



**DIPUTACIÓN
DE BADAJOZ**

Apoyo Cumplimiento Normativo en Seguridad

XVII Encuentro Informática Municipal.

Jerez de los Caballeros

4 de Abril de 2019

sopra  steria

Índice

1. SOPRA STERIA.
2. ¿COMO LO HAREMOS?
3. ¿COMO OS PODEMOS AYUDAR?
4. PRÓXIMOS PASOS
5. PREGUNTAS Y CUESTIONES





Líder europeo en la transformación digital



3.800 M€

Cifra de negocio 2017



+42.000

Profesionales

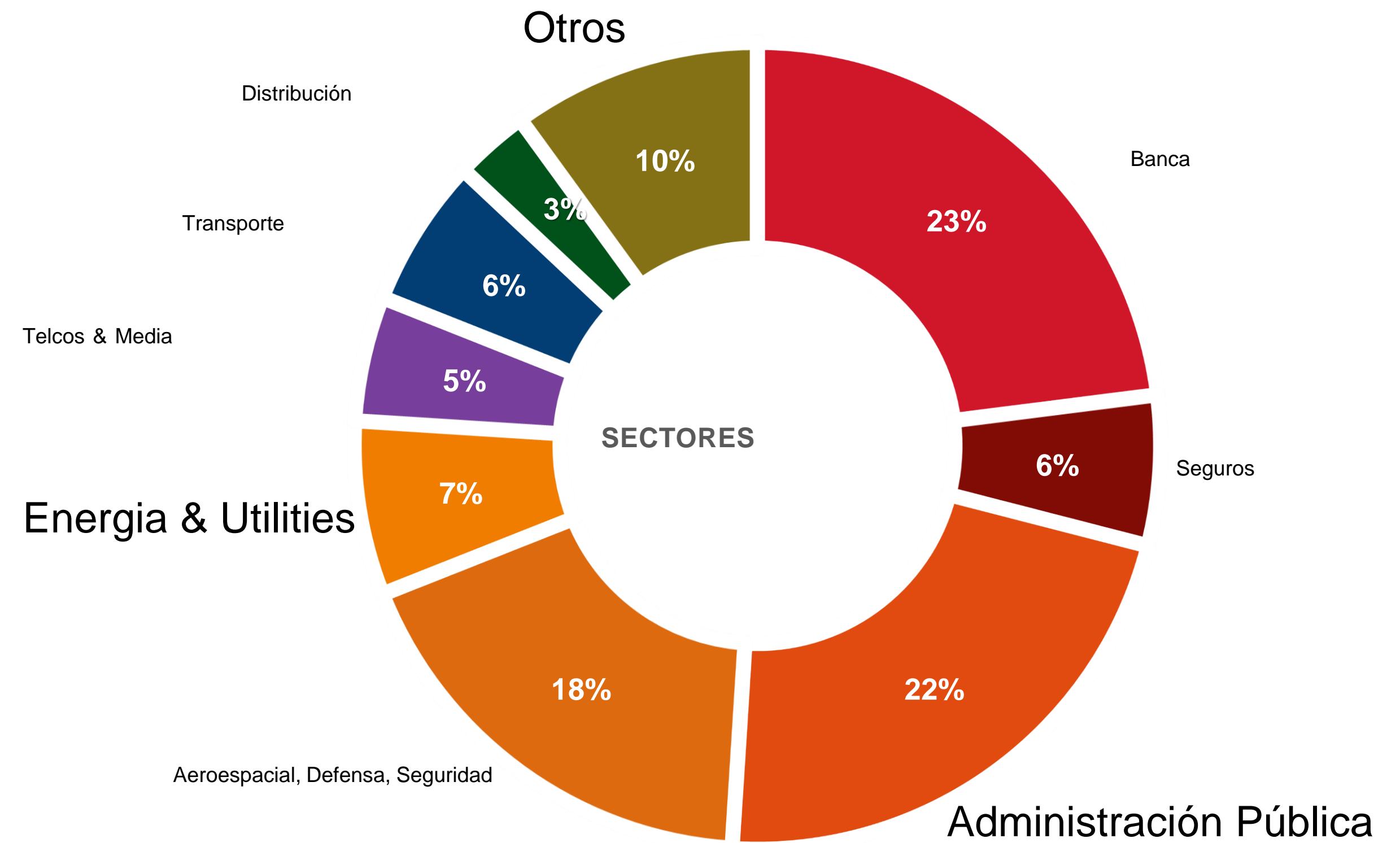
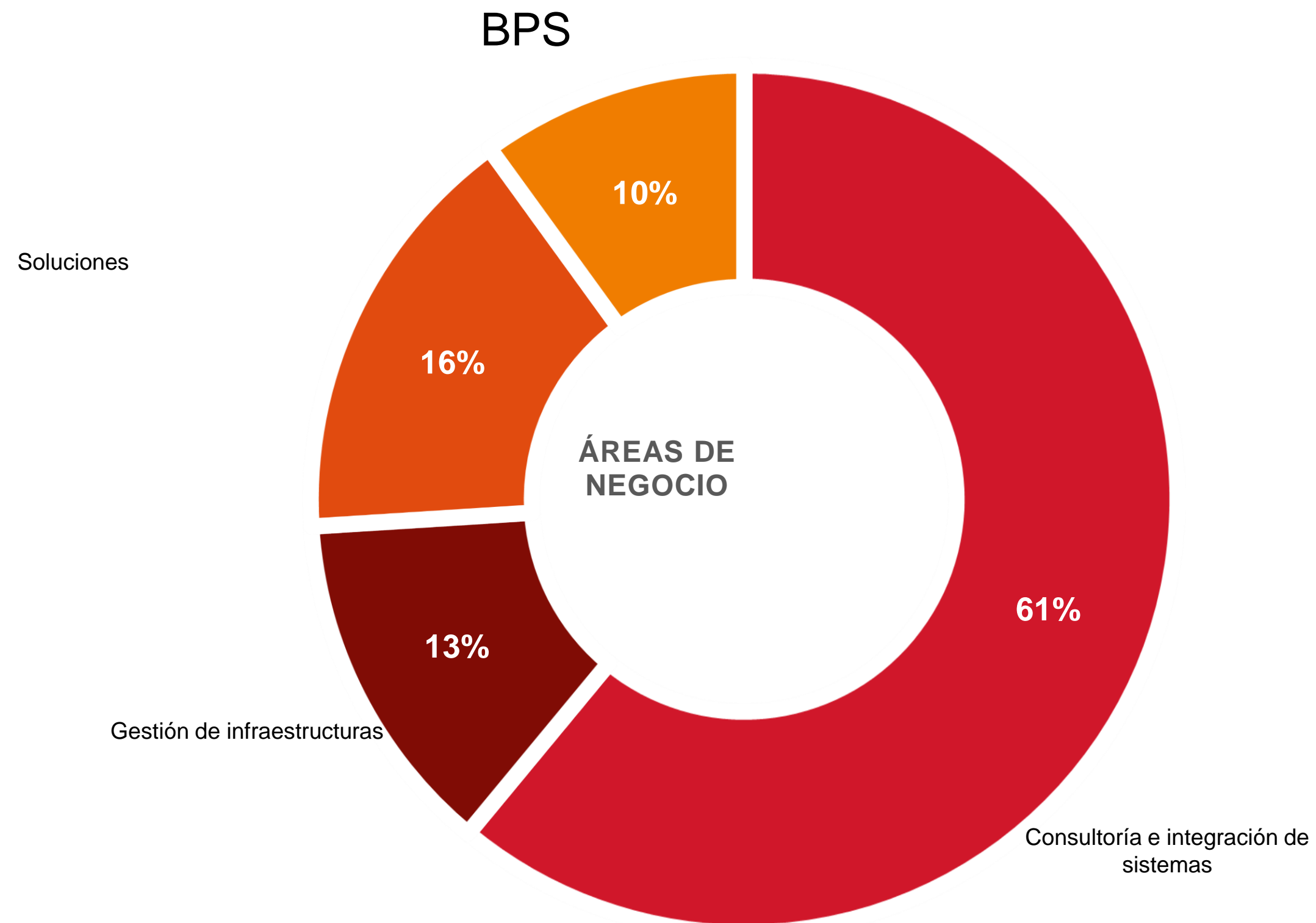


+20 países

Presencia internacional



Áreas de negocio y sectores de actividad



Una propuesta de gran valor añadido

- Un grupo líder con 50 años de experiencia
- Oferta End to End
- Excelencia en el delivery
- Equipos certificados en metodologías ágiles
- Enfoque sectorial del negocio



Sopra Steria en España.

