JORNADA DE FORMACIÓN: DELEGADO DE PROTECCIÓN DE DATOS

Administración Local

JORNADA DE FORMACIÓN: DELEGADO DE PROTECCIÓN DE DATOS

Administración Local

JORNADA DE FORMACIÓN DPD ADMINISTRACIÓN AUTONÓMICA Y LOCAL

Diputación de Málaga, 28 de marzo de 2019

9:00 – 9:30
Inauguración
Mar España Martí
Directora de la AEPD
Jacobo Florido Gómez
Vicepresidente de la Diputación de Málaga

9:30 – 10:00

- *Introducción práctica al Reglamento general de protección de datos: Principios y licitud del tratamiento de datos personales* (***Agencia Española de Protección de Datos***).

10:00-10:30

- *El principio de responsabilidad proactiva: Registro de actividades de tratamiento, determinación de la base jurídica del tratamiento, cláusulas informativas, adaptación de contratos* (***Antonio Troncoso Reigada, Catedrático de Derecho Constitucional de la Universidad de Cádiz y ex-Director de la Agencia de Protección de Datos de la Comunidad de Madrid***).

10:30 – 11:15

- *El enfoque del riesgo: Análisis de riesgos, evaluaciones de impacto, consulta a la autoridad de control, medidas de seguridad. Brechas de seguridad* (***Luis de Salvador Carrasco, Agencia Española de Protección de Datos***)

11:15 – 11:45
Pausa

11:45 – 12:15

- *El Delegado de Protección de Datos (DPD), en particular en las entidades locales. El DPD en las reclamaciones en materia de protección de datos* (***Antonio Troncoso Reigada, Catedrático de Derecho Constitucional de la Universidad de Cádiz y ex-Director de la Agencia de Protección de Datos de la Comunidad de Madrid y Concepción Labao Moreno, Directora Delegada Gobierno Abierto Transparencia y Comunicación Corporativa Diputación de Málaga***)

12:15
Clausura
Manuel Medina Guerrero
Director del Consejo de Transparencia y Protección de Datos de Andalucía

Proyecto co-financiado por el programa Derechos, Igualdad y Ciudadanía de la Unión Europea

La aplicación del Reglamento General de Protección de Datos (EU) 2016/679 (RGPD) desde el pasado 25 de mayo ha supuesto un **reto para las administraciones locales.**

Nuevas obligaciones:

- El principio de responsabilidad proactiva.
- El enfoque de riesgo en el cumplimiento de las obligaciones que establece.

El principio de responsabilidad proactiva

Hemos tenido que aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.

Hemos analizado **qué datos** se tratan, con qué **finalidades** lo hacemos y qué **tipo de operaciones** de tratamiento se llevan a cabo, para lo que el **Registro de Actividades de Tratamientos** es un instrumento básico y fundamental.

Diputación ha creado el Registro de Actividades de Tratamientos en el que se recopilan y describen los **96 tratamientos de datos personales** que realiza la Corporación. Y es Accesible desde el **Portal de Transparencia de Diputación**.

http://www.malaga.es/gobierno/7278/registro-tratamientos

A partir de la información recopilada en el Registro de Actividades de Tratamiento.

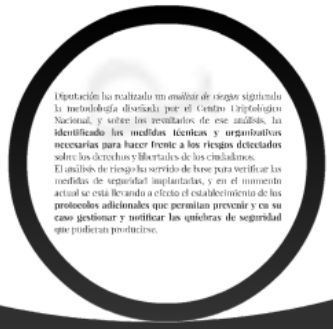
Se ha diseñado la forma en que aplicarán las **medidas que el RGPD** prevé y son adecuadas para su cumplimiento. Que podamos demostrarlo ante los interesados y ante las autoridades de supervisión.

La elaboración del Registro de Actividades de Tratamiento **ha exigido** analizar las bases jurídicas que legitiman la posibilidad de que ese tratamiento se realice.

El enfoque de riesgo

Implica que las medidas dirigidas a garantizar su cumplimiento deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los **derechos y libertades de las personas**.

Algunas de las medidas que el RGPD establece se aplicarán sólo cuando exista un **alto riesgo** para los derechos y libertades, mientras que otras deberán modularse en función del nivel y tipo de riesgo que los tratamientos presenten.



Diputación ha realizado un *análisis de riesgos* siguiendo la metodología diseñada por el Centro Criptológico Nacional, y sobre los resultados de ese análisis, ha **identificado las medidas técnicas y organizativas necesarias para hacer frente a los riesgos detectados** sobre los derechos y libertades de los ciudadanos.

