EXPOSICIÓN DE BLOQUES TEMÁTICOS

1. Organización de cumplimiento, sobre aspectos tales como:
    a. Roles y figuras, obligatorios y voluntarios.
    Se trata de conocer si la Organización cuenta con personal dedicado a esta actividad. En caso positivo si se trata de figuras obligatorias (responsable/s de seguridad) o voluntarias (DPO u otras) y su grado de dedicación (total o parcial).
    b. PbD, PIAS.
    Se trata de conocer si la Organización realiza estas actividades. En caso positivo en qué porcentaje de proyectos se realiza.
    c. Externalización: grado, materias, etc.
    Se trata de conocer si la Organización tiene el servicio externalizado total o parcialmente y en el caso parcial qué porcentaje. También saber si lo que se tiene es un servicio de ayuda/consultoría pero llevándose el servicio de forma interna.
    d. Cuadros de mando.
    Se trata de conocer si la Organización tiene establecido este tipo de cuadros. En caso positivo la frecuencia de realización y los destinatarios de los mismos.
    e. Nuevos retos: cloud, bigdata, IoT, menores…
    Se trata de conocer si la Organización realiza alguna de estas actividades. En caso positivo, con qué grado de cumplimiento se llevan a cabo.

2. Principios de Protección de datos.
    a. Calidad, principalmente conservación.
    Se trata de conocer si la Organización tiene establecidos procedimientos de evaluación para saber si los datos personales que manejan son necesarios, procedimientos para mantener su actualización y procedimientos de purga de información.
    b. Información y consentimiento, principalmente respecto a apps, web…
    Se trata de conocer si la Organización informa en la recogida de datos personales, si dispone de cláusulas estándar de información del artículo 5. Si las tiene impresas en los formularios de recogida de los mismos, en las páginas web, etc.
    c. Compra de bbdd.
    Se trata de conocer si la Organización compra o usa bases de datos externas. En caso positivo si se lo comunica a los interesados y si les pide consentimiento para su utilización.

d. Cookies.
   Se trata de conocer si la Organización utiliza cookies y en caso afirmativo lo comunica a los interesados.
e. Videovigilancia.
   Se trata de conocer si la Organización utiliza este sistema de seguridad. En caso afirmativo si cumple todos los requisitos.

3. Seguridad de los datos.
   a. Documento de seguridad.
      Se trata de conocer si la Organización dispone de este documento, si es uno o varios, si está/n actualizado/s, si lo conocen los usuarios y si se tiene prueba de este conocimiento.
   b. Medidas de seguridad.
      Se trata de conocer si la Organización ha dispuesto las medidas de seguridad correspondientes, si éstas son específicas para el tema de la privacidad o por el contrario están embebidas dentro de las medidas de carácter general.
   c. Fugas de información.
      Se trata de conocer si la Organización ha tenido fugas de información (leves, graves o muy graves), En caso positivo si se han comunicado a la AEPD y/o a los interesados.
   d. Continuidad de negocio
      Se trata de conocer si la Organización dispone de este plan, realiza las pruebas correspondientes y la frecuencia de las mismas.

4. Acciones de cumplimiento hacia fuera: clientes, proveedores, etc.
   Se trata de conocer si la Organización ha informado del artículo 5, ha pedido consentimiento en los casos que se precise, etc. hacia los terceros externos y si guarda prueba de su cumplimiento. También si tiene procedimientos para el ejercicio de los derechos ARCO.

5. Acciones de cumplimiento hacia dentro: empleados.
   Se trata de conocer si la Organización ha informado del artículo 5, ha pedido consentimiento en los casos que se precise, etc. hacia los empleados y si guarda prueba de su cumplimiento. También en este apartado se incluye la concienciación que se imparte a los empleados como usuarios que manejan datos de carácter personal en su trabajo.

6. Formación, interna y externa.
   Se trata de conocer si la Organización imparte formación específica al personal que tiene responsabilidad en temas de protección de datos. Si esta formación se realiza de forma interna o se acude a cursos externos. En casos de ambas maneras, el porcentaje de formación interna/externa.

7. Auditorías, obligatorias y voluntarias.
   Se trata de conocer si la Organización realiza auditorías sobre protección datos distinguiendo las obligatorias de las voluntarias. En el caso de las voluntarias, con qué periodicidad y si éstas son internas y/o externas. En el caso de ambas modalidades, con qué porcentaje.

8. Modelo de gestión (conocimiento y asimilación) de novedades en Protección de Datos (AEPD, Audiencia Nacional, Tribunales, etc.).
   Se trata de conocer si la Organización tiene establecido algún iniciativa/procedimiento por el que el personal que tiene roles en protección de datos se deba mantener actualizado con la actividad de la AEPD y la jurisprudencia que se va generando día a día de forma que se vaya más allá del conocimiento exclusivo de la legislación. En caso positivo saber si esta actividad es interna o se tiene contratada de forma externa.

9. Pertenencia a asociaciones, grupos de interés y similar (que no sean ISMS/DPI).
   Se trata de conocer si la Organización pertenece a alguna organización que entre sus objetivos tenga la privacidad o la protección de datos incluido la pertenencia a un código tipo sectorial. En caso positivo, qué organización/es o código tipo.