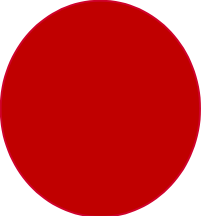
>80% Empresas IBEX 35



+ 4000 profesionales



10 Oficinas



2 Digilabs

Banca



Seguros



Servicios, Transporte & Utilidades



Industria



Telecom & Medias



Sector Público

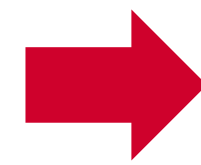


Distribución



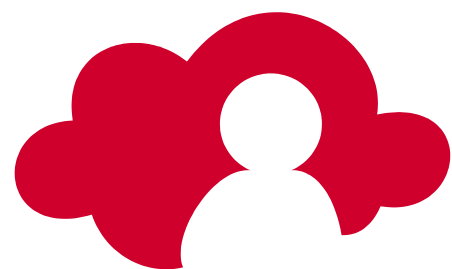
Transformar los cambios en oportunidades para nuestros clientes

Revolución digital

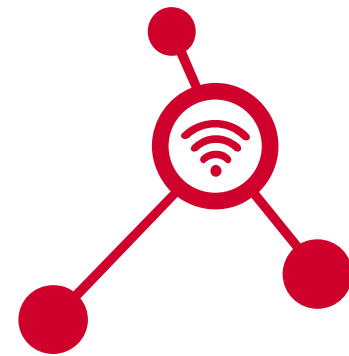


Retos

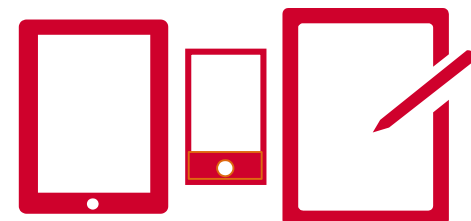
Social



IoT



Móvil



Big Data



Cloud



Ciberseguridad



- Acompañar a nuestros clientes en su transformación digital
- Crear y operar servicios innovadores para transformar estos cambios en ventajas relevantes
- Ganar en reactividad y flexibilidad para acompañar el crecimiento y la competitividad
- Controlar la calidad y los costes de los sistemas existentes

Ciber-Seguridad

CIBER-VIGILANCIA

- SIEM/SOC.
- Detección APT.
- NGIPS/HIPS.
- Observatorio/CERT.
- Análisis.
- Gestión de crisis.



ESTRATEGIA, RIESGOS & GOBIERNO

- Estrategia y planificación.
- Análisis de riesgos.
- Gestión de Sistemas Seguridad.
- Control Servicios Gestionados.
- Control Procesos.

AUDITORÍAS & CONFORMIDAD

- Conformidad normativa.
- Conformidad SI.
- Auditorías organizativas.
- Pruebas de intrusión.
- Gestión de vulnerabilidades.

IDENTIDAD DIGITAL

- Gestión de identidades y accesos.
- Firma electrónica.
- Gestión de accesos y privilegios.
- *SmartCard*/Biometría.

PROTECCIÓN DE DATOS

- Clasificación.
- Cifrado.
- DLP.



UNA RED MUNDIAL DE MÁS DE 600 EXPERTOS DEDICADOS A CIBER-SEGURIDAD







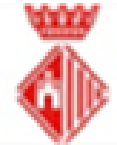



3 CENTROS DE CIBER-SEGURIDAD EN 24X7 (FRANCIA, UK Y SINGAPUR)



METODOLOGÍA DE GOBIERNO POR RIESGOS (IPPCOR) BASADO EN ISO 27001 Y CISM



Algunas referencias Cumplimiento Normativo

 Consejería de Hacienda y Administración Pública	<ul style="list-style-type: none">■ Adecuación al ENS, ISO27002 y RGPD. Análisis de Riesgos y Plan Director de Seguridad.
 Ajuntament de Barcelona	<ul style="list-style-type: none">■ Auditoría Bienal LOPD/Definición e implantación de proceso de evaluación continua de cumplimiento/Sesiones formativas/Definición de Hoja de ruta/Implantación acciones correctivas/Diseño e Implantación de DS
 CatSalut Servei Català de la Salut	<ul style="list-style-type: none">■ Soporte y asesoramiento en proceso de Auditoría externa LOPD/Diseño e Implantación de DS/Definición y redacción de procedimientos y políticas seguridad/ Asesoramiento continuado
 Generalitat de Catalunya ACCIÓ	<ul style="list-style-type: none">■ Auditoría Bienal LOPD■ Sesiones formativas/Definición de Hoja de ruta
 Ajuntament de Terrassa	<ul style="list-style-type: none">■ Auditoría Bienal LOPD■ Asesoramiento Continuado
 UNIVERSITAT POMPEU FABRA	<ul style="list-style-type: none">■ Definición de Hoja de ruta/Implantación acciones correctivas/Asesoramiento Continuado/Diseño e implantación Documento de Seguridad (DS)
 3 CATALUNYA RÀDIO Corporació Catalana de Mitjans Audiovisuals	<ul style="list-style-type: none">■ Auditoría Bienal LOPD■ Definición de Hoja de ruta
 CanalSur RADIO Y TELEVISIÓN	<ul style="list-style-type: none">■ Auditoría de Adecuación al RGPD■ Definición de Hoja de ruta