El análisis de riesgo ha servido de base para verificar las medidas de seguridad implantadas, y en el momento actual se está llevando a efecto el establecimiento de los **protocolos adicionales que permitan prevenir y en su caso gestionar y notificar las quiebras de seguridad** que pudieran producirse.

Plan de mejora en la Seguridad y adaptación al RGPD

Para **implantar** en la institución los requerimientos de la nueva normativa de protección de datos y del Esquema Nacional de Seguridad

Se han realizado **entrevistas con las distintas Áreas** y Servicios de Diputación, para adaptar las previsiones generales a las peculiaridades de cada Servicio, de manera que en un periodo de **dos años** se encuentre totalmente implantado.

Las **medidas de seguridad:**

- Adaptado a las características de los tratamientos, al tipo de datos tratados y a la tecnología disponible en cada momento.
- Garantizan la integridad de la información tratada por Diputación.
- Permiten su recuperación en caso de incidentes.
- Evitan accesos no autorizados.

Las **medidas de seguridad:**

- Adaptado a las características de los tratamientos, al tipo de datos tratados y a la tecnología disponible en cada momento.
- Garantizan la integridad de la información tratada por Diputación.
- Permiten su recuperación en caso de incidentes.
- Evitan accesos no autorizados.

Algunas medidas concretas cumplimiento ENS-RGPD

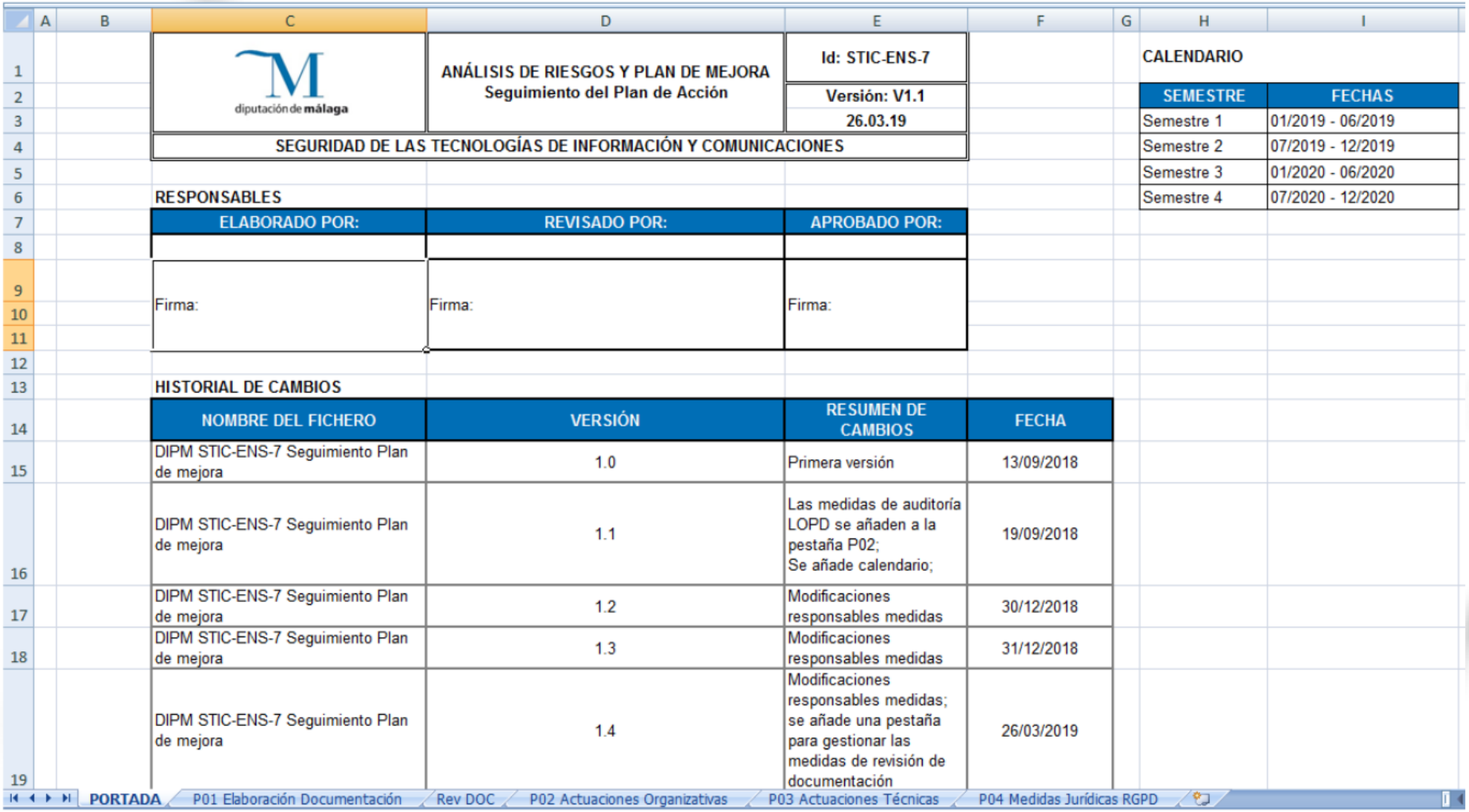
*Se han adecuado los formularios que recaban datos personales de los ciudadanos para adaptar el derecho de información a los requisitos del RGPD.

