CENID CENTRO DE INTELIGENCIA DIGITAL PROVINCIA DE ALICANTE

PROYECTO

Observatorio de cumplimiento de normativa de Protección de Datos en los municipios de la Provincia de Alicante

OPPA Observatorio de Privacidad de la Provincia de Alicante

Informe de estado de seguimiento del Proyecto

INFORME CENID-OPPA-21/01

DIPUTACIÓN DE ALICANTE Universitat d'Alacant Universidad de Alicante UNIVERSITAS Miguel Hernández

Indice

ANEXO II: Enlace a Cuestionario sobre Esquema Nacional de Seguridad en municipios provincia de Alicante

ANEXO III: Enlace a repositorio donde se alojan los entregables de las Actividades 2 y 3.

Introducción

Es un hecho notorio que la administración pública en general y las entidades locales en particular manejan a diario infinidad de datos de carácter personal tanto de los ciudadanos a quienes prestan diariamente sus servicios (el censo y el padrón municipal, las licencias y autorizaciones de todo tipo, la escolarización, las ayudas e impuestos, etc,..) cuanto de las propias personas que los prestan (miembros de la corporación, cargos públicos, funcionarios, personal laboral, colaboradores, etc,..) siendo lo cierto que el mero uso de todos estos datos personales afecta sensiblemente a nuestra privacidad e intimidad y es por ello que nuestra Carta Magna (la Constitución Española) los protege como un derecho fundamental frente a todo aquél que realice actividades de tratamiento de los mismos, sea como Responsable o Encargado de tratamiento.

El fenómeno de la digitalización o como se le ha venido a llamar últimamente "la cuarta revolución industrial" como paradigma del exponencial avance de las nuevas tecnologías de la información y la comunicación (las denominadas TIC) ha supuesto, también en el sector público, una auténtica revolución en la manera en que todos estos servicios públicos pueden ser ahora prestados a los ciudadanos durante las 24 horas, de los 7 días de la semana, o lo que es lo mismo: desde cualquier momento y lugar. Es la denominada "administración electrónica" un auténtico paso de gigante en la nueva era digital pero que, al igual que en el ámbito privado, no está exenta de un incremento de los riesgos por daños a la privacidad de los administrados, en este caso, ya sea por fallos (incluida la negligencia) o por ataques deliberados contra los sistemas de información sobre los que descansa toda la infraestructura de estos servicios prestados ahora de forma telemática por las entidades locales.

Esta y no otra es la razón por la que el ordenamiento jurídico, tanto a nivel comunitario como estatal ha promulgado normas para garantizar la seguridad de esta información y proteger los datos personales de los ciudadanos en toda la unión europea con los más altos estándares de calidad y transparencia. En nuestro caso, como decimos, además de la Constitución, tenemos el Reglamento Europeo de Protección de Datos (RGPD), la Ley de Protección de Datos y Derechos Digitales (LOPDDG)y el Esquema Nacional de Seguridad (ENS).

En orden a colaborar con las EELL para cumplir con estas normas se crea este proyecto OPPA que parte de la elaboración de un perfil de cumplimiento (cual es el nivel de cumplimiento de las normas que debe tener una entidad local en función de su dimensión, carta de servicios, etc,.) para determinar, tras un análisis de cada municipio, a modo de punto de partida, el grado efectivo y real de cumplimiento de esta normativa por cada ayuntamiento (perfil de cumplimiento) para, finalmente, a partir de este diagnóstico, a modo de propuesta o plan de acción de mejora, proponer todas aquellas medidas técnico organizativas necesarias para que estas entidades puedan garantizar la máxima excelencia en lo que a "seguridad y privacidad" de la información personal que manejan estás entidades se refiere dando así debido cumplimiento a las normas anteriormente referidas (RGPD/LOPDDG/ENS) facilitando al mismo tiempo herramientas de todo tipo para alcanzar dichos fines (formación, concienciación, herramientas, etc,.).

