INFORME DE AUDITORIA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL PARA

AYUNTAMIENTO DE VILLATOYA

(ART. 96 R.D. 1720/2007)

Auditado por:

EULEN SEGURIDAD, S.A.
Dpto. Consultoría de Seguridad

INDICE

INTRODUCCIÓN

El Reglamento de Desarrollo del RD 1720/2007, sobre los ficheros de carácter personal establece, cuando existen ficheros de nivel medio o alto: *Artículo 96* – Auditoría.

"1.-A partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa, que verifique el cumplimiento del presente título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el apartado anterior.

Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

2.-El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, 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.

3.-Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas."

FASES EN LA REALIZACIÓN DE LA AUDITORÍA

La auditoría se ha realizado conforme a la contratación por parte del Ayuntamiento de Albacete a EULEN Seguridad del "Servicio de Auditorias en los aspectos que marca la Ley Orgánica 15/1999 sobre Protección de Datos (LOPD), para realizarse en ayuntamientos de la Provincia y el Ayuntamiento de Albacete."

La auditoría se ha realizado según el RD 1720/2007, en el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal, se ha realizado durante el 11 julio 2011 y ha constado de las siguientes fases:

Conocimiento genérico del A*yuntamiento*, de los sistemas de información de que disponen y sus relaciones con los organismos oficiales, instituciones y empresas de servicios.

Elaboración de un programa de trabajo en el que se detallan las actividades o tareas a auditar, teniendo para ello en cuenta, por un lado, los requisitos de revisión impuestos por el Reglamento de Desarrollo en relación con la auditoría, artículo 96.

Realización del trabajo de campo, esto es, la revisión de las actividades incluidas en el plan de trabajo.

Análisis de los puntos débiles y obtención de conclusiones y recomendaciones.

Elaboración del informe.

PLAN DE TRABAJO

A partir del hecho de que la auditoría debe verificar el cumplimiento del Reglamento, según la Ley 13/1999 de Protección de Datos de Carácter Personal, el Plan de Trabajo incluye específicamente la comprobación de todos los artículos de aquel que sean de aplicación a tenor de los tipos de ficheros de que disponga el Ayuntamiento (Niveles medio y/o alto).

Para la realización organizada de esta auditoría se ha preparado una tabla de control denominada. Esta tabla esta divida en una serie de áreas, de manera que se puedan identificar aquellos ítems a auditar. De esta manera las áreas auditadas han sido las que a continuación se exponen:

1. REVISIÓN DEL DOCUMENTO DE SEGURIDAD
2. FUNCIONES DEL RESPONSABLE DE SEGURIDAD
3. ANÁLISIS DE LOS SISTEMAS DE INFORMACIÓN
4. IDENTIFICACIÓN, AUTENTICACIÓN Y CONTROLES DE ACCESO
5. REGISTRO DE ACCESOS
6. GESTIÓN DE SOPORTES
7. COPIAS DE SEGURIDAD
8. REGISTRO DE INCIDENCIAS
9. PRUEBAS CON DATOS REALES
10. TRANSMISIONES
11. REGISTROS DE ACCESO FUERA DE LOS LOCALES DE TRABAJO
12. FICHEROS TEMPORALES
13. CONTROL DE ACCESO FÍSICO
14. FICHEROS NO AUTOMATIZADOS
    - 14.1 CRITERIOS DE ARCHIVADO Y ALMACENAMIENTO
    - 14.2 COPIA O REPRODUCCIÓN
    - 14.3 ACCESO A LA DOCUMENTACIÓN
    - 14.4 TRASLADO DE LA DOCUMENTACIÓN

A continuación se incluye la información referente cada uno de los puntos auditados de las áreas anteriormente mencionadas, así como los resultados obtenidos en cada apartado.

1. REVISIÓN DEL DOCUMENTO DE SEGURIDAD

El objetivo de la revisión del Documento de Seguridad, que deben tener todas las empresas y organismos públicos que posean ficheros con datos personales es doble;

- Por un lado, el auditor analizará que su contenido cumpla con los requisitos establecidos en el Reglamento de desarrollo de la LOPD (RD 1720/2007).
- Y en segundo lugar, permite al auditor identificar aquellos procedimientos y controles de seguridad que ha definido la organización, para su posterior verificación de cumplimiento.