*Se han implantado los **procedimientos** para atender el ejercicio de los derechos de acceso, rectificación, supresión, oposición, limitación y portabilidad de los datos personales; y los procedimientos para acreditar el consentimiento y garantizar la posibilidad de revocarlo.

http://www.malaga.es/gobierno/7285/ejercicio-derechos

*Se ha **diseñado un protocolo** que asegure que los encargados de tratamiento, los adjudicatarios de contratos administrativos que en su ejecución realicen tratamientos de datos por cuenta de la Diputación, ofrezcan las garantías exigidas por el RGPD.

*Creado y ocupado el puesto del **delegado de protección de datos** (DPD) "Supervisión del cumplimiento interno"



diputación de málaga	ANÁLISIS DE RIESGOS Y PLAN DE MEJORA Seguimiento del Plan de Acción
	Id: STIC-ENS-7
	Versión: V1.1
	26.03.19

SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

RESPONSABLES

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Firma:	Firma:	Firma:

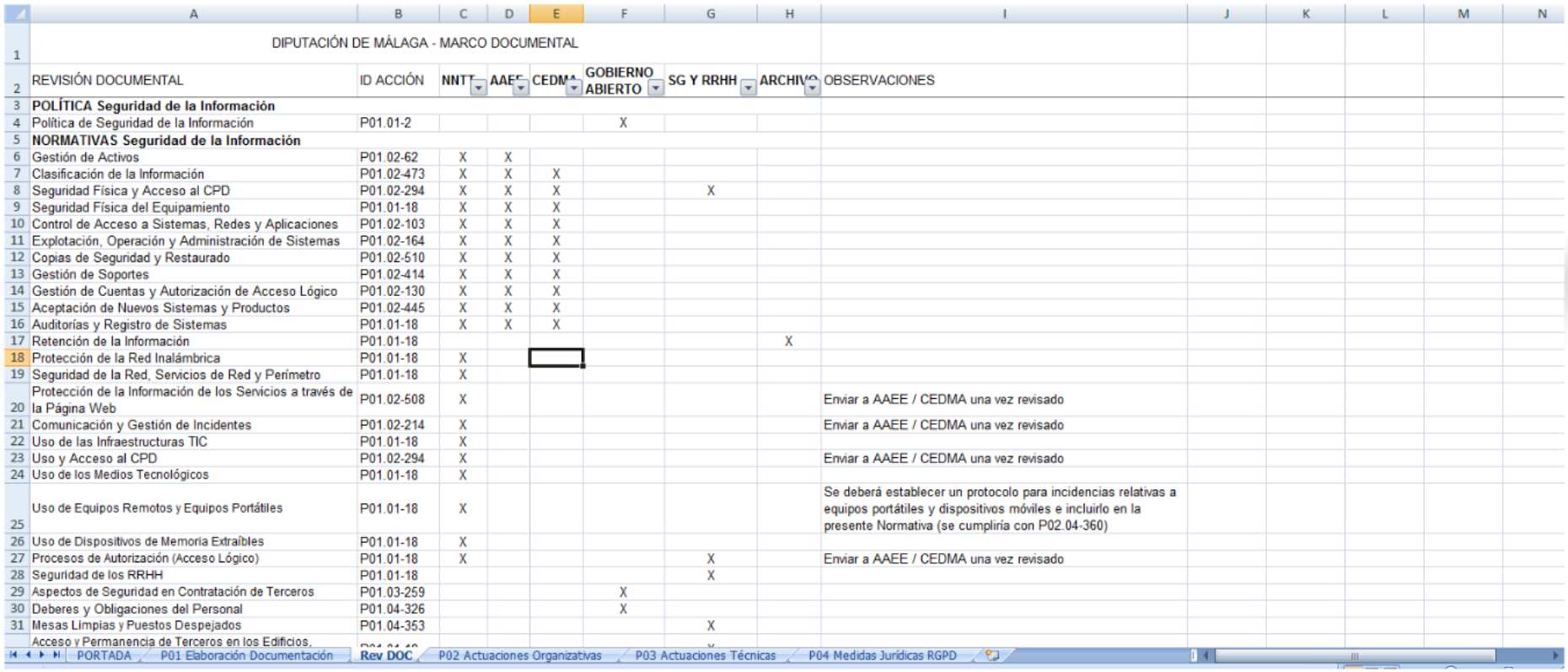
HISTORIAL DE CAMBIOS

NOMBRE DEL FICHERO	VERSIÓN	RESUMEN DE CAMBIOS	FECHA
DIPM STIC-ENS-7 Seguimiento Plan de mejora	1.0	Primera versión	13/09/2018
DIPM STIC-ENS-7 Seguimiento Plan de mejora	1.1	Las medidas de auditoría LOPD se añaden a la pestaña P02; Se añade calendario;	19/09/2018
DIPM STIC-ENS-7 Seguimiento Plan de mejora	1.2	Modificaciones responsables medidas	30/12/2018
DIPM STIC-ENS-7 Seguimiento Plan de mejora	1.3	Modificaciones responsables medidas	31/12/2018
DIPM STIC-ENS-7 Seguimiento Plan de mejora	1.4	Modificaciones responsables medidas; se añade una pestaña para gestionar las medidas de revisión de documentación	26/03/2019

CALENDARIO

SEMESTRE	FECHAS
Semestre 1	01/2019 - 06/2019
Semestre 2	07/2019 - 12/2019
Semestre 3	01/2020 - 06/2020
Semestre 4	07/2020 - 12/2020

PORTADA | P01 Elaboración Documentación | Rev DOC | P02 Actuaciones Organizativas | P03 Actuaciones Técnicas | P04 Medidas Jurídicas RGPD

