

Noves pràctiques de Ciberseguretat per fer front al nou panorama legislatiu europeu.

La resposta del professional d'informàtica
davant aquest repte.

Prof. Manel Medina

Dir. MsC Cybersecurity Management

Coord. Científico APWG.EU

Dir. esCERT-inLab-UPC

Contenido

- ○ ○ ● ○ ○ ○ ○ ○ ○ ○ ○ ○ ●
- Legislación comunitaria de:
 - Reglamento General de Protección de datos
 - Directiva de Ciberseguridad
- Análisis de riesgos: legales, sociales, corporativos
 - Para el pequeño
 - Para el grande
- ¿Estamos solos en el ciberespacio?
 - ¿De quién debemos protegernos?
 - ¿Seremos capaces de afrontar el reto?
 - ¿A quién podemos pedir ayuda?

Estrategia Europea de Ciberseguridad

La estrategia establece planes para afrontar retos en cinco áreas prioritarias:

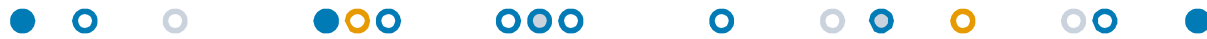
- Alcanzar cyber **resilience**
- Reducir drásticamente el **ciberdelito**
- Desarrollar política y capacidades de **ciber defensa** relacionada con la política de seguridad y defensa común de la UE (CSDP)
- Desarrollar **recursos industriales** y tecnológicos de ciber-seguridad
- Establecer una **política internacional coherente** para el ciberespacio en la UE

Contexto Legislativo (I):

● Protección de Datos Personales

- European Commission's proposal on a comprehensive reform of data protection rules (2012): [Art. 30, 31 y 32](#) abordan las medidas de seguridad y la notificación de incidentes
- Communication on Personal Data Protection in the European Union COM (2010) 609
- Framework Decision 2008/977/JHA
- Directiva 2002/58/EC on privacy and electronic communications (ePrivacy Directiva). Art. 4: "*Security of processing*"
- Old: Data Protection Directive **95/46/EC**
- **New: GDPR** approved spring 2016. Due 2018

Contexto Legislativo (II): Cyber-crimen



- European Commissions' Communication on "Towards a general policy on the fight against cyber crime", COM(2007) 267 final
- Council Framework Decision [2005/222/JHA](#) of 24 February 2005 on attacks against information systems
- the work of the G8 and the [Council of Europe Convention on cybercrime](#) (Budapest, 23.XI.2001)
- New: **NIS Directive** approved spring 2016.

Contexto Legislativo (III):

Telecomunicaciones

- EU electronic communications regulatory framework (Directive 2009/140/EC, Art. 13a)
 - Oper. Telecom & ISP deben tomar medidas para garantizar la seguridad de sus redes.
 - Proveedores deben informar a las autoridades competentes (CNA) incidentes relevantes: s/impacto, afectados, cobertura.
 - CNA deben informar ENISA y otras CNAs cuando sea necesario, ej. incidentes con impacto transfronterizo.
 - CNA deben informar anualmente los incidentes a ENISA y la CE.

Contexto Legislativo (IV): Sistemas de control Industrial

- NIST SP800-82 Guide to Industrial Control System Security (ICS)
- ICS-CERT US Control System Security Program (CSSP)
- NERC CIP-003-4
- ISA/IEC-62443
- ENISA Protecting Industrial Control Systems. Recommendations for Europe and Member States
- INTECO Estudio sobre la seguridad de los sistemas de monitorización y control de procesos e infraestructuras (SCADA)
- Guía de Buenas Prácticas para la elaboración de los Contenidos Mínimos de los Planes de Seguridad del Operador
- Idem. de los Planes de Protección Específicos
- **Ley 8/2011 por la que se establecen medidas para la Protección de las Infraestructuras Críticas**
- **R.D. 704/2011 por la que se aprueba el Reglamento para la Protección de las Infraestructuras Críticas**
- Acuerdo Consejo de Ministros sobre Protección de Infraestructuras Críticas
- Estrategia Española de Seguridad
- Ley 2/1985 Protección Civil
- R.D. 407/1992 Norma Básica de Protección Civil
- R.D. 1468/2008 que modifica R.D. 393/2007 Norma Básica de Autoprotección de Centros y Establecimientos
- **Directiva 2008/114/CE del Consejo, sobre Identificación y Designación de las Infraestructuras Críticas Europeas** y la Evaluación de la Necesidad de Mejorar su Protección