ACTIVIDAD 1. Tareas

Para realizar esta actividad del proyecto se han definido las siguientes tareas cuyos resultados se expondrán en páginas sucesivas de este informe:

Tarea 1.1. Definición de indicadores relevantes

Tarea 1.2. Distribución de cuestionarios en los municipios seleccionados

- Segmento 1: Municipios de población mayor de 50.000 habs. (8 unidades)
- Segmento 2: Municipios con población entre 20.001 y 50.000 habs. (18 unidades)
- Segmento 3: Municipios con población entre 5.001 y 20.000 habs. (31 unidades)
- Segmento 4: Municipios con población entre 501 y 5.000 habs. (50 unidades)
- Segmento 5: Municipios con población entre 1 y 500 habs. (34 unidades)

Tarea 1.3 Diseño de herramienta de raspado de las páginas web

Tarea 1.4. Raspado de webs de los municipios seleccionados

Tarea 1.5. Hacking ético a sistemas de información seleccionados

Tarea 1.6. Recogida de resultados

Tarea 1.1. Definición de indicadores relevantes

A continuación se detallan los indicadores que serán evaluados en el estudio, y que se tomarán con base para la elaboración del cuestionario sobre el grado de cumplimiento de la normativa de protección de datos y seguridad de la información en los municipios de la Provincia de Alicante

- Las categorías datos personales objeto de tratamiento

Sensibles/ No sensibles
Necesidad de evaluación previa impacto
Origen de los datos

- Cesiones de datos personales

Dentro UE
Cesión internacional de datos. (Puerto seguro)

- Información a los interesados, titulares de los datos personales

- Capas
- Soporte
- Datos obtenidos interesado/ o de terceros

- Causas de legitimación para el tratamiento de los datos personales

Consentimiento
Ley, relación jurídica previa
Interés general
Interés legítimo
Otras

- Medidas de seguridad implementadas por la organización

MEDIDAS ORGANIZATIVAS (Información que deberá ser conocida por todo el personal con acceso a datos personales)

- deber de confidencialidad y secreto
- derechos de los titulares de los datos personales
- violaciones de seguridad de datos de carácter personal
- captación de imágenes con cámaras y finalidad de seguridad (VIDEO VIGILANCIA)

MEDIDAS TÉCNICAS

Identificación (Política de contraseñas y administración de recursos permisionada, etc.)

Deber de salvaguarda (Actualizaciones, malware, firewall, cifrado, copia de seguridad, etc.)
Certificación de Esquema nacional de Seguridad

- Derechos digitales. Nueva LOPD

- Ejercicio de los derechos POLIARSO

Tarea 1.2. Elaboración/distribución del cuestionario

Con el fin de dar cumplimiento a los indicadores relevantes se realizan los cuestionarios de preguntas que se detallan en los anexos I y II. Los cuestionarios han sido realizados en formato Word para comodidad de los entrevistados pero su contenido se vuelca en la herramienta ***Privacy Driver*** (suite ofimática formato SaaS) y las preguntas se han distribuido en las siguientes secciones:

I. CUESTIONARIO NORMATIVA PROTECCION DE DATOS

1. IDENTIFICACIÓN DEL PROYECTO

Obtener información de identificación de la propia organización, es decir, datos tales como: Datos de la Organización, del responsable del tratamiento (ERT) y dónde se ejercitan los Derechos de los interesados/afectados por el tratamiento de sus datos personales

2. ORGANIZACIÓN

Estructura organizativa del Ayuntamiento. (1) los distintos locales o delegaciones que estén físicamente en lugares o ubicaciones separadas. (2) Los distintos tratamientos (anteriormente denominados ficheros) de datos personales que se realizan en el seno de la organización (empleados, proveedores, contribuyentes, administrados, etc,…) Y, finalmente, (3) e independientemente de su efectiva ubicación física (o sea, pueden estar físicamente en el mismo edificio o no), cuántos departamentos distintos tiene la organización.