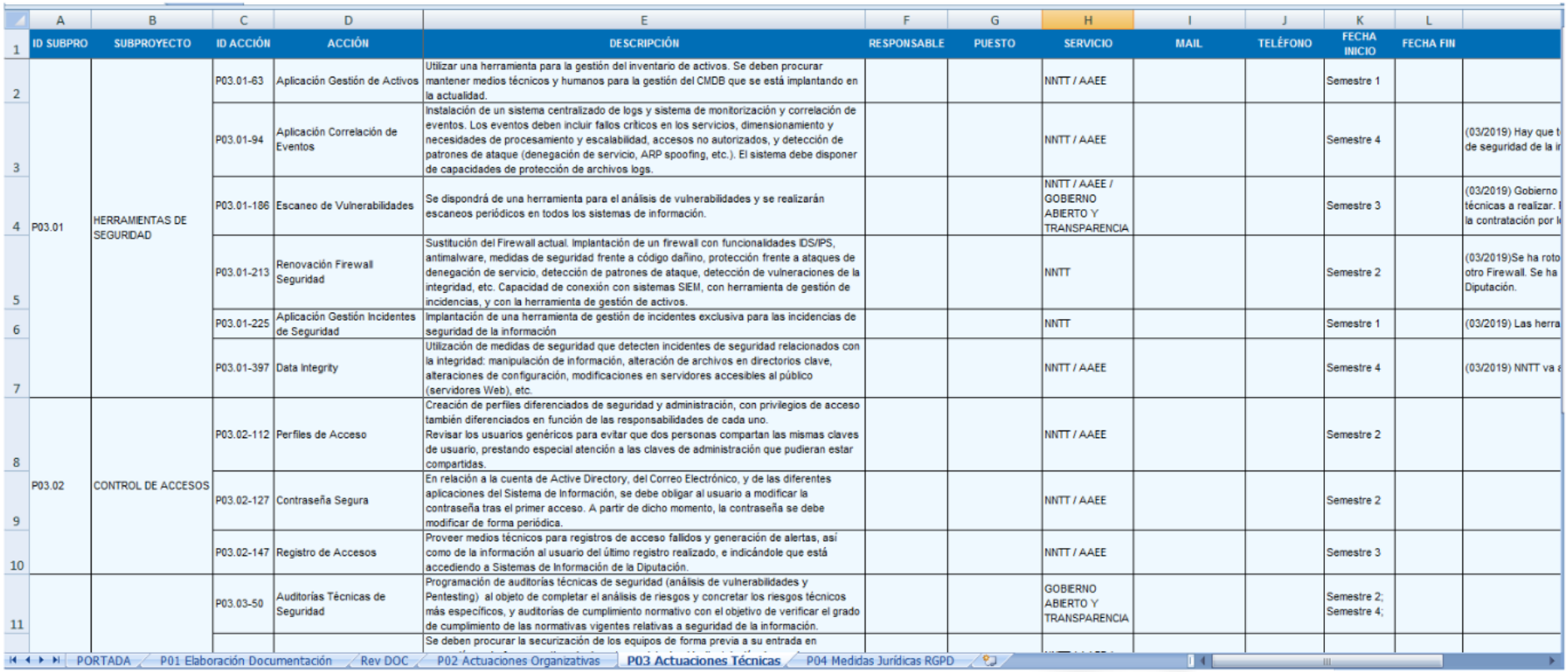


	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	DIPUTACIÓN DE MÁLAGA - MARCO DOCUMENTAL													
2	REVISIÓN DOCUMENTAL	ID ACCIÓN	NNTT	AAEE	CEDMA	GOBIERNO ABIERTO	SG Y RRHH	ARCHIVO	OBSERVACIONES					
3	**POLÍTICA Seguridad de la Información**													
4	Política de Seguridad de la Información	P01.01-2				X								
5	**NORMATIVAS Seguridad de la Información**													
6	Gestión de Activos	P01.02-62	X	X										
7	Clasificación de la Información	P01.02-473	X	X	X									
8	Seguridad Física y Acceso al CPD	P01.02-294	X	X	X		X							
9	Seguridad Física del Equipamiento	P01.01-18	X	X	X									
10	Control de Acceso a Sistemas, Redes y Aplicaciones	P01.02-103	X	X	X									
11	Explotación, Operación y Administración de Sistemas	P01.02-164	X	X	X									
12	Copias de Seguridad y Restaurado	P01.02-510	X	X	X									
13	Gestión de Soportes	P01.02-414	X	X	X									
14	Gestión de Cuentas y Autorización de Acceso Lógico	P01.02-130	X	X	X									
15	Aceptación de Nuevos Sistemas y Productos	P01.02-445	X	X	X									
16	Auditorías y Registro de Sistemas	P01.01-18	X	X	X									
17	Retención de la Información	P01.01-18						X						
18	Protección de la Red Inalámbrica	P01.01-18	X											
19	Seguridad de la Red, Servicios de Red y Perímetro	P01.01-18	X											
