RECOMENDACIONES

Tal como se describe en el punto 2 del Art. 96 del R.D. 1720/2007 "El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas. "

En los puntos anteriores se han incluido los datos, hechos y observaciones en los que se basa el auditor para proponer medidas correctoras. A continuación se exponen para cada uno de los apartados que propuestas recomienda el auditor. Respecto a los datos hechos y observaciones han sido enumerados a lo largo de este documento.

1. REVISIÓN DEL DOCUMENTO DE SEGURIDAD

El sistema informático y de ficheros auditado mantienen las medidas de seguridad que en un principio pudieran ser suficientes y lógicas para preservar la información vital del Ayuntamiento.

1.1 Comprobación del contenido y alcance.

- Debe tener una mayor difusión entre los usuarios del fichero de forma que para cada empleado del Ayuntamiento y usuario sea éste una herramienta más en su quehacer diario
- El documento de seguridad debe incluir los nombramientos de las diferentes personas como responsable del fichero, responsable de seguridad, etc.
- Documentar todos los procesos que afectan al documento de seguridad como son los controles que se hacen con un carácter mensual, medidas sobre la reutilización de soportes, periodos de contraseñas, etc.

1.2 Revisión de las políticas relacionadas con el Documento de seguridad

- El documento debe tener una mayor difusión entre los empleados y debe ser actualizado en el caso de descubrirse unas mejores prácticas que la que se estén realizando.
- El documento debe tener difusión entre los diferentes proveedores y colaboradores externos.

1.3 Conocimiento práctico entre los empleados

- Los empleados deben no sólo conocer la existencia del documento de seguridad del fichero que le afecta como usuario, sino además poner en práctica el contenido del mismo especialmente en la comunicación de las incidencias, la aplicación de los controles y medidas de seguridad, , etc.

1.4 Revisión del documento

- El documento no ha sido revisado desde su creación y se recomienda su evolución continua. También se recomienda que se eviten los procedimientos que son técnicos y son responsabilidad de sistemas haciendo mención a ellos según necesidad

2. ANÁLISIS DE LOS SISTEMAS DE INFORMACIÓN

Este apartado de la auditoría es correcto y está bien documentado en el informe de auditoría.

3. IDENTIFICACIÓN, AUTENTICACIÓN Y CONTROLES DE ACCESO

Puesto que es el Ayuntamiento posee un dominio/servidor en red utilizado un Sistema Operativo Windows Server, debiera de nombrarse en el documento de seguridad ya que su utilización permite dar mayores garantías de cumplimiento de la materia de Protección de datos. Se recomienda:

- No utilizar usuarios genéricos, que imposibilitan el establecimiento de las medidas de control.

Las medidas de control permiten observar la actividad que desarrollan los diferentes usuarios de la corporación municipal.

4. REGISTRO DE ACCESOS

La monitorización de los accesos que se tiene activada en la actualidad es suficiente para el cumplimiento de la Ley.

5. GESTIÓN DE SOPORTES Y DOCUMENTOS

Respecto al uso y tratamiento de los soportes de datos, se obtienen las siguientes conclusiones y recomendaciones.

- Se deberá verificar que el listado de soportes y documentos que contienen datos de carácter personal es revisado periódicamente.
- El sistema de etiquetado de la documentación debería permitir la identificación de su contenido al personal autorizado, dificultando la comprensión e identificación al personal no autorizado.

6. COPIAS DE SEGURIDAD

La metodología empleada para la realización de las copias de seguridad es adecuada.

- Las copias que contienen datos de carácter persona es interesante que se encuentren cifradas para evitar que puedan ser recuperadas por personal no autorizado y en otros sistemas, siendo obligatorio para los datos de carácter personal de nivel alto.
- El Ayuntamiento debería realizar periódicamente, 3 ó 6 meses, para verificar que las copias de seguridad y respaldo son correctas y en el caso de necesidad, al recurrir a las mismas, el resultado será satisfactorio.

7. REGISTRO DE INCIDENCIAS

El Ayuntamiento debería mantener un registro de incidencias y procedimientos documentados para la notificación y gestión de las mismas.

Además debería proporcionar al personal la información necesaria para que todas las incidencias de seguridad fueran notificadas y puestas en conocimiento del personal encargado de su gestión o tratamiento.

Las recomendaciones que se proponen son las siguientes:

Se sugiere una formación a los usuarios de los diferentes ficheros sobre la gestión y reconocimiento de una incidencia, recordatorios del cumplimiento de la LOPD, etc.

8. PRUEBAS CON DATOS REALES

Al no realizarse pruebas con datos reales, no existe mayor problema en este apartado.

De todas formas se debe considerar que si en un futuro se hicieran pruebas con datos reales, las medidas de seguridad que se aplican en producción deben ser aplicadas a pruebas

9. TRANSMISIONES

La transmisión de datos mediante los sistemas de telecomunicaciones se realiza mediante el establecimiento de redes privadas virtuales.

