



**“Reflecting on a long established
enforcement experience,
by the Spanish Data Protection
Agency”**

Mercedes Ortuño
Head of International Department, AEPD

Joaquín Pérez
Data Inspector, AEPD
CISA, CISM (ISACA)



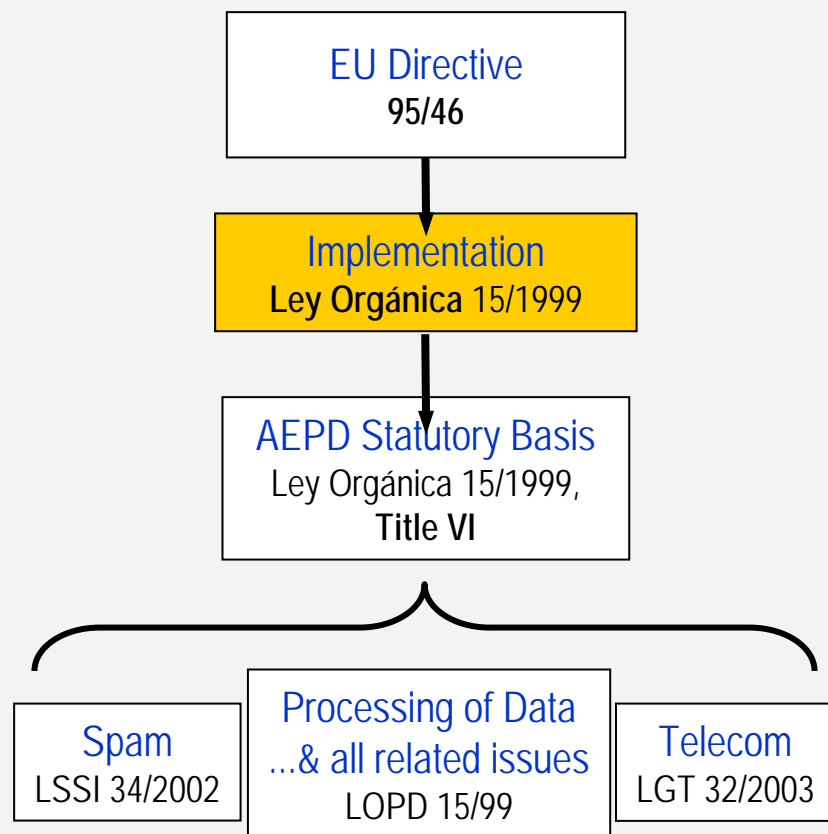
Outline

1. Jurisdiction and enforcement at AEPD
2. AEPD organization
3. Enforcement procedure
 - 3.1 Reactive: complaint handling
 - 3.2 Preventive: Ex-officious audits
4. Statistics
5. Some reflections



1. Jurisdiction of AEPD

- The AEPD has supervisory responsibility over all issues related to protection of personal data.
 - Private Sector
 - Public Sector (except local public sector Madrid, Cataluña and País Vasco)
- The AEPD “acts with full independence of the Public Administration in the exercise of its functions...” (LOPD art. 35.1)





• “Enforcement” is understood as “application” of the Data Protection Law. Under this law, the AEPD is responsible for both Preventive and Reactive activities.

– Preventive ($\pm 20\%$ of our enforcement activity)

- Guidance on compliance by industrial sectors
- Ad hoc consultation
- Raising awareness \rightarrow public and business community