2.1. Número y ubicación exacta de Locales /delegaciones del Aytmo
2.2. Número y denominación de todos los tratamientos de datos personales (ficheros/tratamientos)
2.3. Número, denominación y ubicación de los Departamentos existentes en la organización (físicos o lógicos)

3. ESTRUCTURA TÉCNICA Y ORGANIZATIVA

Qué medidas de seguridad (físicas y lógicas) de la información en general y de los datos personales en particular, tiene implementadas la organización. Y para ello, necesitaremos saber primero qué recursos se usan en CADA DEPARTAMENTO a nivel de: *Hardware/Mobiliario/Soportes/Software* para el tratamiento de estos datos personales

4. MEDIDAS DE SEGURIDAD APLICADAS DESDE EL DISEÑO Y POR DEFECTO

- Confidencialidad de la información
- Sistemas de información
- Integridad de la información (copia respaldo interna/ externa y disponibilidad datos)
- Tratamientos específicos
- Organización
- Otras medidas de seguridad

5. INFORMACIÓN Y COMUNICACIÓN DEL TRATAMIENTO

- Cláusulas, contratos y documentos

6. INTERVINIENTES EN EL TRATAMIENTO

II. CUESTIONARIO SOBRE ESQUEMA NACIONAL DE SEGURIDAD

Cuestionario ENS Ayuntamientos