Reglamento General de Protección de Datos



Consejo min. EU: Será Reglamento (15/12/15)

- **Controldores de datos** deben solicitar **inambiguamente** el consentimiento del sujeto de los datos
- **Derechos de protección de datos:**
 - **Acceso más sencillo** a sus datos
 - Información más detallada y transparente sobre la gestión de los datos personales
 - Política de privacidad en lenguaje claro y sencillo
 - **Derecho al Olvido**, sin dilación innecesaria
 - **Dercho a la portabilidad**, ej. Entre redes sociales
 - **Perfilado** limitado
 - Los sujetos de datos podrán **apelar** decisions de su DPA a sus **tribunals nacionales**, independientemente del país de establecimiento del controlador de los datos: One-stop-shop

Consejo min. EU: Será Reglamento (15/12/15)

- Conjunto único de reglas en toda la UE, aumento de cooperación entre DPA,s
- Controladores pueden establecer **mecanismos adecuados a los niveles de riesgo** definidos, basándose en una estimación del riesgo asociado a su proceso de datos personales.
- Controladores deben **implantar medidas de seguridad y auditabilidad adecuadas**, proporcionando, sin retraso indebido, **notificación de robo de datos** a CNA y afectados.
- **Multas para controladores** de hasta **20M€ o 2% o 4% de cifra de negocio anual global** (la mayor de ellas, según casos)
- **Transferencias de DP a 3º países** garantizadas por decisiones y salvaguardas adecuadas (clausulas de PPD, reglas corporativas vinculantes, cláusulas contractuales)

Requisitos Generales para organizaciones

- **Informar** brechas de datos **en 72h**
- Derecho de **recuperar** en soporte electr. **Portable**
- **Portabilidad** entre procesadores
- Derecho **cancelación**, si retención ilegítima
- **Consentimiento** de adquisición de PII revocable
- Obtener **autorización** para **transf.** Fuera de la EEA
- **Identificar DPO**: >250 trabajadores, >5.000 sujetos/año, **AAPP**.
- Info **contacto** controlador
- **Privacidad por diseño** en desarrollo de procesos de negocio, productos y servicios

Obligaciones de auditabilidad para controladores

1. maintain certain **documentation to allow audit**
2. put in place effective procedures and mechanisms, and **conduct a data protection impact assessment** for more risky processing (DPAs should compile lists of what is caught), to consider the **likelihood and severity of the risk**.
3. implement **data protection by design and by default, e.g. data minimization**
4. Implement **Binding Corporate Rules (BCRs)** as a means of legitimising **intra-group international transfers**. The BCRs must be legally binding and apply to and be **enforced by every member of the group** of undertakings/ enterprises engaged in a joint economic activity, including employees.

Recomendaciones para preparación a la GDPR

1. **Políticas y prácticas** para reaccionar rápidamente a brechas de datos, y notificar a tiempo (72h) si se requiere.
2. Marco de **auditabilidad**: estandarizado, monitorización, revisión, evaluación, minimizar procesado y retención de datos, mecanismos de protección. Validar formación de empleados. Estimación del impacto de procesos de DP.
3. **Demostrar cumplimiento de privacidad por diseño: Evaluación y validación sistemáticas.**
4. **Documentos de consentimiento** adecuados: informar, especificidad y libertad. O interés legítimo de proceso.
5. **Políticas accesibles e inteligibles.**
6. Derecho legítimo: **retención**. Portabilidad. Olvido/Cancel.
7. **Contratos de servicio: responsabilidad compartida**
8. **BCR**: Reglas corporativas vinculantes. Derecho legítimo de transferencia internacional

Notificación Brechas datos (BD) Cyber-seguridad

- Comité Art.29, subgr. Technol (sustituido por el **comité europeo de protección de datos: EDPB**) & ENISA acuerdan con Telcos y APD,s: criterios de tipos de incidents a informar:
 - **Impacto: Físico** (salud), Material (admin, financ., legal), **Emocional** (social: humillat, psico.: miedo, stress,...)
 - **Severidad BD =**
Criticidad datos * facilidad identif + circunstancias BD
 - **Procesado automático notificaciones y medidas:**
 - Estadísticas, respuestas, análisis, harmon. transfronter.