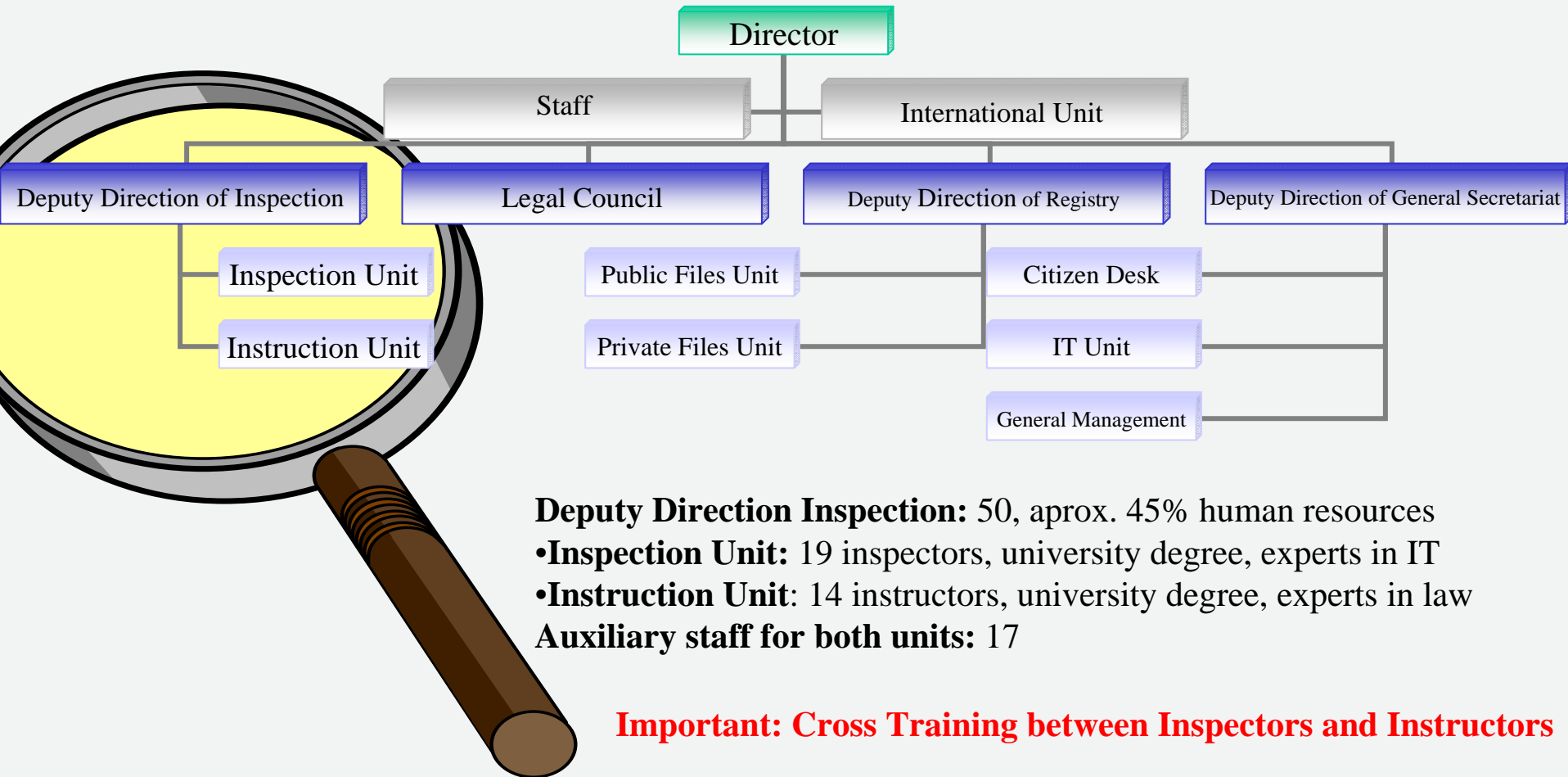
– Reactive ($\pm 80\%$ of our enforcement activity)