CARACTERÍSTICAS GENERALES DEL ENS

CARACTERÍSTICAS ESPECÍFICAS DEL ENS

SOBRE LOS USUARIOS, SU CONCIENCIACIÓN y LAS AUTORIZACIONES

SOBRE LA ARQUITECTURA DE SEGURIDAD

SOBRE EL CONTROL DE ACCESO

SOBRE EL INVENTARIO Y LA CONFIGURACIÓN DE SEGURIDAD

SOBRE EL TRABAJO CON TERCEROS

SOBRE LA CONTINUIDAD

SOBRE LA MONITORIZACIÓN

SOBRE LA PROTECCIÓN DE INSTALACIONES E INFRAESTRUCTURAS

SOBRE LA PROTECCIÓN DE LAS COMUNICACIONES

SOBRE LA PROTECCIÓN DE LOS SOPORTES

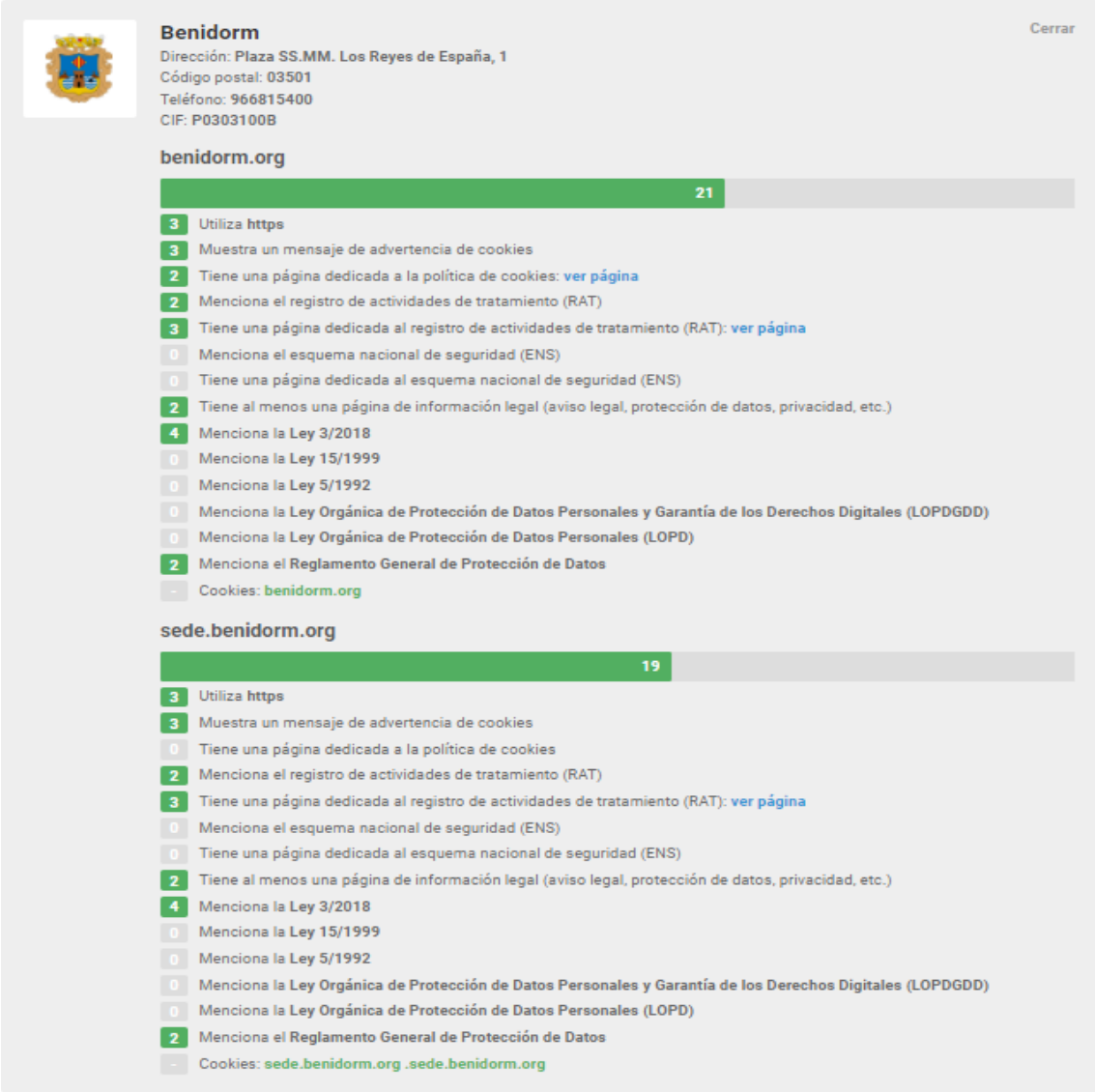
SOBRE LA PROTECCIÓN DEL SOFTWARE Y LA INFORMACIÓN

SOBRE LA PROTECCIÓN DE LOS SERVICIOS

Tarea 1.3. Diseño de herramienta de raspado de las páginas web

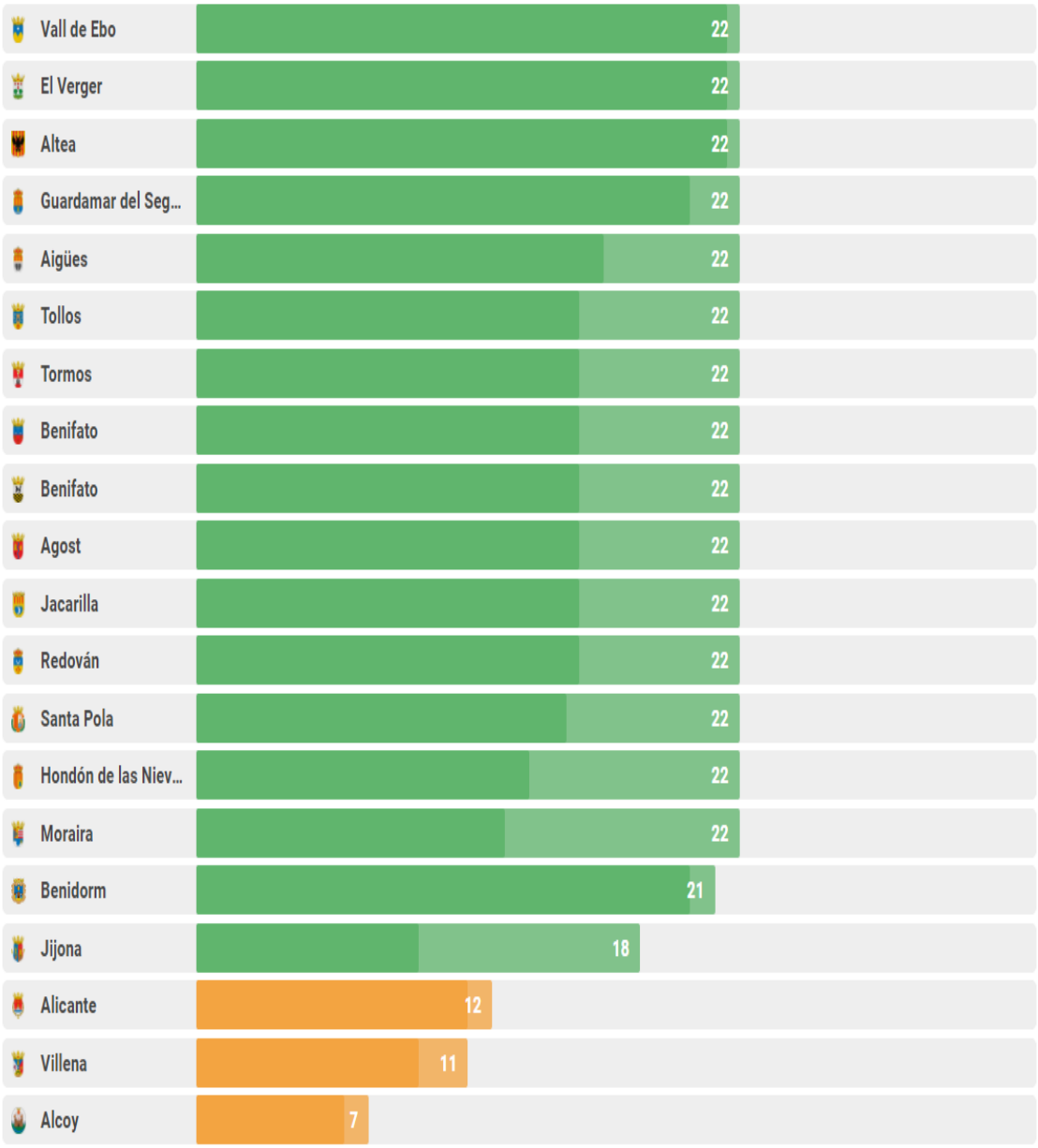
Con objeto de poder hacer una primera aproximación al grado de implementación de la normativa de protección de datos en los municipios seleccionados se ha diseñado una herramienta de raspado (web scraping) que es una técnica utilizada mediante programas de software para extraer información de sitios web simulando la navegación de un humano en la World Wide Web y cuya demo está alojada en el siguiente enlace: https://demos.gplsi.es/oppa/