Valores cuantitativos



- **Criticidad:**

- 1. simple, 2. comportamiento, 3. financiero, 4. sensible
- No asociado al tipo de dato sino a la información que revela del individuo y el impacto potencial privacidad
 - + Volumen datos + Campo oper. + Personas (VIP)
 - - Datos inválidos – Conocidos – naturaleza datos

- **Identificabilidad:** $\frac{1}{4}$ Despreciable, $\frac{1}{2}$ limitada, $\frac{3}{4}$ apreciable, 1. Máxima

- **Circunstancias BD:**

- + Confidencial: 0. limit./incierto, $\frac{1}{4}$ extenso/identif, $\frac{1}{2}$ descon
- + Integr.: 0. recuperado, $\frac{1}{4}$ algún inconv, $\frac{1}{2}$ uso incorr/ileg
- + Dispon.: 0. recuperable, $\frac{1}{4}$ temporal, $\frac{1}{2}$ irrecuperable
- + Intención maliciosa: $\frac{1}{2}$ daño indiv/contr, beneficio

Análisis cuantitativo de severidad



Impacto estimado: severidad

- <2: No afecta, poco inconveniente
- <3: Inconv. Significante, superable poca dificultad
- <4: consec. Importante, difícil superar, daño econ.
- ≥ 4 : consec irreversible, insuperable, largo plazo

Banderolas peculiaridad:

- +100 registros ? Dificultad identificar 1 individuo
- Ininteligibilidad dato: - impacto final