- Complaints handling

Investigation,
Inspection,
Resolution

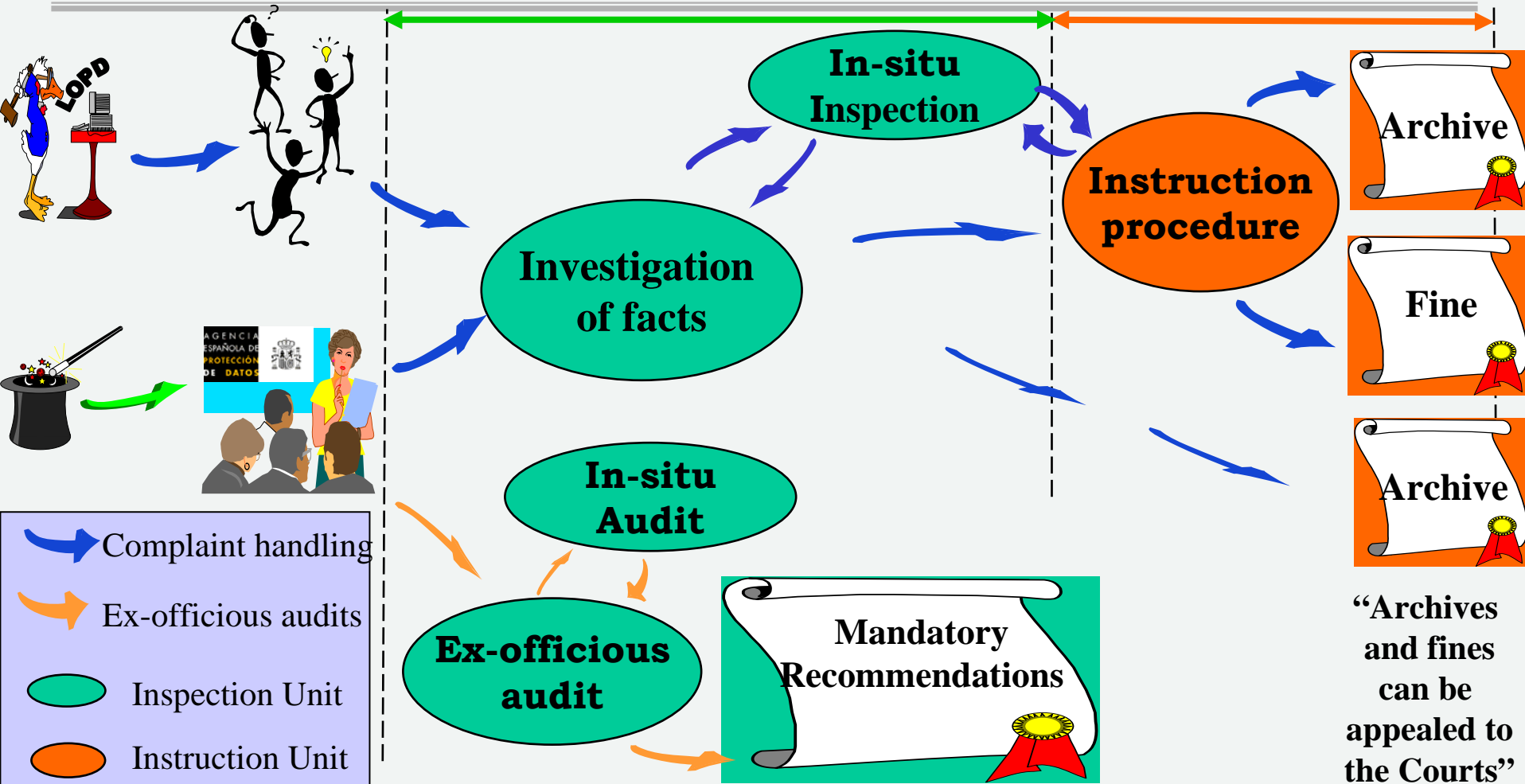


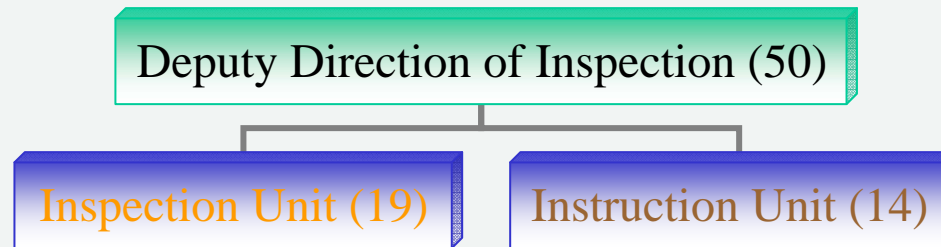
2. AEPD Organization





3. Enforcement Procedure





Skill:

- University degree
- IT Experts

Objectives:

- Previous investigations to state facts
- Not juridical evaluations

Skill:

- University degree
- Experts in Law

Objectives:

- Juridical evaluations



- The AEPD answers and resolves (mandatory) every complaint
- The AEPD exercises the investigative and enforcement authority of the state. (LOPD Art. 40)
- Because the Agency has the power to impose sanctions, it must guarantee due process to all parties.

Tools:

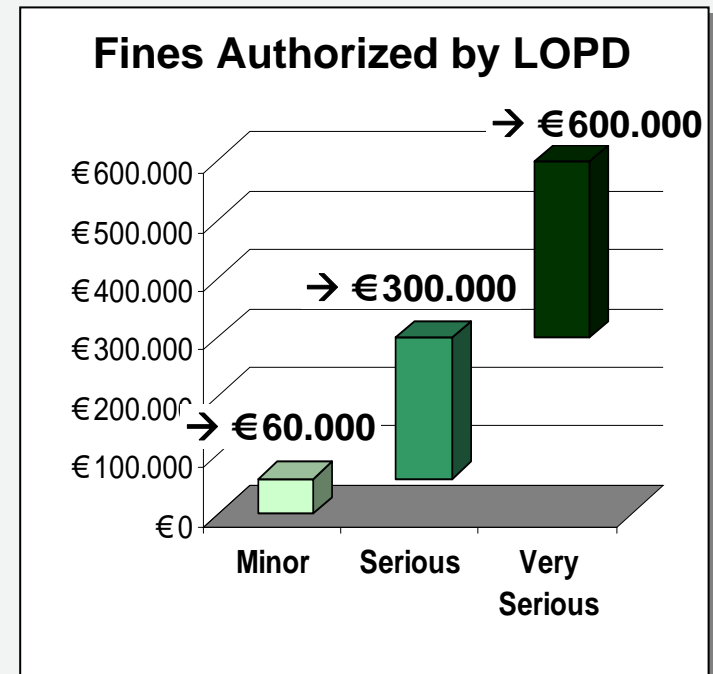
- Request for voluntary submission of information
- Inspection “in situ”** (Not collaborate in the investigation is a serious infringement)
- Fines are authorized by law
- Possibility of adopting preventive measures of blocking the processing
- Content of Inspection Minute (valid evidence at court and can be challenged “iuris tantum”)