Se analizan los ítems previamente definidos y se obtiene un resultado de cada web visitada.



Tarea 1.4. Raspado de webs de los Ayuntamientos seleccionados

El resultado de este raspado de las webs de los Ayuntamientos seleccionados en relación a los ítems introducidos como indicadores de implementación de normativa de protección de datos y esquema nacional de seguridad ofrece un listado a modo de ránking en que se muestra la puntuación de cada municipio.



Tarea 1.5. Hacking ético a sistemas de información de los Ayuntamientos seleccionados

Con igual finalidad se ha diseñado una herramienta que permite testar el grado de implementación de medidas de seguridad que impidan el acceso a la información o los propios sistemas de información de los ayuntamientos seleccionados a través de ataques éticos en busca de debilidades por donde dichos sistemas sean vulnerables a ataques.

Esta acción no pretende ser intrusiva en las diferentes administraciones locales por tanto se realiza conforme se reciben la autorización previa de los ayuntamientos seleccionados.

Tarea 1.6. Recogida de resultados

Se acompaña como Anexo III un cuadro que permite monitorizar el avance del proyecto en términos de recogida de la información. El anexo recoge ayuntamiento por ayuntamiento los siguientes posibles informes en función de los datos obtenidos:

- Amenazas de protección de datos
- Análisis de riesgos
- Informe acerca de las medidas de seguridad del Esquema Nacional de Seguridad (ENS)

ACTIVIDADES 2 y 3. Tareas

Para realizar estas actividades del proyecto se han definido las siguientes tareas cuyos resultados se expondrán en páginas sucesivas de este informe:

Tareas:

