquema Nacional de Interoperabilidad** se desarrollará de acuerdo con los principios generales establecidos en el artículo 4 de la Ley 11/2007, de 22 de junio, y con los siguientes **principios específicos** de la interoperabilidad:

- La interoperabilidad como **cualidad integral**.
- **Carácter multidimensional** de la interoperabilidad.
- **Enfoque** de **soluciones multilaterales**.

La interoperabilidad como cualidad integral (Art. 5)

La **interoperabilidad** se tendrá presente de **forma integral** desde la **concepción** de los **servicios** y **sistemas** y **a lo largo** de su **ciclo de vida**: [1]**planificación**, [2]**diseño**, [3]**adquisición**, [4]**construcción**, [5]**despliegue**, [6]**explotación**, [7]**publicación**, [8]**conservación** y [9]**acceso** o [10]**interconexión** con los mismos.

Carácter multidimensional de la interoperabilidad (Art. 6)

La **interoperabilidad** se entenderá contemplando sus **dimensiones organizativa**, **semántica** y **técnica**. La **cadena** de **interoperabilidad** se **manifiesta** en la práctica en los [1]**acuerdos interadministrativos**, en el despliegue de los [2]**sistemas** y **servicios**, en la determinación y uso de [3]**estándares**, en las [4]**infraestructuras** y **servicios básicos** de las Administraciones públicas y en la publicación y reutilización de las [5]**aplicaciones** de las Administraciones públicas, de la documentación asociada y de otros objetos de información

Enfoque de soluciones multilaterales (Art. 7)

Se **favorecerá** la aproximación **multilateral** a la **interoperabilidad** de forma que se puedan obtener las **ventajas** derivadas del [1]**escalado**, de la aplicación de las [2]**arquitecturas modulares** y **multiplataforma**, de [3]**compartir**, de [4]**reutilizar** y de [5]**colaborar**.

INTEROPERABILIDAD ORGANIZATIVA (Cap. 3)

Servicios de las Administraciones públicas disponibles por medios electrónicos (Art. 8)

Las **Administraciones públicas** establecerán y publicarán las **condiciones** de **acceso** y **utilización** de los **servicios**, **datos** y **documentos** en formato **electrónico** que pongan a disposición del resto de Administraciones **especificando** las [1]**finalidades**, las [2]**modalidades de consumo**, [3]**consulta** o [4]**interacción**, los [5]**requisitos** que deben satisfacer los posibles **usuarios** de los mismos, los [6]**perfiles** de los **participantes** implicados en la utilización de los servicios, los [7]**protocolos** y **criterios funcionales** o **técnicos** necesarios para **acceder** a dichos **servicios**, los necesarios [8]**mecanismos de gobierno** de los **sistemas interoperables**, así como las [9]**condiciones de seguridad** aplicables. Estas **condiciones** deberán en todo caso resultar **conformes** a los principios, derechos y obligaciones contenidos en la **Ley Orgánica 15/1999** de 13 de diciembre, de [1]**Protección de Datos de Carácter Personal** y su normativa de desarrollo, así como a lo dispuesto en el [2]**Esquema Nacional de Seguridad**, y los instrumentos jurídicos que deberán suscribir las Administraciones públicas requeridoras de dichos servicios, datos y documentos.

Se **potenciará** el establecimiento de **convenios** entre las **Administraciones públicas** emisoras y receptoras y, en particular, con los **nodos de interoperabilidad** previstos en el apdo. 3 de este artículo, con el objetivo de **simplificar** la **complejidad organizativa** sin menoscabo de las garantías jurídicas.

Al objeto de dar cumplimiento de manera eficaz a lo establecido en el artículo 9 de la Ley 11/2007, de 22 de junio, en el **Comité Sectorial de Administración electrónica** se **identificarán**, **catalogarán** y **priorizarán** los **servicios de interoperabilidad** que deberán prestar las diferentes Administraciones públicas.

Las **Administraciones públicas** **publicarán** aquellos **servicios** que pongan a disposición de las demás administraciones **a través** de la **Red de comunicaciones** de las Administraciones públicas españolas, o de

cualquier **otra** red **equivalente** o **conectada** a la misma que **garantice** el **acceso seguro** al resto de administraciones.

Las **Administraciones públicas** podrán **utilizar nodos de interoperabilidad**, entendidos como **entidades** a las cuales se les **encomienda** la **gestión** de apartados **globales** o **parciales** de la **interoperabilidad organizativa**, **semántica** o **técnica**.

Inventarios de información administrativa (Art. 9)

Cada **Administración Pública** mantendrá **actualizado** el conjunto de sus **inventarios de información administrativa** que incluirá, al menos:

- La relación de los **procedimientos administrativos** y **servicios** prestados de forma **clasificada** y **estructurada**.

  Las Administraciones Públicas **conectarán electrónicamente** sus **inventarios** con el **Sistema de Información Administrativa** gestionado por el **Ministerio de Política Territorial y Función Pública** en **colaboración** con el **Ministerio de Asuntos Económicos y Transformación Digital**.

- La relación de sus **órganos administrativos** y **oficinas orientadas al público** y sus relaciones entre ellos. Dicho inventario se **conectará electrónicamente** con el **Directorio Común de Unidades Orgánicas y Oficinas**, gestionado por el **Ministerio de Asuntos Económicos y Transformación Digital**, en **colaboración** con el **Ministerio de Política Territorial y Función Pública**, que proveerá una **codificación unívoca**.

INTEROPERABILIDAD SEMÁNTICA (Cap. 4)

Activos semánticos (Art. 10)

Se establecerá y mantendrá **actualizada** la **Relación de modelos** de **datos de intercambio** que tengan el **carácter** de **comunes**, que serán de preferente **aplicación** para los **intercambios** de **información** en las **Administraciones públicas**, de acuerdo con el procedimiento establecido en disposición adicional primera.