EL PROYECTO



Objetivos principales del Proyecto

Cultura Seguridad

Fomentar la cultura de la seguridad y privacidad de datos entre el personal

Apoyo Toma Decisiones

Asistir a la Dirección en la toma de decisiones de Seguridad mediante información confiable



ALCANCE



DIP-BADAJOZ, CONSORCIOS Y OOAA

160 Municipios <20.000 hab

16 EELL Menores

16 Mancomunidades

1 AÑO DE PLAZO DE EJECUCIÓN



¿COMO LO HAREMOS?



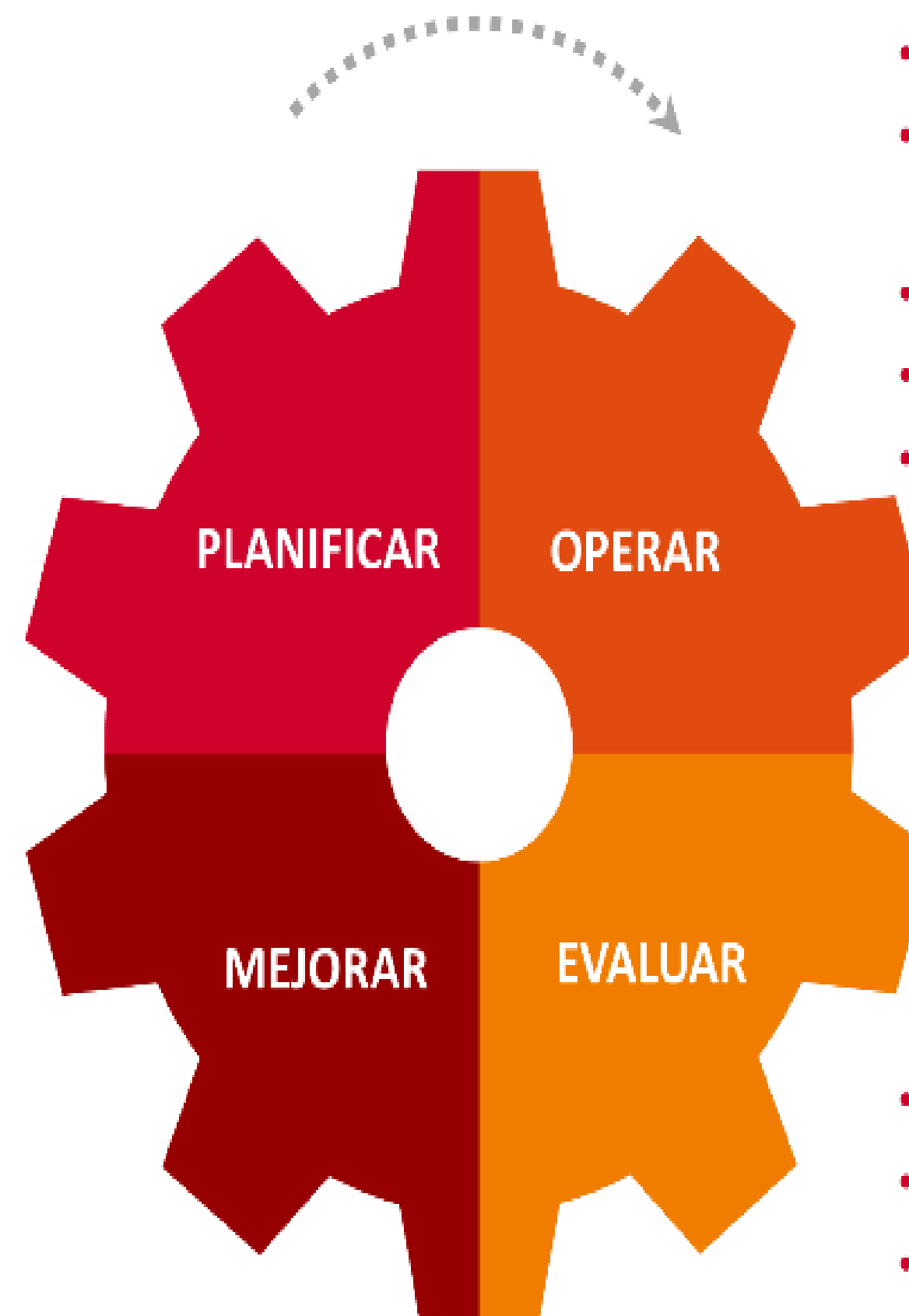
Metodología y Planificación

PLANIFICAR

- Definir alcance del SGSI
- Definir la Política de Seguridad
- Metodología de Evaluación de Riesgos
- Identificación de activos, amenazas y vulnerabilidades
- Análisis y evaluación de riesgos
- Selección de controles (aplicabilidad)

INICIO / ARRANQUE

- Compromiso de la Dirección
- Planificación y fechas
- Responsables



OPERAR

- Definir el plan de tratamiento de riesgos
- Implantar el plan de tratamiento de riesgos
- Implementar los controles
- Formación y concienciación
- Operar el SGSI

MEJORAR

- Implementar mejoras
- Acciones correctivas
- Acciones preventivas
- Comprobar eficacia de las acciones

EVALUAR

- Revisar el SGSI
- Medir eficacia de los controles
- Revisar riesgos residuales
- Realizar auditorías internas del SGSI
- Registrar acciones y eventos



Metodología y Planificación



Metodología y Planificación

Nombre de tarea	Duración	Timeline													
		tri 2, 2019			tri 3, 2019			tri 4, 2019			tri 1, 2020			tri 2, 2020	
		abr	may	jun	jul	ago	sep	oct	nov	dic	ene	feb	mar	abr	ma