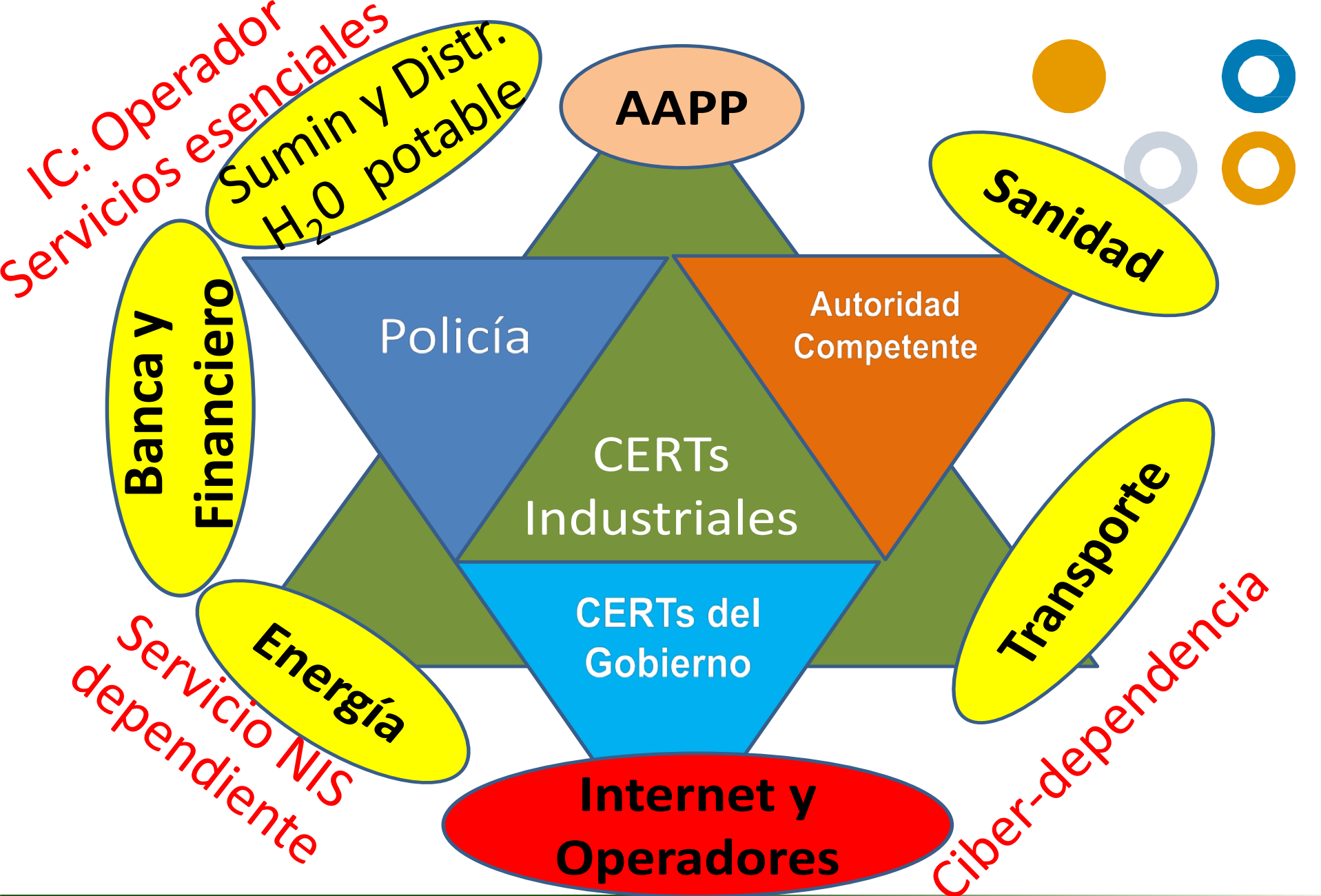
Directiva Ciberseguridad

Medidas propuestas

- Adoptar **estrategia** ciberseg nacional
- Designar **autoridad** ciberseg con recursos adecuados:
 - preven, gestion, responder incidents y riesgos
- Crear mecanismo **cooperación**: EM, EC, ENISA
 - **Compartir alertas de riesgos e incidentes** entre puntos de acceso únicos nacionales: n/g CSIRTs, y CERT-EU
 - **Intercambiar info** y responder ataques e incidentes
 - **Crear red de CSIRTs** nacionales para favorecer coop.
- Adoptar **gestión riesgo e informar** incidentes relevantes

Acuerdo Trilog 2015/06/29

- **Prov. Servicios Soc Info** (PSSI: buscadores, (redes sociales), portales e-comm, proveedores cloud) serán tratados de forma diferente a los servicios esenciales
- Cumplimiento parcial directiva a Proveedores SSI
- Deben cumplir: Operadores infraestructs Mercado financiero, interconex internet, cadena alimenticia...
- Cada estado miembro (EM) determina operadores esenciales,
 - según criterio establecido en Directiva NIS.
 - Ej. **Si un PSSI ofrece servicios a un CIP, estará obligado como un Operador de Mercado**
- **Multas de hasta 5% volum negocio nac/EU o 100M€.**



Sectores crítics



- **digital infrastructure** — internet exchange points, TLD name registries, and DNS service providers;
- **energy** — electricity/gas suppliers & system operators of: distribution, transmission, storage, LNG operators, and operators of oil and natural gas production, refining and treatment facilities;
- **transport** — air and maritime carriers, traffic management control operators, airports, railways, road traffic management control and intelligent transport system operators;
- **banking** — credit institutions in accordance with the Capital Requirements Regulation (575/2013);
- **financial market infrastructure** — stock exchanges and central counterparties;
- **health** — healthcare providers (including hospitals and private clinics);
- **drinking water** — supply and distribution entities.

Criterios selección Operador Infrastruct. crítica

- Número de **usuarios** dependientes del servicio
- La de otros sectores críticos del servicio ofrecido dependenciado por el operador;
- El **impacto económico, social o en seguridad**, que los incidentes podrían tener según naturaleza y duración
- la **cuota de Mercado** del operador;
- el **ámbito geográfico** que podría ser afectado por un incidente; y
- la **importancia del operador** para mantener un nivel de servicio suficiente, a la vista de operadores alternativos potenciales.