Debe incluirse una política sobre el acceso a Internet y las telecomunicaciones, prestando especial atención en el caso de transmitirse datos de nivel alto, que tendrían que cumplir las características que especifica el RD 1720/2007.

10. REGISTROS DE ACCESO FUERA DE LOS LOCALES DE TRABAJO

La monitorización de los accesos que se tiene activada en la actualidad es suficiente para el cumplimiento de la Ley.

11. FICHEROS TEMPORALES

La utilización de ficheros temporales que contienen datos de carácter personal, deberán cumplir los usuarios que necesiten de su uso para realizar el trabajo, tendrían que poseer el mismo nivel que el fichero original, ya sea un documento en papel o digital.

12. CONTROL DE ACCESO FÍSICO

El acceso a las salas está restringido exclusivamente al personal de autorizado por lo que en un principio parece que la seguridad física de los mismos es la correcta.

Tras el examen de los diferentes puntos de la L.O. 15/1999 y RD 1720/2007 que afectan a este punto, no se realiza ninguna recomendación especial pero se recuerda que el tratamiento informático se encuentra, en líneas generales, al máximo de lo exigible por lo recursos que posee.

13. CRITERIOS DE ARCHIVADO Y ALMACENAMIENTO DE FICHEROS NO AUTOMATIZADOS.

Al tratarse de organismos públicos como son los Ayuntamientos, el archivado y almacenamiento de ficheros no automatizados lo realizan siguiendo las pautas establecidas por motivos legales.

14. COPIA O REPRODUCCIÓN DE FICHEROS NO AUTOMATIZADOS

La utilización de copias o reproducción de ficheros no automatizados tienen que cumplir el mismo nivel de seguridad que el fichero original.

15. ACCESO A LOS DOCUMENTOS NO AUTOMATIZADOS.

Existe un registro de acceso en cada uno de los documentos que contienen datos de carácter personal de nivel alto.

En el caso de que tengan que tener acceso a parte de los documentos no automatizados personal externo al Ayuntamiento, se deberá otorgar la autorización pertinente, debiéndose quedar está registrada.

16. TRASLADO DE LA DOCUMENTACIÓN NO AUTOMATIZADA.

Durante el traslado de la documentación no automatizada se deberán establecer las medidas de seguridad necesarias para que dicha información no sea accesible o manipulable por personal no autorizado.

17. FUNCIONES DEL RESPONSABLE DE SEGURIDAD

El resultado de la auditoria de este apartado descubre oportunidades de mejora. De esta manera se recomienda lo siguiente:

- Elaborar un cuadro de controles en el tiempo del sistema y en la documentación que deberá revisar el responsable de seguridad
- Conservar los informes que elabore el responsable de seguridad para poder hacer evolucionar al sistema informático
- Definir en el tiempo las revisiones a realizar.

CONCLUSIÓN FINAL

En opinión del auditor, la evolución de la implantación realizada en esta materia en la que se funden aspectos tanto informáticos como jurídicos, se ha realizado de una manera acertada.

Debe evitarse la asociación que en el día a día hacemos de la palabra “dato” con sistemas informáticos y por derivación con la informática. En realidad estamos hablando de información sin importarnos el soporte ya sea automatizado o no.

En este punto debe leerse la definición que nos da la LOPD y en este caso aplicar el Art. 3 “a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables”.

Parece quedar claro que hablamos de información y deben ser los diferentes departamentos propietarios de la misma los encargados de protegerla, exigiendo al Dpto. de informática en el caso de existir, la colaboración total y absoluta en este tema.

Centrándonos en esta auditoría:

- Deben verificarse cada cierto tiempo el cumplimiento de los contratos con los diferentes proveedores y clientes para que se ajusten al Art. 12 de la L.O. 15/1999 y no incurrir en cesión no autorizada de información de carácter personal.
- Debieran crearse normas de actuación, de aplicación por parte del personal, cuando se realice una llamada telefónica o una visita a un ciudadano de manera que no se vulneren los derechos que otorga la Ley 15/1999, a la vez que marca un guión de actuación y funde aspecto de la confidencialidad y de la protección de datos.

- También debe tener en consideración aquellas recomendaciones que han sido reflejadas en el apartado Recomendaciones de este mismo documento.

- Revisar los ficheros inscritos ante la Agencia Española de Protección de Datos (AGPD), para verificar que siguen manteniendo el mismo nivel de seguridad y aplicar las medidas indicadas en el RD 1720/2007.

- Las copias de seguridad de los ficheros que contienen datos de carácter personal, deberían estar sometidas a diferentes riesgos que los ficheros originales, esto es, tendrían que estar en ubicaciones diferentes a las originales.