Serious Violations include (not exhaustive):

- Failure to maintain accuracy
- Failure to provide security measures
- Failure to register or notify as required
- Creation of data files without consent
- Active refusal of rights
- Obstruction of investigation

Very Serious Violations include (not exhaustive):

- Unauthorized transfer of data
- Unauthorized processing of specialty protected data (medical, racial, sexual, ideological, etc.)
- Fraudulent collection of data
- Systematic violations





Key elements:

- **Role of Inspectors**: they check the facts, but do not make juridical evaluations (except in issues relates to security legislation)
- **Role of Instructors**: they make juridical evaluations
- **Definition of roles and responsibilities** in each case
- Possibility to make **inspections in situ** (computers check up, receiving)
- **Inspectors** are considered as “**public authority**”
- **Inspection working team** (a responsible and a partner)
- **Cross training** inspectors-instructors



3.2 Preventive Enforcement Ex-officious audit procedure

1. Choose a sector (objective and scope)
2. Choose an inspector responsible for the sectorial plan
3. Preliminary study of the sector
4. Explain to the sector the objectives of the plan to receive collaboration
5. Select a representative sample of the sector
6. Create an audit team
7. Choose an inspector responsible for each institution or company to be audited
8. Create and audit plan
9. Perform the audit plan in each organization
 - Request of preliminary information and a “high level” contact person
 - Planning interviews with all relevant people in the audited organization
 - **Facts finding (including direct computer check-up)**
 - Elaboration of the Inspection statement
 - Elaboration of the audited organization report
10. Elaboration of a draft conclusions and sending them to the sector for comments
11. Elaboration and Publication of mandatory recommendations

Risk based audit



3.2 Preventive Enforcement

Ex-officious audit procedure: sanctions

- Both “hard” and “soft” sanctions are used, in practice, to ensure compliance in a particular case and promote a culture of compliance.

- Injunctions
- Publication of decisions
- Sanctions

- Communication to Ombudsman
- Recommend personal liability (public officers)



Key elements:

- Fines?
- Previous meeting with the sector representatives.
- To define roles and responsibilities
- Select a representative sample of the sector
- A “high level” contact person in the audited organization
- Possibility to direct computer check-up in the audited organization
- The audited organization remain anonymous in the final report and recommendations
- Report with mandatory recommendations
- Publication of mandatory recommendations: transparency and visibility of the sectorial audit



3.2 Preventive Enforcement

Example: Public and Private Schools

Basic information:

- Public Centers: 18.239
- Private Centers 7.470
- Total Centers 25.709
- Type of centers: 4
- Autonomous Regions
(Comunidades autónomas): 17
- Inspectional Centers: 61
- Resources per inspection:
 - 2 inspectors in-situ/3-4 dias
 - 30-40 sheets/inspection statement
(without annexes)
- Inspectors: 14
- Duration: more than 2 years
- Final report with 118 sheets and including more than 100 recommendations**

Regions	Public centers		Private centers	Private centers	TOTAL
	School	High school	Public budget	Private budget	
ANDALUCÍA	1	1	1	1	4
ARAGÓN	1	1	1	1	4
ASTURIAS	1	1	1	1	4
CANARIAS	1	1	1	1	4
CANTABRIA	1	1	1	1	4
CASTILLA-LA MANCHA	1	1	1	1	4
CASTILLA Y LEÓN	1	1	1	1	4
CATALUÑA	(*)	(*)	1	1	2
C. VALENCIANA	1	1	1	1	4
EXTREMADURA	1	1	1	1	4
LA RIOJA	1	1	1	(**)	3
GALICIA	1	1	1	1	4
ISLAS BALEARES	1	1	1	1	4
MADRID	(*)	(*)	1	1	2
MURCIA	1	1	1	1	4
NAVARRA	1	1	1	1	4
PAÍS VASCO	(*)	(*)	1	1	2
TOTAL	14	14	17	16	61

(*) Estas Comunidades Autónomas tienen Agencia de Protección de Datos Autónoma.