Los órganos de la **Administración pública** o **Entidades de Derecho Público** vinculadas o dependientes de aquélla, titulares de competencias en materias sujetas a **intercambio** de **información** con los **ciudadanos** y con **otras Administraciones públicas**, así como en materia de **infraestructuras**, **servicios** y **herramientas comunes**, establecerán y publicarán los correspondientes **modelos de datos de intercambio** que serán de obligatoria aplicación para los intercambios de información en las Administraciones públicas.

Los **modelos de datos** a los que se refieren los apartados 1 y 2, se ajustarán a lo previsto sobre estándares en el artículo 11 y **se publicarán**, junto con las **definiciones** y **codificaciones** asociadas, **a través** del **Centro de Interoperabilidad Semántica** de la **Administración**, según las condiciones de licenciamiento previstas en el artículo 16.

INTEROPERABILIDAD TÉCNICA (Cap. 5)

Estándares aplicables (Art. 11)

Las **Administraciones públicas** usarán **estándares abiertos**, así como, en su caso y de **forma complementaria**, **estándares** que sean de **uso generalizado** por los **ciudadanos**, al objeto de **garantizar** la **independencia** en la **elección** de alternativas **tecnológicas** por los ciudadanos y las Administraciones públicas y la adaptabilidad al progreso de la tecnología y, de forma que:

- Los **documentos** y **servicios** de **administración electrónica** que los órganos o Entidades de Derecho Público emisores pongan a disposición de los ciudadanos o de otras Administraciones públicas se encontrarán, como mínimo, **disponibles** mediante **estándares abiertos**.
- Los **documentos**, **servicios electrónicos** y **aplicaciones** puestos por las Administraciones públicas a disposición de los ciudadanos o de otras Administraciones públicas serán, según corresponda, **visualizables**, **accesibles** y **funcionalmente operables** en condiciones que permitan **satisfacer** el

principio de **neutralidad tecnológica** y **eviten** la **discriminación** a los **ciudadanos** por razón de su **elección tecnológica**.

En las **relaciones** con los **ciudadanos** y con **otras Administraciones públicas**, el **uso** en exclusiva de un **estándar no abierto sin** que se ofrezca una alternativa basada en un **estándar abierto** se **limitará** a aquellas **circunstancias** en las que **no** se **disponga** de un **estándar abierto** que satisfaga la **funcionalidad satisfecha** por el estándar **no abierto** en **cuestión** y sólo mientras dicha disponibilidad no se produzca. Las **Administraciones públicas** promoverán las **actividades** de **normalización** con el fin de **facilitar** la **disponibilidad** de los **estándares abiertos relevantes** para sus necesidades.

Para la **selección** de **estándares**, en general y, para el **establecimiento** del **catálogo** de estándares, en particular, se atenderá a los siguientes **criterios**:

- El **uso** de las **especificaciones técnicas** de las **TIC** en la **contratación pública** junto con las definiciones de **norma** y **especificación técnica** establecidos en el **Reglamento** Nº **1025/2012**, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre normalización europea.
- La definición de **estándar abierto** establecida en la **Ley 11/2007**, de 22 de junio, anexo, letra k).
- Carácter de **especificación formalizada**.
- Definición de «**coste** que **no** suponga una **dificultad de acceso**», establecida en el anexo de este real decreto.
- **Consideraciones adicionales** referidas a la **adecuación** del estándar a las **necesidades** y **funcionalidad** requeridas

En cualquier caso los **ciudadanos** podrán **elegir** las **aplicaciones** o **sistemas** para **relacionarse** con las **Administraciones públicas**, o dirigirse a las mismas, siempre y cuando **utilicen** [1]**estándares abiertos** o, en su caso, aquellos otros que sean de [2]**uso generalizado** por los **ciudadanos**.

Para **facilitar** la **interoperabilidad** con las Administraciones públicas el **catálogo de estándares contendrá** una relación de **estándares abiertos** y en su caso **complementarios** aplicables.

INFRAESTRUCTURAS Y SERVICIOS COMUNES (Cap. 6)

Uso de infraestructuras y servicios comunes y herramientas genéricas (Art. 12)

Las **Administraciones públicas enlazarán** aquellas **infraestructuras** y **servicios** que puedan implantar en su ámbito de actuación con las infraestructuras y servicios comunes que proporcione la Administración General del Estado para **facilitar** la **interoperabilidad** y la **relación multilateral** en el **intercambio** de **información** y de **servicios** entre todas las Administraciones públicas.

COMUNICACIONES DE LAS ADMINISTRACIONES PÚBLICAS (Cap. 7)

Red de comunicaciones de las Administraciones públicas españolas (Art. 13)

Al objeto de satisfacer lo previsto en el artículo 43 de la Ley 11/2007, de 22 de junio, las Administraciones públicas utilizarán **preferentemente** la **Red de comunicaciones de las Administraciones públicas españolas** para **comunicarse entre sí**, para lo cual **conectarán** a la misma, bien **sus** respectivas [1]**redes**, bien sus [2]**nodos de interoperabilidad**, de forma que se facilite el **intercambio** de **información** y de **servicios** entre las mismas, así como la interconexión con las [3]**redes** de las **Instituciones** de la **Unión Europea** y de **otros Estados miembros**.

La **Red Sara*** **prestará** la citada **Red de comunicaciones** de las **Administraciones públicas españolas**.

Plan de direccionamiento de la Administración (Art. 14)

Las **Administraciones Públicas** aplicarán el **Plan de direccionamiento e interconexión de redes** en la Administración, desarrollado en la **norma técnica de interoperabilidad** correspondiente, para su **interconexión** a través de las **redes de comunicaciones**.