20	Protección de la Información de los Servicios a través de la Página Web	P01.02-508	X						Enviar a AAEE / CEDMA una vez revisado					
21	Comunicación y Gestión de Incidentes	P01.02-214	X						Enviar a AAEE / CEDMA una vez revisado					
22	Uso de las Infraestructuras TIC	P01.01-18	X											
23	Uso y Acceso al CPD	P01.02-294	X						Enviar a AAEE / CEDMA una vez revisado					
24	Uso de los Medios Tecnológicos	P01.01-18	X											
25	Uso de Equipos Remotos y Equipos Portátiles	P01.01-18	X						Se deberá establecer un protocolo para incidencias relativas a equipos portátiles y dispositivos móviles e incluirlo en la presente Normativa (se cumpliría con P02.04-360)					
26	Uso de Dispositivos de Memoria Extraíbles	P01.01-18	X											
27	Procesos de Autorización (Acceso Lógico)	P01.01-18	X				X		Enviar a AAEE / CEDMA una vez revisado					
28	Seguridad de los RRHH	P01.01-18					X							
29	Aspectos de Seguridad en Contratación de Terceros	P01.03-259				X								
30	Deberes y Obligaciones del Personal	P01.04-326				X								
31	Mesas Limpias y Puestos Despejados	P01.04-353					X							
	Acceso y Permanencia de Terceros en los Edificios,													

PORTADA | P01 Elaboración Documentación | Rev DOC | P02 Actuaciones Organizativas | P03 Actuaciones Técnicas | P04 Medidas Jurídicas RGPD