Además de la revisión del contenido del Documento de Seguridad, se han auditado en el Ayuntamiento aquellos procedimientos que afectan tanto a su desarrollo, mantenimiento, como a su actualización.

En el caso de esta auditoría, se comprueba la existencia de un único Documento de Seguridad y procedimientos para todos los ficheros.

A continuación se exponen todos estos aspectos auditados.

1.1. COMPROBACIÓN DEL CONTENIDO Y ALCANCE

En este apartado se verificará el contenido y el alcance del Documento de Seguridad que posee el Ayuntamiento.

PUNTO AUDITADO	CONCLUSIÓN
Medidas, controles, procedimientos, normas y estándares de seguridad.	Satisfactorio. El Documento de Seguridad incluye todos los apartados exigidos por el Reglamento de Desarrollo.
Relación de las funciones y obligaciones del personal	Satisfactorio. Se incluyen las figuras, funciones y responsabilidades que parecen las lógicas para la coordinación de la seguridad y la gestión de los ficheros que tiene el Ayuntamiento.
Estructura de los ficheros con datos personales.	Satisfactorio. Se presentan como Anexos dentro del Documento de Seguridad, aunque algunos de ellos carecen de completitud.
Procedimientos de notificación y gestión de incidencias.	No satisfactorio. No poseen de documentos para la notificación y gestión de incidencias.
Procedimientos de realización de copias de respaldo y de recuperación de datos.	Satisfactorio. Tienen procedimiento para las copias de respaldo y para la

PUNTO AUDITADO	CONCLUSIÓN
	recuperación de los datos.
Relación de personal autorizado a conceder, alterar o anular el acceso sobre datos y recursos.	Satisfactorio. Incluido en el Documento de Seguridad, aunque no está actualizado.
Identificación del responsable o responsables de seguridad.	Satisfactorio. Incluido en el Documento de Seguridad.
Relación de controles periódicos a realizar para verificar el cumplimiento del documento.	Satisfactorio.
Medidas a adoptar cuando un soporte vaya a ser desechado o reutilizado	Satisfactorio. Sería recomienda incluir dentro de la gestión de soportes las buenas prácticas recogidas en la ISO 27002:2007 sobre eliminación de soportes.
Relación de personal autorizado a acceder a los locales donde se encuentren ubicados los sistemas que tratan datos personales.	Satisfactorio. Sólo accede personal autorizado por el Ayuntamiento.
Relación de personal autorizado a acceder a los soportes de datos.	Satisfactorio. Incluido en cada uno de los ficheros el personal autorizado.
Período máximo de vida de las contraseñas.	No Satisfactorio. No se obliga al cambio de contraseñas periódicamente. Se recomienda actualizar las buenas prácticas de vida y uso de contraseñas de la ISO 27002:2007

1.2. REVISIÓN DEL DOCUMENTO DE SEGURIDAD:

Se evalúa la revisión, actualización, comunicación y difusión del Documento de Seguridad.

PUNTO AUDITADO	CONCLUSIÓN
Evaluar la existencia de difusión del documento entre el personal del Ayuntamiento.	Satisfactorio. Se ha difundido al personal que utiliza datos de carácter personal.
Procedimientos para la revisión y actualización del documento.	Satisfactorio. Existe un apartado dentro del mismo que indica su revisión y actualización.

1.3. REVISIÓN DEL GRADO DE ACTUALIZACIÓN.

Para realizar la evaluación del grado de actualización se ha procedido a realizar un análisis de la adecuación y efectividad de los controles que en la práctica existen en el Ayuntamiento y contrastarlo con los controles que están identificados e incluidos en el

Documento de Seguridad, por lo que este ha sido el último punto en cumplimentarse, tras finalizar la auditoría.

El Documento de Seguridad al tratarse de un documento vivo y de evolución continua a lo largo del tiempo, así como sus procedimientos y registros que le acompañan, deben mantenerse en todo momento actualizado y ser revisado siempre que se produzcan cambios relevantes en los sistemas de información, en el sistema de tratamiento empleado en el Ayuntamiento, en el contenido de la información incluida en los ficheros o tratamientos, o en su caso, como consecuencia de los controles periódicos realizados.