Cumplimiento Normativo Dip Badajoz	265 días	[Timeline bar]													
Captura de la información	1 sem	[Task bar]													
Recopilación y organización información	2 sem.	[Task bar]													
S01 - Análisis Situación Actual	3 sem.	[Task bar]													
S02 - Análisis Riesgos	4 sem.	[Task bar]													
S03 - Evaluación Cumplimiento Normativo	4 sem.	[Task bar]													
S04 - Elaboración del Plan de Mejora	10 sem.	[Task bar]													
S05 - Concienciación y Formación	50 sem.	[Task bar]													
S06 - Resolución Consultas	40 sem.	[Task bar]													
S07 - Seguimiento Actividades del Plan de Mejora	40 sem.	[Task bar]													
S08 - Elaboración Cuadros Mando	40 sem.	[Task bar]													
S09 - Auditorias ENS y RGPD	4 sem.	[Task bar]													
S10 - Servicio DPD	49 sem.	[Task bar]													





¿COMO OS PODEMOS AYUDAR?



Funciones del DPO



Resolución Consultas

Informar y Asesorar a los Ayuntamientos en Materias de Protección de Datos



Supervisión Cumplimiento

Supervisar el cumplimiento de los planes de Adecuación a RGPD y ENS



Incidentes

Apoyar en la gestión de los Incidentes de Seguridad y Privacidad



Cooperación

Cooperación con la Autoridad de Control



Apoyo

Apoyar al DPD Diputación en las tareas de Asesoramiento, Difusión y Control



Evaluaciones Impacto

Apoyo en las tareas relativas a Evaluaciones de Impacto



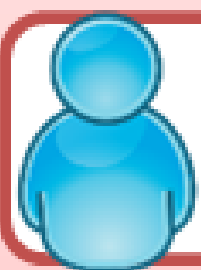
Divulgación

Divulgar y concienciar a los empleados de las diferentes AALL de la importancia de la privacidad y Seguridad de Datos