	A	B	C	D	E	F	G	H	I	J	K	L
1	ID SUBPRO	SUBPROYECTO	ID ACCIÓN	ACCIÓN	DESCRIPCIÓN	RESPONSABLE	PUESTO	SERVICIO	MAIL	TELÉFONO	FECHA INICIO	FECHA FI
14				Plan de Acción LOPD 2017. Almacenamiento de información en papel (datos de categoría normal)	Los expedientes en papel de datos de categoría normal deben almacenarse en armarios o archivadores con mecanismos que obstaculicen su apertura. Las llaves de armarios, archivadores, despachos, salas de archivo, etc., deben guardarse en lugar seguro.			GOBIERNO ABIERTO Y TRANSPARENCIA. Servicios implicados: Servicios Sociales Comunitarios; Empleo; Información Territorial; Tercer Sector y Ciudadanía;			Semestre 1	
15				Plan de Acción LOPD 2017. Cambios de emplazamiento	Disponer de un procedimiento en relación a los cambios de ocupación de las diferentes zonas de trabajo de la Diputación, que contemple la revisión de los espacios para evitar que documentos con daos de carácter personal queden expuestos, así como el formateo de los ordenadores.			GOBIERNO ABIERTO Y TRANSPARENCIA. Servicios implicados: genérico;			Semestre 1	
16			P02.02-470	Plan de Acción LOPD 2017. Almacenamiento de información en papel (datos de categoría especial)	Los documentos que contengan datos personales de categoría especial deben ubicarse en zonas protegidas mediante llave o algún sistema equivalente. En el interior de dichas zonas, la documentación debe almacenarse en armarios o archivadores con mecanismos que obstaculicen su apertura			GOBIERNO ABIERTO Y TRANSPARENCIA. Servicios implicados: Tercer Sector y Atención a la Ciudadanía; Servicios Sociales Comunitarios; Sindicato ASED; sindicato ATD; sindicato UGT; Igualdad de Género; Partidos Políticos: Ciudadanos; Asesoría Jurídica; Prevención de Riesgos; Fomento Empleo Agrario;			Semestre 1	
17				Plan de Acción LOPD 2017. Destrucción de papel	Definir el procedimiento de destrucción de papel y destrucción de soportes, y adecuar los espacios y áreas de la Diputación con los medios necesarios.			GOBIERNO ABIERTO Y TRANSPARENCIA			Semestre 1	
18	P02.03	ROLES Y RESPONSABILIDADES	P02.03.4	Roles Comité de Seguridad	Se debe procurar la operatividad funcional y designación de los roles relacionados con la seguridad de la información			GOBIERNO ABIERTO Y TRANSPARENCIA			Semestre 1	
19			P02.03.321	Caracterización Puestos de Trabajo	En relación a los puestos de trabajo en la Diputación, se deben definir los requisitos de seguridad de cada puesto de trabajo, y las capacidades y formación en materia de seguridad de la información de las persona que ocupe el puesto. Para nuevas contrataciones, se deberán tener en cuenta estas especificaciones de requisitos. Relacionado con Normativa de Seguridad de RRHH. Se debe revisar dicha Normativa por parte de RRHH.			GOBIERNO ABIERTO Y TRANSPARENCIA; RRHH			Semestre 1	
20			P02.03.327	Firma Deberes y Obligaciones	El personal de la Diputación, interno y externo, debe firmar el documento de deberes y obligaciones respecto al buen uso de los elementos que componen los sistemas de información: carpetas del servidor, navegación por Internet, correo electrónico, aplicaciones específicas, etc.			GOBIERNO ABIERTO Y TRANSPARENCIA; implica a RRHH			Actividad continua	
21			P02.04-341	Plan de Concienciación	Elaborar e implantar un plan de concienciación dirigido al personal de Diputación. El plan podrá estar basado en diferentes medios (sesiones presenciales, banners en la intranet, correos periódicos, mensajes en carteles, trípticos o alfombrillas de ratón, blog de seguridad de la información, envío de circulares periódicas, simulación de entradas de correo phishing, etc.) en función de los recursos disponibles.			GOBIERNO ABIERTO Y TRANSPARENCIA			Actividad continua	
					Contemplar las necesidades de formación relativas a la seguridad de la información en el Plan de Formación Anual de la Diputación. El plan deberá incluir, al menos, acciones							

PORTADA | P01 Elaboración Documentación | Rev DOC | P02 Actuaciones Organizativas | P03 Actuaciones Técnicas | P04 Medidas Jurídicas RGPD



