SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

PRO.PD-10

PROCEDIMIENTO
AUDITORÍA INTERNA

Diputación de Córdoba	DIPUTACIÓN DE CÓRDOBA

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	PR.PD-10	DOCUMENTO:	PROCEDIMIENTO DE AUDITORIA INTERNA

REVISIÓN NÚMERO:	00	FECHA DE ENTRADA EN VIGOR:	15/11/2019

ES ORIGINAL:	☒	ES COPIA CONTROLADA:	☐	ES COPIA NO CONTROLADA:	☐

ELABORADOR POR:	REVISADO POR:	APROBADO POR:
TIC4YOU SL	DAVID YUBERO REY DPD DIPUTACIÓN DE CÓRDOBA	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN
		FECHA:
		15/11/2019

CONTROL DE CAMBIOS:

REVISIÓN Nº:	FECHA:	APARTADO MODIFICADO:	CAUSA DEL CAMBIO:	ENTRADA EN VIGOR:

DOCUMENTACIÓN OBSOLETA:	☐	FECHA:	

CLASIFICACIÓN DE LA INFORMACIÓN:

PÚBLICA:	☐	PUBLICABLE:	☒	USO INTERNO:	☐	CONFIDENCIAL:	☐	SECRETA:	☐

ÍNDICE

1. OBJETO

El objeto del presente procedimiento es establecer las responsabilidades y requisitos para la planificación y la realización de auditorías internas en la Diputación de Córdoba y en el Instituto Provincial de Bienestar Social, el Instituto Provincial de Cooperación con la Hacienda Local, el Instituto Provincial de Desarrollo Económico, el Consorcio Provincial de Prevención y Extinción de Incendios, el Patronato Provincial de Turismo de Córdoba, la Agencia Provincial de la Energía, la Fundación Provincial de Artes Plásticas Rafael Botí, la Empresa Provincial de Aguas de Córdoba, la Empresa Provincial de Residuos y Medio Ambiente y la Empresa Provincial de Informática (en adelante, la Diputación de Córdoba y su sector público institucional) que permitan probar, analizar y evaluar de manera periódica la efectividad de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento de datos, así como para informar de los resultados y mantener registros.

2. ALCANCE

Este procedimiento es de aplicación a todas las actividades de tratamiento de datos.

3. REFERENCIAS

Para la elaboración de este procedimiento se ha utilizado como referencia:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Artículo 58 Poderes, en el punto b)* llev*ar a cabo investigaciones en forma de auditorías de protección de datos.*
- Corrección de errores del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.
- Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Norma UNE-EN-ISO/IEC 27001:2017. “Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos”.

- Norma UNE-EN-ISO-9001:2015: “Sistemas de Gestión de la Calidad. Requisitos”.

4. RESPONSABILIDADES

La Diputación de Córdoba y su sector público institucional tendrán la responsabilidad de poner en marcha los mecanismos para verificar en qué medida se cumple el propio RGPD y cualquier norma complementaria de las autoridades de protección de datos que resulte aplicable, así como la normativa interna de la entidad y además su grado de alineamiento con el RGPD, y contratos y compromisos que afecten así como garantizar el cumplimiento de los mismos.

5. DESARROLLO

5.1. PLANIFICACIÓN

Las auditorías internas de la Diputación de Córdoba y su sector público institucional se programan anualmente por el responsable del tratamiento en coordinación con el DPD. La frecuencia mínima de realización es tal que al menos cada año se realice una auditoría completa de la medidas técnicas y organizativas ejecutadas para el cumplimiento del Reglamento.

A principios de año, el responsable del tratamiento, en función del estado e importancia de los procesos a auditar, así como de los resultados de auditorías previas, elabora el Plan Anual de Auditorías Internas, que se revisa y aprueba por el Comité de Seguridad.

Además de las auditorias previstas en el Plan Anual, se podrán proponer la realización de otras auditorias cuando

- Se hayan producido cambios significativos en la implantación, como cambios organizativos o modificaciones de procedimientos documentados.
- Se sospeche o se tenga certeza, basada en no conformidades documentadas, de que las actividades relativas a la protección de datos no cumplen las disposiciones previstas.
- Se deba verificar la implantación de acciones correctivas.

Si durante la vigencia del Plan se considera conveniente incluir alguna de estas auditorías extraordinarias u otras causas aconsejan modificar la planificación, el proceso a seguir para emitir el nuevo Plan es el mismo que el descrito para el original

5.2. EQUIPO AUDITOR

El personal que realiza auditorias debe estar cualificado previamente salvo que se trate de empresas externas de reconocido prestigio y experiencia demostrada.