En todo caso se entenderá que un cambio es relevante, cuando pueda repercutir de alguna manera en el cumplimiento de las medidas de seguridad implantadas en el Ayuntamiento. Por esto se ha realizado una comprobación de la una evolución en los contenidos del documento de seguridad.

La conclusión es que el Documento de Seguridad y los procedimientos para todos los ficheros registrados no han sido revisados desde su creación.

2. FUNCIONES DEL RESPONSABLE DE SEGURIDAD

El Reglamento obliga a nombrar uno o más Responsables de Seguridad por la mera existencia de ficheros de nivel medio o alto, según el *Artículo 95 – Responsable de seguridad*:

"En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento."

En la auditoría se ha comprobado si las funciones definidas para el responsable de seguridad son coherentes con las definidas en el Reglamento y se ha procedido a realizar una evaluación del grado de cumplimiento de las mismas.

El resultado obtenido, es el que a continuación se detalla:

PUNTO AUDITADO	CONCLUSIÓN
Evidenciar si se ha nombrado al menos un Responsable de Seguridad en el Ayuntamiento.	Satisfactorio. En el Ayuntamiento sólo hay un Responsable de Seguridad
Estudiar y analizar las funciones encomendadas a cada uno de los responsables de seguridad	Satisfactorio. Existen funciones especificas y detalladas en el Documento de Seguridad
Determinar si entre ellas se encuentran aquellas especificadas en el Reglamento para los ficheros de Nivel Alto	Satisfactorio. Se encuentran las específicas a ficheros de Nivel Alto.
Analizar el grado de cumplimiento de las funciones encomendadas	Satisfactorio.
Estudiar y analizar los controles definidos para su realización por parte de los responsables de seguridad y comprobar su operatividad y grado de adecuación	Satisfactorio aunque puede ser necesaria una revisión de las funciones del responsable de seguridad de manera que se defina en el tiempo.

3. ANÁLISIS DE LOS SISTEMAS DE INFORMACIÓN

El objetivo de este apartado es determinar aquellos sistemas de información que contienen datos personales, e identificar los distintos niveles de los ficheros existentes. La importancia de esta tarea reside en que el cumplimiento de determinadas y específicas medidas de seguridad sólo exigidas por el Reglamento a los ficheros de nivel Medio y Alto.

La identificación de los sistemas que contienen estos ficheros puede permitir al Ayuntamiento a delimitar las medidas de seguridad exclusivamente a aquellas aplicaciones que precisen de las mismas, lo que puede redundar en un abaratamiento de costes. En segundo lugar, este análisis de los sistemas de información permite al auditor centrar la revisión de algunos de los controles exclusivamente en aquellos sistemas y ficheros para los que, en función de su nivel, el Reglamento exige su aplicación.

Para la realización de este punto, el auditor solicitó un inventario de ficheros y sistemas de información que contuviesen datos personales, que en el caso del Ayuntamiento cuenta con una listad de documentos. El inventario habrá sido elaborado probablemente en el mismo momento que el propio documento de seguridad.

PUNTO AUDITADO	CONCLUSIÓN
Determinar los campos (de los ficheros) que reflejan datos de nivel medio o alto.	Cumplimentado y Satisfactorio.
Detectar todos los ficheros que incluyen alguno de esos campos y además algún otro que permita identificar a la persona.	Satisfactorio.
Detectar todos los ficheros que incluyen algún dato identificativo de la persona.	Satisfactorio
Con los ficheros así clasificados en niveles, verificar que la estructura de esos ficheros está incluida en el Documento de Seguridad.	Satisfactorio. La información se encuentra en explícita en los Anexos del Documento de Seguridad.

4. IDENTIFICACIÓN, AUTENTICACIÓN Y CONTROLES DE ACCESO

Para cada uno de los sistemas que contienen datos de carácter personal, el auditor ha revisado los controles y normas relacionados con la identificación y autenticación de usuarios, así como los derechos de acceso concedidos.