	A	B	C	D	E	F	G	H	I	J	K	L	
1	ID SUBPRO	SUBPROYECTO	ID ACCIÓN	ACCIÓN	DESCRIPCIÓN	RESPONSABLE	PUESTO	SERVICIO	MAIL	TELÉFONO	FECHA INICIO	FECHA FIN	
2	P03.01	HERRAMIENTAS DE SEGURIDAD	P03.01-63	Aplicación Gestión de Activos	Utilizar una herramienta para la gestión del inventario de activos. Se deben procurar mantener medios técnicos y humanos para la gestión del CMDB que se está implantando en la actualidad.			NNTT / AAEE			Semestre 1		
3			P03.01-94	Aplicación Correlación de Eventos	Instalación de un sistema centralizado de logs y sistema de monitorización y correlación de eventos. Los eventos deben incluir fallos críticos en los servicios, dimensionamiento y necesidades de procesamiento y escalabilidad, accesos no autorizados, y detección de patrones de ataque (denegación de servicio, ARP spoofing, etc.). El sistema debe disponer de capacidades de protección de archivos logs.			NNTT / AAEE			Semestre 4		(03/2019) Hay que t de seguridad de la ir
4			P03.01-186	Escaneo de Vulnerabilidades	Se dispondrá de una herramienta para el análisis de vulnerabilidades y se realizarán escaneos periódicos en todos los sistemas de información.			NNTT / AAEE / GOBIERNO ABIERTO Y TRANSPARENCIA			Semestre 3		(03/2019) Gobierno técnicas a realizar. I la contratación por l
5			P03.01-213	Renovación Firewall Seguridad	Sustitución del Firewall actual. Implantación de un firewall con funcionalidades IDS/IPS, antimalware, medidas de seguridad frente a código dañino, protección frente a ataques de denegación de servicio, detección de patrones de ataque, detección de vulneraciones de la integridad, etc. Capacidad de conexión con sistemas SIEM, con herramienta de gestión de incidencias, y con la herramienta de gestión de activos.			NNTT			Semestre 2		(03/2019)Se ha roto otro Firewall. Se ha Diputación.
6			P03.01-225	Aplicación Gestión Incidentes de Seguridad	Implantación de una herramienta de gestión de incidentes exclusiva para las incidencias de seguridad de la información			NNTT			Semestre 1		(03/2019) Las herra
7			P03.01-397	Data Integrity	Utilización de medidas de seguridad que detecten incidentes de seguridad relacionados con la integridad: manipulación de información, alteración de archivos en directorios clave, alteraciones de configuración, modificaciones en servidores accesibles al público (servidores Web), etc.			NNTT / AAEE			Semestre 4		(03/2019) NNTT va a
8	P03.02	CONTROL DE ACCESOS	P03.02-112	Perfiles de Acceso	Creación de perfiles diferenciados de seguridad y administración, con privilegios de acceso también diferenciados en función de las responsabilidades de cada uno. Revisar los usuarios genéricos para evitar que dos personas compartan las mismas claves de usuario, prestando especial atención a las claves de administración que pudieran estar compartidas.			NNTT / AAEE			Semestre 2		
9			P03.02-127	Contraseña Segura	En relación a la cuenta de Active Directory, del Correo Electrónico, y de las diferentes aplicaciones del Sistema de Información, se debe obligar al usuario a modificar la contraseña tras el primer acceso. A partir de dicho momento, la contraseña se debe modificar de forma periódica.			NNTT / AAEE			Semestre 2		
10			P03.02-147	Registro de Accesos	Proveer medios técnicos para registros de acceso fallidos y generación de alertas, así como de la información al usuario del último registro realizado, e indicándole que está accediendo a Sistemas de Información de la Diputación.			NNTT / AAEE			Semestre 3		
11			P03.03-50	Auditorías Técnicas de Seguridad	Programación de auditorías técnicas de seguridad (análisis de vulnerabilidades y Pentesting) al objeto de completar el análisis de riesgos y concretar los riesgos técnicos más específicos, y auditorías de cumplimiento normativo con el objetivo de verificar el grado de cumplimiento de las normativas vigentes relativas a seguridad de la información.			GOBIERNO ABIERTO Y TRANSPARENCIA			Semestre 2; Semestre 4;		
					Se deben procurar la securización de los equipos de forma previa a su entrada en								

PORTADA | P01 Elaboración Documentación | Rev DOC | P02 Actuaciones Organizativas | P03 Actuaciones Técnicas | P04 Medidas Jurídicas RGPD