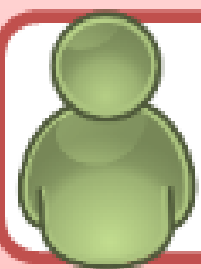


Equipo de Trabajo

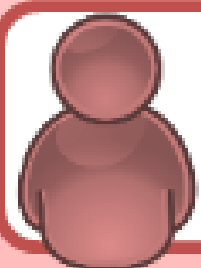
ORGANIZACIÓN EQUIPO DE TRABAJO



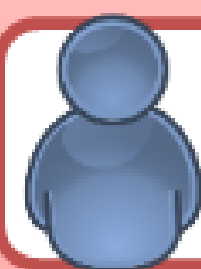
JEFE DE PROYECTO



CONSULTOR DE SEGURIDAD



DELEGADO DE PROTECCIÓN DE DATOS



AUDITOR

OTROS CONSULTORES APOYO



- Asesor Centros de CyberSeguridad
- Asesoramiento Legal
- Asesor en Procesos de Industrialización
- Especialista en Marketing. Gestión del Cambio
- Consultor Design Thinking
- Asesor Centros de Gestión de Infraestructuras

Catálogo de Formación

FO-01-CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN

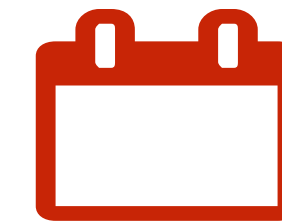
Dirigido a:	Todo el personal de la Diputación y Ayuntamientos interesado	Duración:	3 horas
Nº jornadas:	1 jornada.	Número de participantes:	Hasta 100



+10
Sedes Formación

FO-02-REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

Objetivos:	<ul style="list-style-type: none"> o Conocer la importancia y de la información personal. 	Dirigido a:	Personal de Diputación responsables de Tratamientos de Datos personales	Duración:	5 horas
Nº jornadas:	1 jornada.	Número de participantes:	20 (máx)		



+80
Horas Formación

FO-03-ESQUEMA NACIONAL DE SEGURIDAD

Objetivos:	<ul style="list-style-type: none"> o Que el personal que trata datos de carácter personal conozca las novedades relativas a la protección de datos. 	Dirigido a:	Personal de Diputación responsables de Servicios de Administración Electrónica	Duración:	5 horas
Nº jornadas:	1 jornada.	Número de participantes:	20 (máx)		

FO-04-Curso Básico de RGPD y ENS

Objetivos:	<ul style="list-style-type: none"> o Que el personal responsable de Servicios de Administración Electrónica Y tratamiento de Datos Personales conozca los conceptos técnicos de RGPD y ENS. 	Dirigido a:	Personal responsable de Servicios de Administración Electrónica Y tratamiento de Datos Personales	Duración:	5 horas
Nº jornadas:	1 jornada.	Número de participantes:	20 (máx)		

FO-05-Usos de la herramienta de análisis de riesgos: PILAR

Objetivos:	<ul style="list-style-type: none"> o Formar y concienciar al personal afectado por ambas normativas, ya que especialmente en el ámbito de la Administración Electrónica, se derivan de ambas normativas obligaciones a seguir para cumplir con las mismas. 	Dirigido a:	Personal que usará la herramienta de análisis de riesgos PILAR	Duración:	5 horas
Nº jornadas:	1 jornada.	Número de participantes:	20 (máx)		

FO-06-DELEGADO DE PROTECCIÓN DE DATOS

Objetivos:	<ul style="list-style-type: none"> o Introducir al personal que usará la herramienta PILAR en la configuración, parametrización, botones, etc. o Revisar el archivo de configuración de la herramienta PILAR. o Introducir al personal que usará la herramienta PILAR en la configuración, parametrización, botones, etc. 	Dirigido a:	Actuales Delegados de Protección de Datos y posibles responsables de esta función. Deben haber asistido al curso FO-02-REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS O disponer de los conocimientos y experiencia adecuados.	Duración:	10 horas
Nº jornadas:	2 jornadas.	Número de participantes:	10 Max		
Objetivos:	<ul style="list-style-type: none"> o Formar y concienciar a los actuales y/o futuros DPD, además de en sus funciones típicas, en aspectos como la protección de datos personales, grabación de videos, uso de redes sociales y 				

A photograph of three people (two men and one woman) in a starting crouch on a wooden floor in a bright, modern room with large windows and track lighting. They are looking forward with determination, ready to start a race or a project.

Próximos pasos

- Mecanismo comunicación formal
Ayuntamientos. Consultas y Comunicación
incidentes Seguridad
- Plan de Entrevistas
- Repositorio de Documentación Seguridad
y Privacidad
- Plan de Formación





¿PREGUNTAS?

¿SUGERENCIAS?

¿OPINIONES?



Manuel Castro Ruiz

Gerente para Extremadura

Manuel.CastroRuiz@soprasteria.com

+34.600.963.839



sopra  steria

Gracias!