El equipo auditor debe estar integrado de la siguiente forma:

- El Auditor Jefe, que será persona cualificada para ello.

- Otras personas que, por su competencia o por la misión que cumplen, sean de utilidad para el buen funcionamiento de la auditoria.

No podrán ser designados como auditores las personas relacionadas directamente con el área auditada, con objeto de garantizar la objetividad e imparcialidad del proceso de auditoría.

5.3. PREPARACIÓN

Para comenzar la auditoría, el equipo auditor podrá mantener una reunión con objeto de preparar cuestionarios adaptados al proceso a auditar que permitan hacer observaciones y entrevistas útiles, sirviendo de guía de trabajo.

El Plan de Auditoria será comunicado por el responsable del tratamiento al área/s a auditar, con la suficiente antelación para trasmitir al responsable del tratamiento las discrepancias y objeciones.

5.4. REALIZACIÓN

La auditoría se realizará por el equipo designado en las fechas indicadas en el Plan de Auditorias.

El auditor comprueba si las actividades relacionadas con la protección de datos se realizan de acuerdo a lo especificado en el REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del consejo de 27 de abril de 2016 relativo a la Protección de las Personas Físicas en lo que respecta al tratamiento de Datos Personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos-RGPD) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, recabando la presencia del responsable de la actividad auditada, o a la persona que éste delegue como interlocutor válido, para que facilite las evidencias objetivas y datos necesarios solicitados por los auditores para el cumplimiento satisfactorio de la actividad dentro del alcance fijado. Para ello puede serle de utilidad el listado de cumplimiento del RGPD recogido en el registro RG.PD-01_PRO.PD-10.

Las verificaciones a efectuar durante la auditoria son, en general, de la siguiente naturaleza:

- Revisión de los documentos de la implantación, para comprobar que la actividad auditada dispone de los que le son aplicables, controlando además que la emisión, distribución y control de los documentos es el adecuado.
- Examen de los registros y evidencias documentales que demuestren el cumplimiento de las medidas técnicas y organizativas de la implantación.
- Supervisión directa de las actividades realizadas, para comprobar si se desarrollan de la manera prevista en la documentación de la implantación.
- Comprobación y seguimiento de la implantación y efectividad de las acciones correctivas pendientes de auditorías anteriores.

En caso de detectar una posible deficiencia o no conformidad, se investigará hasta confirmarla o no, y una vez ratificada se averiguará la causa que produce la desviación.

Por cada no conformidad se cumplimenta el RG.PD-02_PRO.PD-10 Registro de No conformidades y Acciones Correctivas, dando un número correlativo a cada uno comenzando por el 01, donde el auditor

la describe analizando las causas y las accione correctivas adoptadas y firmando éste y el responsable del proceso auditado en calidad de conocimiento y aceptación.

5.5. INFORME

Tras la finalización de la auditoria, el Auditor Jefe realiza y difunde un Informe de Auditoria Interna RG.PD-03_PRO.PD-10, incluyendo todas las incidencias contrastadas de los procesos auditados, como evidencia de su realización.

Dicho Informe se facilita al responsable del tratamiento y al DPD y, si procede, se redactará de forma que permita extraer informes parciales para su entrega a los responsables de proceso.

5.6. SEGUIMIENTO Y CIERRE

El responsable del proceso auditado, con la colaboración que precise del responsable del tratamiento y demás personas que puedan estar implicadas, deberá emprender sin demora injustificada las acciones correctivas y preventivas para eliminar las no conformidades, reales o potenciales, detectadas durante la auditoría y sus causas

La aprobación de la acción correctiva o preventiva, se lleva a cabo por el Comité de Seguridad mediante firma en el Informe, designando al encargado de su ejecución, la fecha de implantación y de evaluación de la eficacia.

Si la acción deriva de una no conformidad abierta el Comité de Seguridad nombrará la persona responsable de su seguimiento y cierre**.**

6. REGISTROS/ANEXOS

- **RG.PD-01_PRO.PD-10 Listado de Cumplimiento del RGPD.**
- **RG.PD-02_PRO.PD-10 Registro de No Conformidades y Acciones Correctivas.**
- **RG.PD-03_PRO.PD-10 Informe de Auditoría Interna.**