El resultado auditado de esta es el siguiente:

PUNTO AUDITADO	CONCLUSIÓN
Comprobar que existe una relación de usuarios autorizados a acceder a los sistemas y que incluye los tipos de acceso permitidos	Satisfactorio. La relación de usuarios se encuentra en un anexo del Documento de Seguridad
Verificar que en la práctica los usuarios dados de alta en los sistemas y los tipos de accesos a ellos concedidos son coherentes con los establecidos en el Documento de Seguridad.	Satisfactorio. Se ha realizado un muestreo de los accesos, que parecen coherentes. (Todo el personal del Ayuntamiento accede a todo, al ser personal muy limitado en el Ayuntamiento).
Comprobar que los derechos de acceso concedidos a los usuarios son los necesarios y suficientes para el ejercicio de las funciones que tienen encomendadas, las cuales a su vez se encuentran –o deben estar- documentadas en el Documento de Seguridad.	Satisfactorio. Los derechos de acceso son suficientes y correctos y están documentados en el Documento de Seguridad.
Verificar que no hay dados de alta en el sistema cuentas de usuario genéricas, es decir, utilizadas por más de una persona, no permitiendo por tanto la identificación de la persona física que las ha utilizado.	En el Ayuntamiento todos los usuarios tienen cuentas personales e intransferibles. No existen cuentas genéricas.
Comprobar que en la práctica las personas que tienen atribuciones y privilegios dentro del sistema para conceder derechos de acceso son las autorizadas e incluidas en el Documento de Seguridad.	Satisfactorio.
Verificar que el sistema de autenticación de usuarios guarda las contraseñas encriptadas.	Satisfactorio. Utilizan el cifrado de Microsoft Windows.
Comprobar que en el sistema están habilitadas para todas las cuentas de usuario las opciones que permiten establecer un número máximo de intentos de conexión y un período máximo de vigencia para la contraseña,	No satisfactorio. No se verifica que dichas acciones están implantadas ni habilitadas.

PUNTO AUDITADO	CONCLUSIÓN
coincidente con el establecido en el Documento de Seguridad	
Analizar los procedimientos de asignación y distribución de contraseñas.	Satisfactorio. La distribución y asignación de contraseñas se realiza verbalmente.

5. REGISTRO DE ACCESOS

El registro de acceso, tal como obliga el R.D.: 1720/2007, en su *Artículo 103*, debe contener aquella información que permita al Responsable de Seguridad evaluar la integridad en el tiempo del fichero.

Se han realizado las siguientes comprobaciones:

PUNTO AUDITADO	CONCLUSIÓN
Comprobar la existencia de un registro de accesos a datos no automatizados o mixtos de nivel alto	La mayoría de los ficheros catalogados con nivel alto, en la actualidad ya no lo son, por lo que no sería obligatoria la existencia de registros de acceso para ficheros de nivel alto.
Verificar que la información incluida en el Registro de Accesos cumple los requisitos del Reglamento	Satisfactorio.
Comprobar que están activados los parámetros de activación del Registro para todos los ficheros de Nivel Alto.	Satisfactorio.
Verificar si el acceso a la documentación, así como la generación de copias o reproducción de documentos se limita exclusivamente al personal autorizado	Satisfactorio. Solo accede a la documentación personal autorizado del propio Ayuntamiento.

6. GESTIÓN DE SOPORTES Y DOCUMENTOS

En relación con los soportes de datos, el auditor ha revisado varios aspectos relativos a:

- Identificación de los soportes
- Inventario de soportes
- Registro de entrada/salida de soportes

PUNTO AUDITADO	CONCLUSIÓN
Verificar que existe un inventario de los soportes y documentos que contienen datos de carácter personal.	Satisfactorio. Poseen un inventario actualizado de los soportes y documentos.
Verificar si los soportes con datos de carácter personal considerados especialmente sensibles por el Ayuntamiento, se utilizan sistemas de etiquetado que permitan la identificación de su contenido al personal autorizado y que además dificulte su identificación al personal no autorizado	No Satisfactorio. Las etiquetas están en claro, aunque ubicadas en zonas de acceso restringido.
Verificar si el inventario está actualizado y se verifica periódicamente.	Satisfactorio. El inventario está actualizado, pero no se verifica periódicamente.
Verificar los accesos a los posibles almacenamientos de soportes y comprobar que exclusivamente pueden acceder a ellos las personas autorizadas en el Documento de Seguridad	Satisfactorio. Sólo accede personal autorizado incluido en el Documento de Seguridad.
Analizar los procedimientos en relación con la salida de soportes fuera de su almacenamiento habitual.	Satisfactorio. Existe un registro para la E/S de soportes.
Evaluar los estándares de distribución y envío de estos soportes.	Satisfactorio. Las medidas de seguridad durante el traslado dependerán del tipo de soporte o documento que salga de las instalaciones del Ayuntamiento.
Verificar el Registro de Entrada y Salida de Soportes y comprobar que en él se incluyen los soportes del punto anterior y los desplazamientos que realizan.	Satisfactorio.
Verificar que el Registro de Entrada y Salida refleja la información requerida por el Reglamento.	Cumple con la información requerida por el Reglamento.