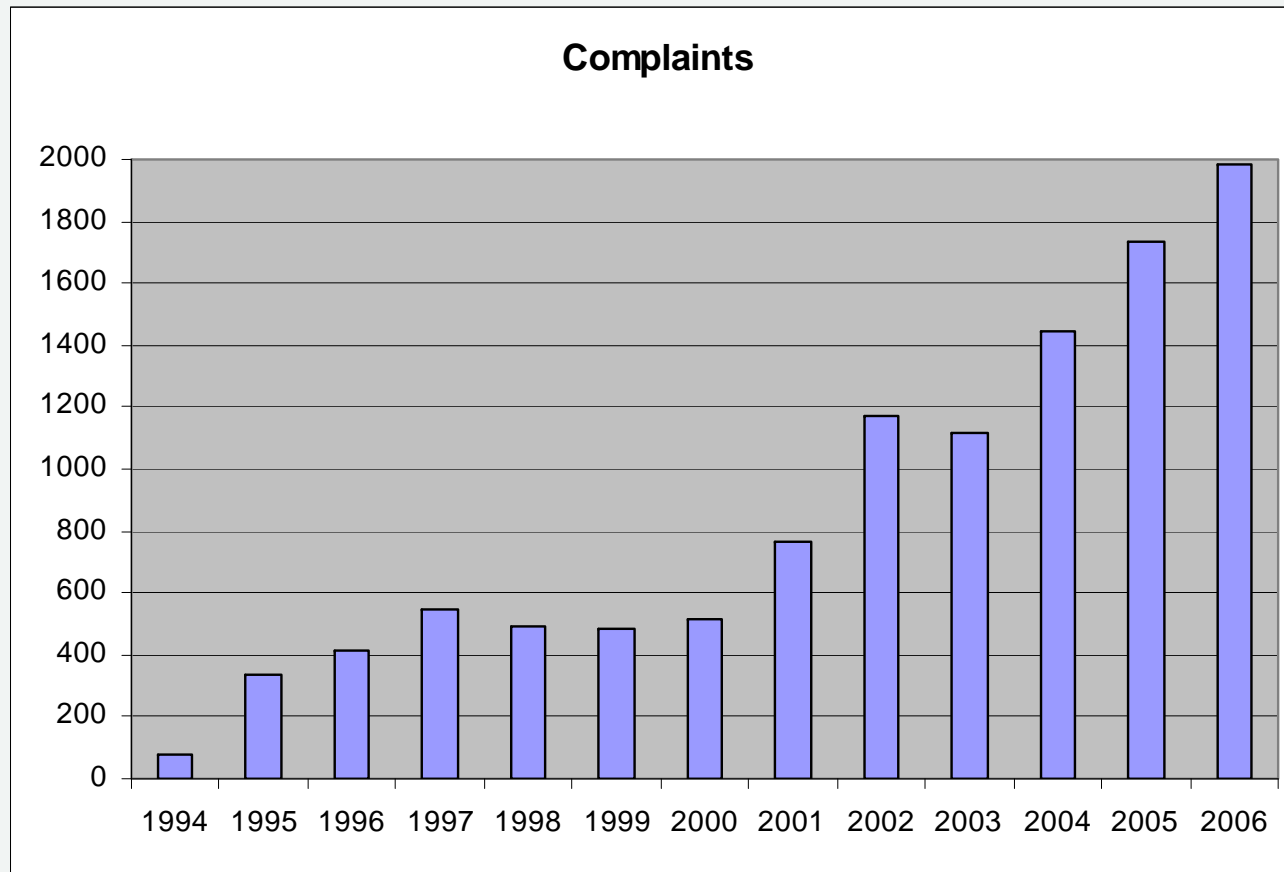
(**) La Comunidad Autónoma de La Rioja no tiene colegios privados, toda la enseñanza básica es pública o concertada.