Qué reportar (recopilar) en caso de incidente

- **Información necesaria** para evaluar la seguridad de sist. Info. y redes:
 - políticas de seguridad.
 - Prácticas de operación.
 - **Registros y supervisión.**
- **Evidencias de implantación efectiva** de la política:
 - **Resultados de auditoria** por auditor cualificado (incl. detalle de pruebas) o
 - Auditorías previas de autoridad competente y **aplicación de recomendaciones vinculantes para remediar disconformidades**
 - Planes de **formación y resultados de ciber-ejercicios y evaluaciones de personal**

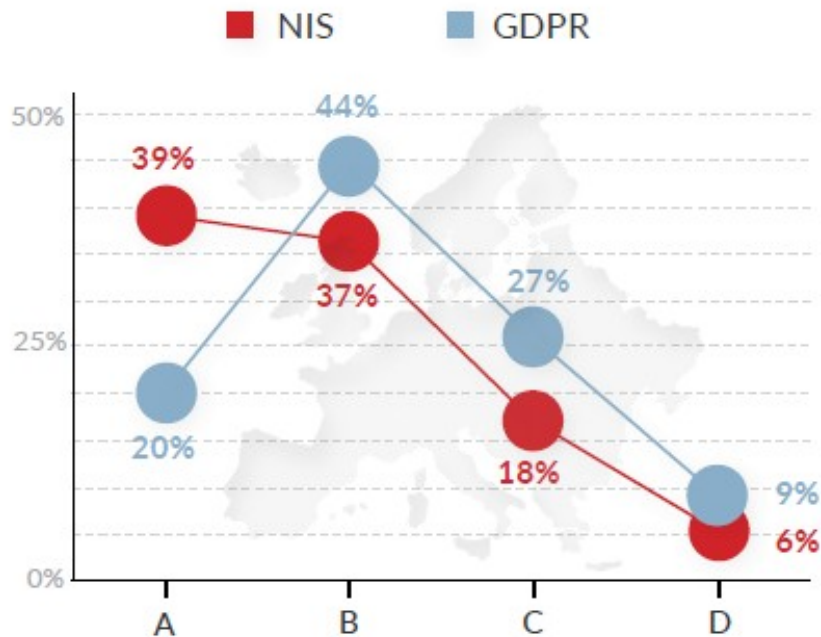
Consideraciones de Privacidad

- Qué:
 - Intercambio info. **Canal seguro entre CERTs**
 - Circular **alertas tempranas** de riesgos e incidents
 - **Publicar regularmente info no-confid de alertas** y resp. coordinada en web común
- Quién: Actores relevantes
- ***Datos incidentes:***
 - ***Simples (pública)***
 - ***Circunstancias: Difusión limitada, no maliciosa***
 - ***Identificación despreciable***

¿Cómo afrontar el Cumplimiento?