PUNTO AUDITADO	CONCLUSIÓN
Analizar los procedimientos de actualización del Registro de Entrada y Salida en relación con el movimiento de soportes.	Satisfactorio.
Comprobar, en el caso de que el Inventario de Soportes y/o el Registro de Entrada/Salida estén informatizados, que se realizan copias de seguridad de ellos, al menos, una vez a la semana.	Satisfactorio. El ayuntamiento realiza una copia con la periodicidad necesaria para salvaguardar su información.

7. COPIAS DE RESPALDO Y RECUPERACIÓN

Los procedimientos respecto a las copias de seguridad y restauración del sistema son el punto crítico en cualquier sistema informático.

Según el *Artículo 94 – Copias de Respaldo y recuperación*:

"1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad."

Para este apartado el auditor ha comprobado los siguientes aspectos:

PUNTO AUDITADO	CONCLUSIÓN
Analizar los procedimientos para la realización de las copias de seguridad.	Satisfactorio. Los procedimientos son válidos y adecuados.
Verificar que los procedimientos aseguran que, de todos los ficheros con datos de carácter personal, se realiza copia al menos una vez cada semana.	Satisfactorio. Se realizan copias a diario y/o semanales.
Comprobar si los procedimientos establecidos para la recuperación de los datos, garantizan que éstos se encuentran en el estado en que se encontraban antes de producirse la pérdida o destrucción.	Satisfactorio, periódicamente se realizan pruebas para garantizar la integridad de las copias de seguridad.
Analizar los controles existentes para la detección de incidencias previas a la realización de las pruebas.	Satisfactorio.

PUNTO AUDITADO	CONCLUSIÓN
Verificar si el responsable del fichero revisa al menos semestralmente el funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.	Satisfactorio. El Responsable del fichero, verifica periódicamente que las copias de respaldo y de recuperación se han realizado correctamente.
Evaluar los controles sobre el acceso físico a las copias de seguridad.	Satisfactorio. La sala dónde se realizan las copias de seguridad sólo es accesible por personal autorizado
Verificar que sólo las personas con acceso autorizado en el documento de seguridad tienen acceso a los soportes que contienen las copias de seguridad.	Satisfactorio. Se ha verificado in situ, dicha acción.
Comprobar que las copias de seguridad de ficheros de nivel alto incluyen los ficheros cifrados si estas copias se transportan fuera de las instalaciones.	La mayoría de los datos de nivel alto del Ayuntamiento han variado su nivel, por lo que deben modificarlo ante la AGPD.

8. REGISTRO DE INCIDENCIAS

El registro de incidencias es la parte del Documento de Seguridad que permitirá la realización de estudios e informes que permitan evolucionar la seguridad dentro del sistema informático de la organización. Una incidencia será todo aquel evento que ponga en peligro la integridad física y/o lógica del fichero.