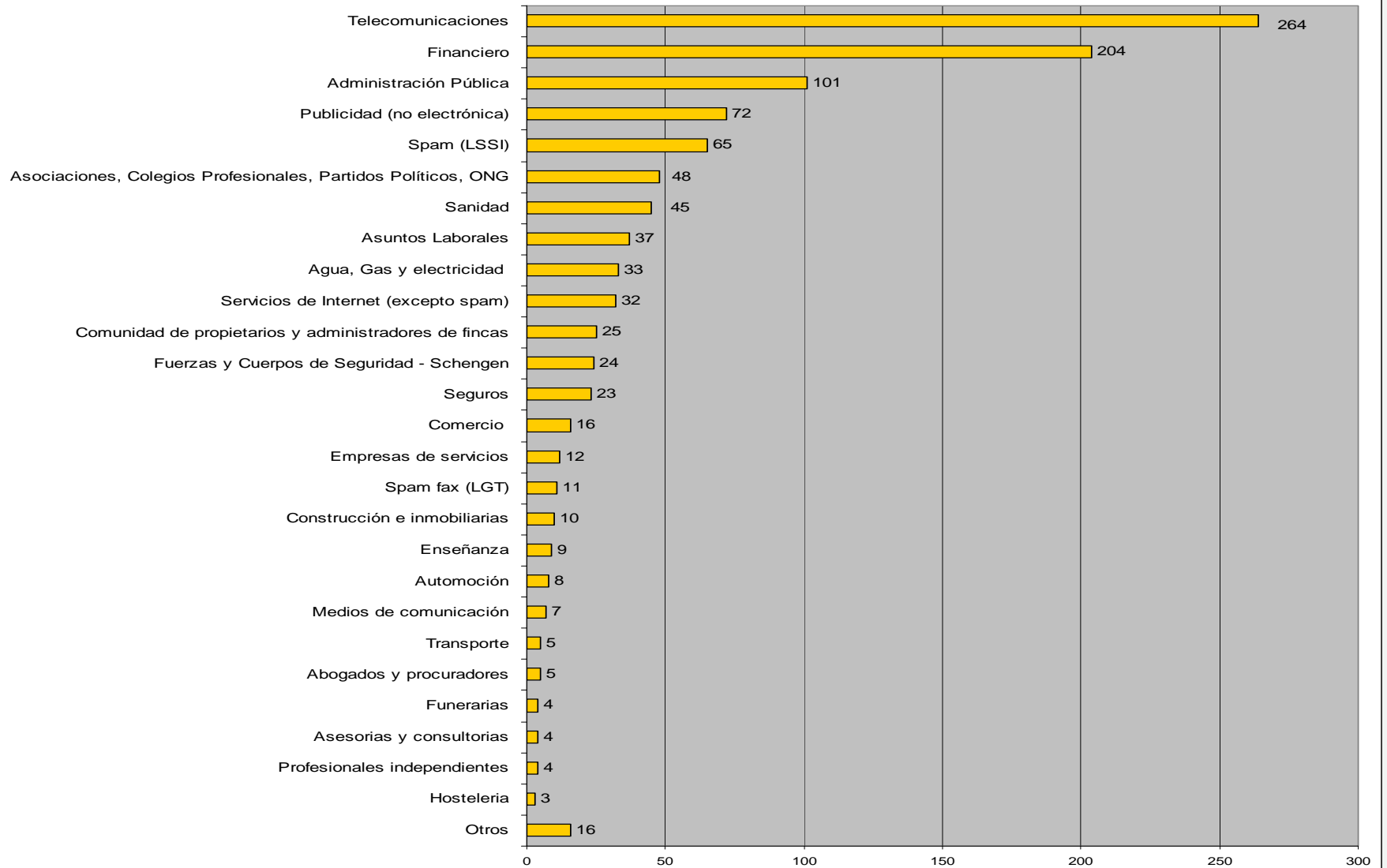
3.2 Preventive Enforcement Sectors Audited by the AEPD