Preparación para NIS/GDPR

Organisations Better Prepared for NIS than GDPR



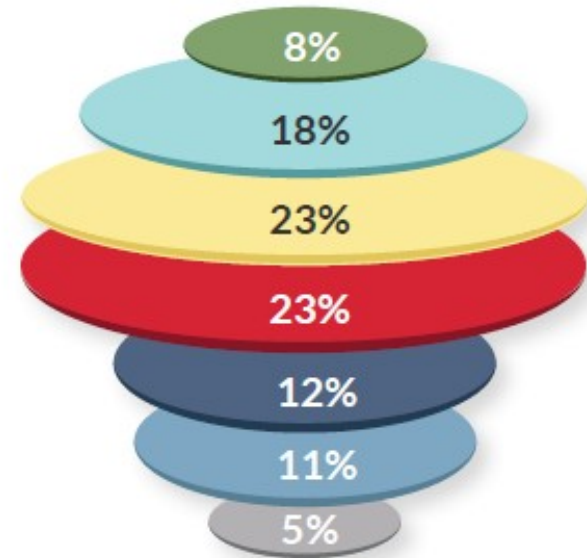
A - All Required Measures are in Place

B - Most Required Measures are in Place

C - Some Required Measures are in Place

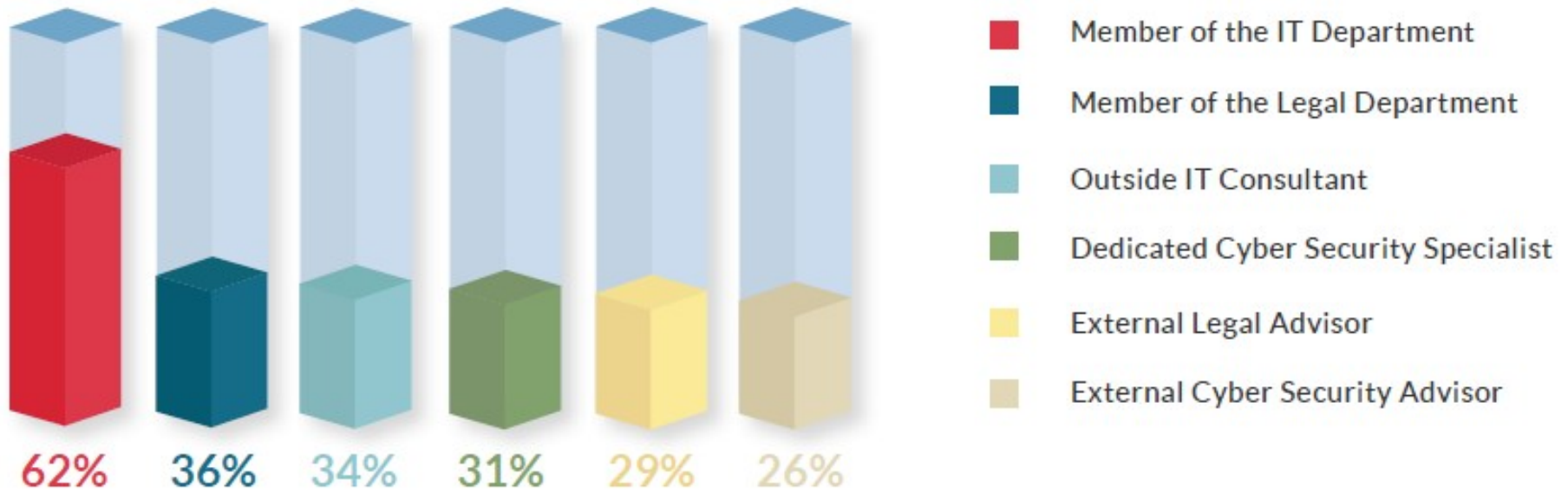
D - No Required Measures are in Place

Cost and Complexity Remain Significant Challenges

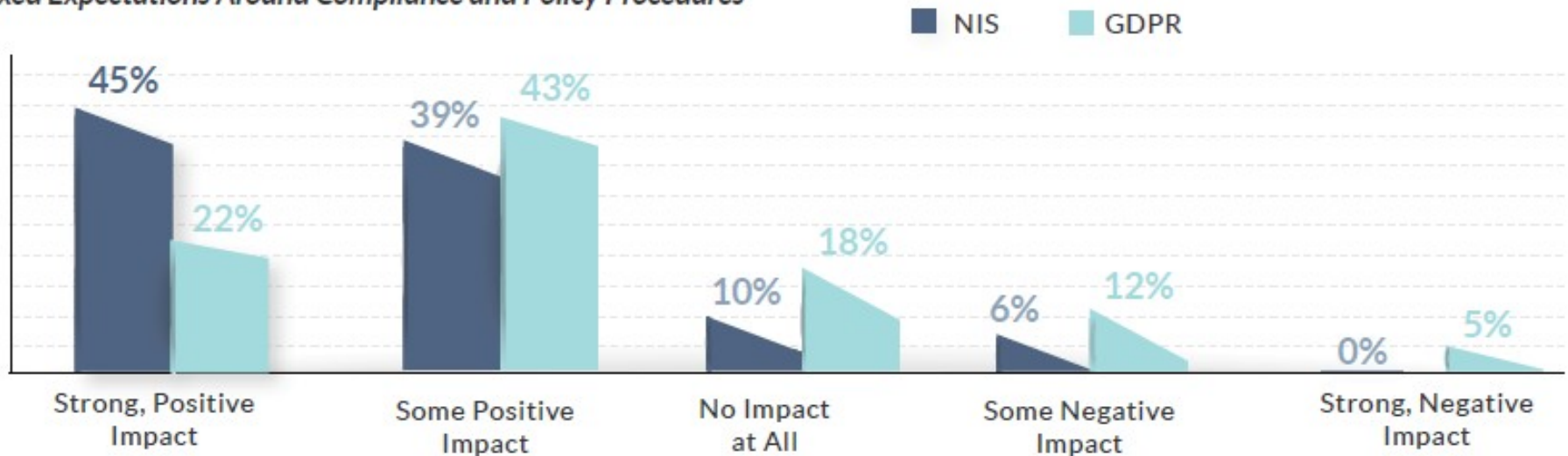


- Incident Reporting Process Requirements
- Policy Complexity
- Implementation Costs
- New Hardware/Software Investment Requirements
- Sourcing Sufficient Expertise
- Pre-enforcement Confirmation of Systems, Processes and Policies
- Incident Reporting Timeframe Requirements

Responsibility for NIS/GDPR Planning



Mixed Expectations Around Compliance and Policy Procedures



Preocupaciones empresas

Loss of Business and/or Revenue



Potential Fines



Damage to Reputation



Decrease in Customer Confidence and Loyalty



Legal Costs



Increased Consultancy Costs to Deal with Fallout



Requirement to Carry Out Extensive Security Audits



Recomendaciones

- Todas las empresas deberían **revisar su infraestructura de red y política TIC**
- Conseguir alguna **certificación / auditoría**
- Adoptar alguna guía o **recomendación colectiva**
- Fomentar la **formación interna** de capacidades
- Identificar **asesores externos** para planificación
- Establecer **canales de Comunicación seguros** con equipo(s) de coordinación de incidentes
- Formalizar **acuerdos de cooperación en gestión de ciberseguridad y respuesta a incidentes**

Iniciativas de soporte al cumplimiento