Los aspectos auditados han sido:

PUNTO AUDITADO	CONCLUSIÓN
Comprobar que está claramente especificado que tipos de sucesos se consideran incidencia de acuerdo con la definición que del término realiza el Reglamento.	Satisfactorio.
Comprobar que los usuarios conocen que tipo de situaciones deben reportar como incidencia.	Conocen las principales situaciones en las que deben reportar como incidencia.
Analizar los procedimientos para la notificación de incidencias, ver que están operativos y comprobar que son conocidos por todos los usuarios.	Satisfactorio. Los procedimientos analizados son válidos.
Evaluar si los procedimientos seguidos en la práctica se corresponden con aquellos definidos en el Documento de Seguridad.	Satisfactorio.
Verificar que la información guardada en el Registro de Incidencias cumple los requisitos establecidos por el Reglamento	No satisfactorio. El ayuntamiento no posee registro de incidencias.
Analizar los procedimientos de inscripción en el Registro de Incidencias.	Satisfactorio.
Si el registro está informatizado, comprobar que se realiza copias de seguridad de él	N/A

9. PRUEBAS CON DATOS REALES

El auditor ha comprobado, en primer lugar, cual es la política del Ayuntamiento en cuanto a la realización de pruebas con datos reales, siempre y cuando el Ayuntamiento las haya realizado, para a continuación analizar, en función de esa política, las normas y procedimientos definidos y verificar su cumplimiento.

En este caso no se realizan pruebas con datos reales y se han verificado los siguientes requisitos.

PUNTO AUDITADO	CONCLUSIÓN
Verificar que los controles y normas que están operativos para los ficheros en producción lo están también para los ficheros del entorno de pruebas.	*No se realizan pruebas con datos reales.*
Analizar los procedimientos para el entorno de pruebas en relación con: Identificación y autenticación de usuarios, control de accesos, políticas de contraseña y número máximo de intentos de conexión, inventario de soportes, registro de E/S de soportes, copias de seguridad, ficheros de soporte enviados fuera de las instalaciones y transmisiones cifradas, registro de incidencias, registro de acceso…	*No se realizan pruebas con datos reales*

10. TRANSMISIONES

Según el *Artículo 104 – Telecomunicaciones*: *"Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros."*

En este apartado deben tenerse en cuenta tanto las redes locales como las conexiones externas que puedan afectar a la integridad del fichero.

En este caso se ha auditado:

PUNTO AUDITADO	CONCLUSIÓN
Verificar si la transmisión de datos a través de redes públicas se realiza de forma cifrada (o por cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por un tercero).	Satisfactorio. Utilizan la red Sara, implementa medidas de seguridad entre las que destaca el establecimiento de redes privadas virtuales (VPN).

11. REGISTROS DE ACCESO FUERA DE LOS LOCALES DE TRABAJO

El auditor ha revisado si el Ayuntamiento ha trabajado con documentos que contuviesen datos de carácter personal, fuera de sus instalaciones, según se indica en el *Artículo 86 – Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento*:

"1. Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas."

En este caso se ha auditado:

PUNTO AUDITADO	CONCLUSIÓN
Comprobar si el Ayuntamiento dispone de ficheros que contenga datos de carácter personal, fuera de las instalaciones en las que está ubicado el fichero.	Sí, el Ayuntamiento posee otras instalaciones desde las que se acceden a ficheros que contienen datos de carácter personal.
Comprobar si la autorización para el almacenamiento de datos personales en dispositivos portátiles o los tratamientos fuera de los locales Han sido autorizados expresamente por el responsable del fichero	Satisfactorio. Existe autorización para tal fin.
Verificar si la autorización está incluida en el documento de seguridad.	Satisfactorio. Existe la autorización en el Documento de Seguridad.
Evidenciar si las medidas de seguridad aplicadas fuera de los locales garantizan la seguridad del fichero	Satisfactorio. Utilizan control de acceso físico y lógico. El personal que accede debe tener usuario del Ayuntamiento con los permisos pertinentes y realizar la conexión segura para su acceso.

12. FICHEROS TEMPORALES

Al igual que el tratamiento de los ficheros fuera de los locales, se debe tratar el uso de ficheros temporales, como se especifica en el RD 1720/2007 en su *Artículo 87 – Ficheros temporales o copias de trabajo de documentos.*

"1. Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81.

2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación."

En este caso se ha auditado: INDICAR ALGUNA PREGUNTA AUDITADA

PUNTO AUDITADO	CONCLUSIÓN
Verificar si cumplen los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales y/o auxiliares el mismo nivel de seguridad correspondiente al expresado en el RDLOPD.	Satisfactorio. Los ficheros temporales/copias de documentos mantienen el mismo nivel de seguridad que el fichero original.
Confirmar si se destruyen o borran los ficheros cuando ya no es necesario para los fines que motivaron su creación.	Satisfactorio. Dicha acción se realiza.