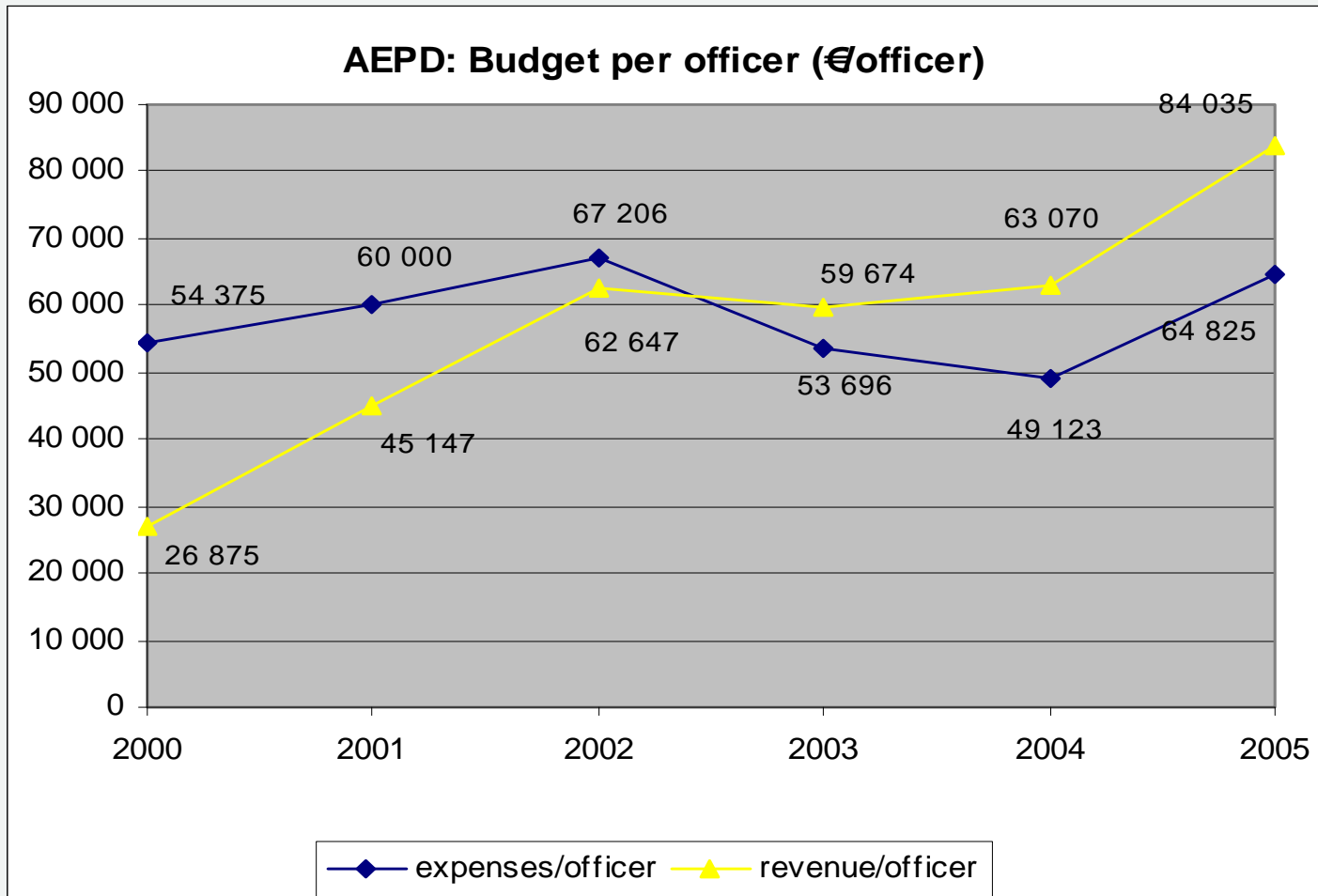
• **Sectorial audits** provide incentive to industry to comply with the law, and support the regulation process. [Most of them in: <https://www.agpd.es/index.php?idSeccion=75>]

- 2006 **Public and Private Schools**
- Internet recommendations
- 2005 Personal Recruitment by Internet
- 2004 Hospitals Laboratories
- National Institute of Public Administration
- **Hotel Chains**
- 2003 **National Institute of Statistics, Censuses of Population and Housing**
- 2002 **Television Game Shows**
- Online Banking
- Common File on Credit History
- 2001 **National Institute of Statistics**
- Auto Insurance Claim History
- Department Stores
- Europol
- 2000 **Telecommunication operators (mobile phones, 3 operators)**
- Electronic Commerce
- Military Hospital
- Psychiatric Prison Hospital
- National AIDS register
- Directorate General of Traffic
- National Center of Epidemiology
- 1999 National Agency for Taxes
- **Insurance companies**
- Common File on Credit History
- Private Detectives
- **Telecommunication operators (fixes lines, 4 operators)**
- 1998 **Bingo Halls**
- 1997 **Large Public Hospitals (more that 1000 beds)**



Investigations by sectors







The essentials for effective enforcement:

1. COMPETENCE AND POWERS:

Effective powers of investigation by law (check-up in situ ; direct access to computers; ability to compel data controllers to collaborate in investigations..)

2. HUMAN RESOURCES:

Skilled technical (IT) and legal experts, working together in permanent cooperation.



3. ORGANIZATIONAL FACTORS:

Definition of roles and responsibilities among inspectors (technical experts) and (legal) instructors.