2.1. Análisis de los datos obtenidos.

2.2. Identificación de riesgos.

2.3. Análisis de riesgos de Municipios TIPO. Matriz de riesgos.

2.4. Mapa de Riesgos por Municipio TIPO.

3.1. Plan de Prevención de Riesgos de Seguridad y Privacidad (Medidas técnicas y Organizativas)

3.2. Medidas de prevención de Riesgos Legales.

3.3. Medidas de prevención de Riesgos Técnicos (medidas de seguridad)

Tras el trabajo de campo (Actividad 1) las tareas de estas Actividades 2 y 3 se han realizado con un aplicativo que permite compilar y tratar todos los datos obtenidos de los cuestionarios cumplimentados por cada consistorio y con el que (i) se han analizado los datos obtenidos de cada Ayuntamiento en orden a poder (ii) identificar los riesgos de privacidad y seguridad detectados en cada uno de ellos para, seguidamente, (iii) analizar y evaluar dichos riesgos y, finalmente poder (iv) proponer medidas concretas para su efectiva mitigación hasta que puedan ser asumibles por la organización, todo ello a modo de Plan de Prevención de Riesgos que contiene las medidas legales y técnicas que podrían aplicarse por cada Ayuntamiento a estos efectos de reducción del nivel de riesgo inicial detectado hasta su nivel de bajo o muy bajo.

A efectos prácticos los entregables de esta Actividad que en conjunto configuran el Mapa de Riesgos y el Plan de Prevención de cada municipio se han agrupado en los tres informes siguientes que se acompañan en el Anexo III, bajo la denominación siguiente.

- INFORME DE ANALISIS DE RIESGOS (Riesgos detectados y evaluación)

- INFORME DE AMENAZAS (medidas a implantar para su minoración)

- INFORME SOBRE MEDIDAS DE SEGURIDAD ENS (riesgos detectados del Esquema Nacional de Seguridad)

Informe de análisis de riesgos (riesgos detectados)

Este documento contiene los siguientes apartados

1. Identificación del Responsable de los tratamientos (el Ayuntamiento en cuestión)

2. Una descripción de los tratamientos que se realizan por dicho responsable con la denominación de "ficheros" de tratamiento y que constituyen la base del RAT (registro de tratamiento de Datos Personales)

3. Un Análisis de Riesgos de Privacidad que trata de responder a las preguntas de **qué se hace con los DP** en el Ayuntamiento en cuestión y **cómo se hacen estos tratamientos** y se desarrolla en los siguientes puntos:

3.1. QUE SE HACE CON LOS DATOS PERSONALES EN CADA AYUNTAMIENTO

- ESTRUCTURA DE DATOS

  Se describe la finalidad del tratamiento, el origen de los datos, la categoría de los mismos y la de los interesados afectados por el tratamiento

3.2. COMO DE HACE ESE TRATAMIENTO DE DATOS PERSONALES EN CADA AYUNTAMIENTO

Se analiza la organización en todas las dimensiones siguientes:

- CUMPLIMIENTO NORMATIVO (Principios del Tratamiento/Responsabilidad del Tratamiento/Política de Información/Política de Seguridad/Medidas de Protección de datos existentes)

- ORGANIZACIÓN (Locales/ delegaciones/sedes y Departamentos en los que la organización se estructura)

- RECURSOS (Recursos con los que trata los DP, Hardware, Software, Mobiliario y Soportes de todo tipo)

- SEGURIDAD DESDE EL DISEÑO Y POR DEFECTO (Se analizan los tratamientos bajo las 5 dimensiones de la seguridad en las AAPP, la confidencialidad/integridad/disponibilidad/autenticidad/trazabilidad)

- AMENAZAS (Se avanza en este informe el informe de amenazas que también se entrega por separado a efectos de su uso por los responsables de aplicar las

medidas propuestas en el mismo sin tener que acceder al informe entero que aquí se trata)

Informe de amenazas de protección de datos (medidas a implantar)

Analizados pues qué datos personales son objeto de tratamiento y cómo se lleva a cabo el mismo por los distintos Ayuntamientos, este informe, como se ha apuntado, refleja ahora las amenazas concretas detectadas sobre dichos tratamientos y las medidas propuestas – omitiendo el extenso análisis de riesgos que ya consta en el informe anterior— en orden a poder mitigar y reducir el riesgo hasta un nivel asumible bajo o muy bajo por cada amenaza detectada.