	A	B	C	D	E	F	G	H	I	J	K	L
1	ID SUBPRO	SUBPROYECTO	ID ACCIÓN	ACCIÓN	DESCRIPCIÓN	RESPONSABLE	PUESTO	SERVICIO	MAIL	TELÉFONO	FECHA INICIO	FECHA FIN
2	P04.01	PRINCIPIOS RGPD	P04.01-559	Clausulado Deber de Información	Configurar y poner en marcha un clausulado que contemple y permita el cumplimiento de cada uno de los principios relativos al tratamiento de datos personales del interesado.			GOBIERNO ABIERTO Y TRANSPARENCIA			Semestre 1	
3			P04.01-560	Registro Actividades de Tratamiento	Para cada tratamiento identificado se deberá indicar la licitud del tratamiento: consentimiento del interesado; es necesario para la prestación de un contrato; es necesario para el cumplimiento de una obligación legal; es necesario para proteger intereses vitales del interesado u otra persona física; es necesario para el ejercicio de las competencias de las AAPP; es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado.			GOBIERNO ABIERTO Y TRANSPARENCIA			Semestre 1	
4			P04.01-561	Acreditación del Consentimiento	Configurar y establecer las medidas necesarias que permitan acreditar el consentimiento del interesado para el tratamiento de sus datos personales, cuando dicho consentimiento tenga lugar, Redactar una cláusula que informe al interesado de su derecho a la retirada del consentimiento prestado.			GOBIERNO ABIERTO Y TRANSPARENCIA			Semestre 1	
5			P04.01-563	Datos Personales de Categoría Especial	Para cada tratamiento identificado en el que haya datos de categorías espaciales (origen étnico o racial, opiniones políticas, convicciones religiosas, afiliación sindical, datos genéticos, datos biométricos, datos de salud, datos de vida sexual), se deberá verificar que bien existe consentimiento explícito, o bien concurre alguna de las circunstancias estipuladas en los apartados 2 y 3 del RGPD.			GOBIERNO ABIERTO Y TRANSPARENCIA			Semestre 1	
6	P04.02	DERECHOS DEL INTERESADO	P04.02-568	Ejercicio Derechos Interesado	Establecer un procedimiento interno que facilite el ejercicio de los derechos por parte del interesado. Poner a disposición del interesado los medios necesarios para permitirle ejercer sus derechos relativos al tratamiento de sus datos personales.			GOBIERNO ABIERTO Y TRANSPARENCIA			Semestre 1	
7			P04.03-584	Documento de Seguridad RGPD	Elaborar un Documento de Seguridad que detalle las medidas técnicas y organizativas que deben ser llevadas a cabo e implantadas en la organización para que garanticen y demuestren que el tratamiento de datos personales es acorde a la normativa vigente en materia de protección de datos personales. Revisar y aprobar el documento.			GOBIERNO ABIERTO Y TRANSPARENCIA			Semestre 1	
					En el caso de que se vayan a realizar nuevos tratamientos de datos, la Diputación deberá tener en consideración lo siguiente:			GOBIERNO				

PORTADA | P01 Elaboración Documentación | Rev DOC | P02 Actuaciones Organizativas | P03 Actuaciones Técnicas | P04 Medidas Jurídicas RGPD

Entidades Locales de menos de 20.000 habitantes

Cuentan con la asistencia de la Diputación para facilitarles el cumplimiento del RGPD según dispone el artículo 36 de la Ley de Bases del Régimen Local.

Personal de nuevo ingreso de la Diputación que asumirán las funciones de delegados de protección de datos, así como la adaptación al resto de exigencias del Reglamento y del Esquema Nacional de Seguridad.

- Alameda
- Almáchar
- Almargen
- Alora
- Alozaina
- Benahavís
- Benalauría
- Bobadilla Estación
- Borge, El
- Carratraca
- Casarabonela
- Colmenar
- Comares
- Cortes de la Frontera
- Cuevas Bajas
- Cútar
- Frigiliana
- Gaucín
- Humilladero
- Igualeja
- Istán
- Iznate
- Jubrique
- Manilva
- Monda
- Parauta
- Salares
- Sierra de Yeguas
- Tolox
- Totalán
- Valle de Abdalajís
- Villanueva de Algaidas
- Villanueva del Rosario
- Villanueva del Trabuco
- Yunquera

Alameda
Almáchar
Almargen
Álora
Alozaina
Benahavís
Benalauría
Bobadilla Estación
Borge, El
Carratraca
Casarabonela
Colmenar
Comares
Cortes de la Frontera
Cuevas Bajas
Cútar
Frigiliana
Gaucín
Humilladero
Igualeja
Istán
Iznate
Jubrique
Manilva
Monda
Parauta
Salares
Sierra de Yeguas
Tolox
Totalán
Valle de Abdalajís
Villanueva de Algaidas
Villanueva del Rosario
Villanueva del Trabuco
Yunquera

Gracias

protecciondedatos@malaga.es

JORNADA DE FORMACIÓN: DELEGADO DE PROTECCIÓN DE DATOS

Administración Local