13. CONTROL DE ACCESO FÍSICO

Al igual que se implantan medidas de seguridad de acceso lógico a los sistemas informáticos y a los ficheros, el acceso físico a la sala dónde se ubican los equipos/servidores debe estar restringido exclusivamente a personal autorizado, tal y como se expone en el *Artículo 99 – Control de acceso físico. "Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información."*

Durante la auditoría se ha realizado las siguientes verificaciones:

PUNTO AUDITADO	CONCLUSIÓN
Comprobar la existencia, como parte del Documento de Seguridad, de una relación de usuarios con acceso autorizado a la sala dónde se ubican los equipos físicos que dan soporte a los sistemas de información.	Satisfactorio. Existe un listado de usuarios con acceso autorizado a los datos.
Verificar que la inclusión del personal en la relación anterior es coherente con las funciones que tienen encomendadas.	Satisfactorio. El acceso a los ficheros es por necesidad de conocer.
Analizar sí la concesión, alteración o anulación de accesos autorizados sobre datos y recursos la realiza exclusivamente el personal autorizado para ello.	Satisfactorio.
Comprobar que la relación es lógica (personal de limpieza, seguridad)	Satisfactorio. Solamente accede personal propio del Ayuntamiento.

14. FICHEROS NO AUTOMATIZADOS.

Durante la auditoría se ha evidenciado que la mayor parte de los ficheros que posee el Ayuntamiento que contienen datos de carácter personal, su tratamiento es mixto, por lo que para aquellos ficheros no automatizados (en formato papel), se deberán seguir los criterios que dicte el Reglamento.

14.1 CRITERIOS DE ARCHIVADO Y ALMACENAMIENTO

PUNTO AUDITADO	CONCLUSIÓN
Verificar si el Ayuntamiento posee unos criterios para el archivo de la documentación que posee datos de carácter personal.	Satisfactorio. Como organismos público que son, poseen criterios de archivado para la documentación.
Comprobar que los criterios garantizan la conservación de los documentos, localización, consulta y la posibilidad de ejercer los derechos ARC	Satisfactorio, cumplen con todo lo anterior.
Confirmar si el acceso a los ficheros físicos que contienen datos de carácter personal está limitado a personal autorizado.	Satisfactorio. Sólo pueden acceder a ellos personal autorizados.
Verificar si el almacenamiento de los documentos se realiza mediante dispositivos que obstaculicen su apertura.	Satisfactorio. La documentación se encuentra en una sala cerrada con llave.
Evidenciar sí el acceso a dicho almacenamiento es realizado exclusivamente por personal autorizado del Ayuntamiento	Satisfactorio. Sólo puede acceder a esta sala personal autorizado.

14.2 COPIA O REPRODUCCIÓN

PUNTO AUDITADO	CONCLUSIÓN
Verificar si se realizan copias de documentos que contienen datos de carácter personal.	Satisfactorio. Se realizan copias para uso temporal de los documentos
Analizar si dichas copias son desechadas o destruidas una vez dejan de ser útiles	Satisfactorio. Una vez finalizado su uso, la/s copia/s se destruyen.

14.3 ACCESO A LA DOCUMENTACIÓN

PUNTO AUDITADO	CONCLUSIÓN
Verificar si el acceso a la documentación se limita a personal autorizado.	Satisfactorio. Sólo pueden acceder a ellos personal autorizados.

PUNTO AUDITADO	CONCLUSIÓN
Evidenciar si se establecen mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios	Satisfactorios. Existe un registro de acceso en cada uno de los documentos que contienen datos de carácter personal de nivel alto.
Identificar si personal no incluido anteriormente, quede registrado de acuerdo al procedimiento establecido en el documento de seguridad	No aplica. Sólo puede acceder personal autorizado.

14.4 TRASLADO DE LA DOCUMENTACIÓN

PUNTO AUDITADO	CONCLUSIÓN
Verificar si se produce el traslado físico de documentación fuera de las instalaciones del Ayuntamiento.	Satisfactorio. Se toman las medidas necesarias para impedir el acceso o manipulación de la información.