Informe de sobre medidas de seguridad ENS (nivel de riesgos detectados en relación al ENS)

Este informe resume el análisis de los riesgos detectados con ocasión de la aplicación de las medidas de seguridad que exige el Esquema Nacional de Seguridad en relación a la protección de Datos personales por parte de una administración Pública de conformidad con la D.A. 1ª de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Se establecen aquí únicamente los niveles de riesgo detectados y se deja para una ulterior actuación la propuesta de medidas correctoras por exceder en mucho el alcance de este proyecto.

De la selección de Ayuntamientos nos encontramos con todo el espectro de situaciones:

Ayuntamientos que implementan y auditan el sistema de seguridad de la información por la Sindicatura de Comptes al sumar más de 50.000 habitantes

Ayuntamientos medianos que no han implementado las medidas conforme al ENS

SALVEDADES IMPORTANTES

Existen **Ayuntamientos pequeños** que cumplen las medidas del ENS únicamente en lo relativo a aquellos servicios prestados a través de las sedes electrónicas que son gestionadas por terceros prestadores de servicios de confianza certificados en ENS, con la importante salvedad que hay que hacer aquí de que no solamente (1) hay servicios que se prestan fuera de la sede electrónica que no cumplen con dicha normativa, si no que, (2) incluso los que se prestan a través de dicha plataforma no garantizan el cumplimiento de dichas medidas respecto de la información que reciben o emiten del propio AYUNTAMIENTO. Es decir, la información en sí misma, incluida la de los datos personales

de empleados y ciudadanos, como activo, no está protegida conforme a las medidas ENS, ya que se genera y/o transmite fuera de la sede electrónica y es obvio que una vez fuera de ella no se garantiza el cumplimento de estas medidas. (por ejemplo, los servicios sociales, becas, asistencia médica, etc,..)

Y también es importante destacar que aquellos grandes municipios auditados (Benidorm, Elche, Alicante) tampoco cumplen satisfactoriamente el ENS por cuanto (y esto es imputable a la propia administración central) las propias guias y normas hacen que deba calificarse de ALTO el riesgo y, por ende, llevar al consistorio a adopción de medidas que no están a su alcance en cuanto se tratan datos sensibles por así establecerlo la propia normativa GDPR-LOPD y esto es un auténtico problema en el ámbito de los EELL que son los que menos recursos disponen para cumplir estas altas exigencias en materia de privacidad de las AAPP. La solución, a menudo, es limitar el alcance de aplicabilidad del propio esquema para evitar esta calificación ALTO.

Anexos

ANEXO. I CUESTIONARIO CHECK LIST GDPR
https://drive.google.com/drive/u/0/folders/1tySISwfW5mAuUtdUWscfezxpw1wlHzMN

ANEXO II. CUESTIONARIO ENS
https://drive.google.com/drive/u/0/folders/1SpYV_VvzWCsP6HgVl-G6gJYQXg6C3IQX

ANEXO III. INFORMES – ENTREGABLES ACTIVIDADES 2 Y 3
https://drive.google.com/drive/u/0/folders/1NssQxKz-Jlb3Eny4FsIqL5rzV8-ys30M

Declaración de Riesgos

La naturaleza singularmente técnica de los trabajos necesarios para implementar con éxito la fase de "obtención de información" por parte de los consistorios seleccionados (se han de inventariar activos, ficheros, departamentos, medidas de seguridad, locales y ubicaciones, etc,..) ha puesto de manifiesto que los ayuntamientos mas modestos no tienen personal formado en materia de protección de datos, si bien tiene el apoyo de la Diputación de Alicante, que precisamente en estos momentos están pasando por una reestructuración importante en la Oficina Provincial de Protección de Datos (órgano que presta servicios en materia de protección de datos a estos pequeños consistorios) pasando auditorías, etc,.

En algunos casos se han detectado discrepancias entre la encuesta recibida y la información disponible en abierto a través de la página web. Esto a veces es consecuencia que la persona que ha rellenado la encuesta está sustituyendo al realmente encargado de la protección de datos. Hemos tomado como cierta por entender que puede estar desactualizada la web aquellas respuestas que maximizan los indicadores dado que entendemos que difícilmente se quitan prestaciones sino que mas bien se añaden nuevas.