Team effort (several inspectors working together in a case..)

Cross training inspectors-instructors (technical/legal expertise)

4. EXPERTISSE:

Since 1997 developing audits in all sectors



5. IN PERFORMING THE AUDITS:

- Selection of representative sample.
- Having high level contact person in the organization as interlocutor
- Direct check-up in the audited organization

6. COMPETENCE TO REQUEST AND PROVIDE INTERNACIONAL ENFORCEMENT COOPERATION



An example of the the importance of direct access to computers...

Microsoft Access

Archivo Edición Ver Insertar Formato Registros Herramientas Ventana ?

alumnos : Tabla

Apellidos	Nombre	Recomendación	Motivo no recomendación	Fecha Nacimi	Código
[REDACTED]	Susana	<input checked="" type="checkbox"/>	Dice que no se siente preparac	15/06/79	50014
[REDACTED]	María	<input checked="" type="checkbox"/>	Teléfono desconocido	17/12/79	50005
[REDACTED]	Vanessa	<input checked="" type="checkbox"/>	Es muy agresiva	30/06/80	50002
[REDACTED]	Cristina	<input checked="" type="checkbox"/>	el nº tfno. Es de una empresa,	29/07/81	50015
[REDACTED]	Isaac	<input checked="" type="checkbox"/>	Esquizofrenia, tiene problemas	22/05/80	50002
[REDACTED]	Beatriz	<input checked="" type="checkbox"/>	Dio problemas en el ciclo	29/06/81	50014
[REDACTED]	Sergio	<input checked="" type="checkbox"/>		21/06/79	50014
[REDACTED]	Jose Antonio	<input checked="" type="checkbox"/>	Mal funcionamiento en FCT	28/11/81	50002
[REDACTED]	José Luis	<input checked="" type="checkbox"/>	Se le han hecho ofertas, no en	19/05/79	50002
[REDACTED]	Maria	<input checked="" type="checkbox"/>	Tratamiento nervios	09/08/77	50007
[REDACTED]	Virginia	<input checked="" type="checkbox"/>	Pasota	13/09/79	50008
[REDACTED]	Ana Patricia	<input checked="" type="checkbox"/>	Quejas en la FCT por temperar	10/03/80	50014
[REDACTED]	Noemi	<input checked="" type="checkbox"/>	Limitada, cometio errores en la	06/11/79	50620
[REDACTED]	Sonia	<input checked="" type="checkbox"/>	Poco Activa	28/03/72	50002
[REDACTED]	Ana Belen	<input checked="" type="checkbox"/>	Tiene muchas limitaciones	10/09/80	50013
[REDACTED]	Elena	<input checked="" type="checkbox"/>	Teléfono desconocido	09/01/79	50620
[REDACTED]	M ^a Dolores	<input checked="" type="checkbox"/>	No tiene cualidades para come	26/11/79	50002
[REDACTED]	Rosa Maria	<input checked="" type="checkbox"/>	No tiene perfil de comercial	17/12/81	50002
[REDACTED]	M ^a Elena	<input checked="" type="checkbox"/>	Ella prefiere trabajar de Saná	18/11/80	50002
[REDACTED]	Ana	<input checked="" type="checkbox"/>	FCT problemática	27/11/81	50002

Registro: 4 de 96 (Filtrado)

Vista Hoja de datos

Microsoft Access

Bolsa de Trabajo

Microsoft Access

6:38

PROTOCOLO ASIGNACION CONTRASEÑAS

FECHA: 23-2-05 (Expiran el 23-9-2005)

Con esta fecha se le asigna la siguiente contraseña, recordando el deber de confidencialidad con respecto a la misma.

Contraseña	NOMBRE Y APELLIDOS	D.N.I	APROBADA POR
[REDACTED]	José [REDACTED]	[REDACTED] 47	[REDACTED]
2	Luis [REDACTED]	[REDACTED] 03	[REDACTED]
3	Eduar [REDACTED]	[REDACTED] 00	[REDACTED]
4	Migu [REDACTED]	[REDACTED] 10	[REDACTED]
5	M ^a Anton [REDACTED]	[REDACTED] 84	[REDACTED]
6	Virg [REDACTED]	[REDACTED] 97	[REDACTED]
7	Pilar [REDACTED]	[REDACTED] 18	[REDACTED]
8	M ^a Jos [REDACTED]	[REDACTED] 76	[REDACTED]
9	M ^a J [REDACTED]	[REDACTED] 98	[REDACTED]



Thanks for your attention!