UK: 5 **requisitos esenciales de ciberseguridad** al alcance de cualquier organización: **SME, AAPP, ...**

1. Cortafuegos y pasarelas perimetrales
2. Configuración segura
3. Control de acceso
4. Protección anti-malware
5. Gestión de parches

Otras iniciativas relacionadas con DNIS/GDPR:

- **CERTSI** ha publicado algunos informes y recomendaciones para empresas y Admin. Pública
- https://www.incibe.es/CERT/guias_estudios/guias//GuiaManual_LOPD_EELL
- **APWG** tiene un mecanismo de notificación de incidentes de robo de datos personales, que puede ser usado por sus miembros.
- Otros países como UK han desarrollado ya el Sistema que requerirá la directiva NIS para compartir información de ciberseguridad: el CiSP (ataques y vulnerabilidades)
- **Europol/EC3 y policías como la Guardia Civil** también están trabajando en definir un **formato de intercambio y compartición de información en tiempo real**, para aplicarlo a gestión de riesgo, garantizando la confidencialidad.

UPC School: Postgrado Gestión Riesgo y Cumplimiento

Postgrado orientado a auditorías de cumplimiento,

Integrado en Máster de gestión de la ciberseguridad eminentemente técnico

<http://www.talent.upc.edu/esp/professionals/presentacio/codi/221100/cybersecurity-management/>



UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
School of Professional & Executive Development

Inicio Portada	Conoce la UPC School Quiénes somos	Másters y posgrados Para profesionales	Soluciones corporativas Para empresas	
Formación	Descuentos, préstamos y ayudas	Alumnos internacionales	Bolsa de trabajo	Servicios Académicos

- Presentación
- Contenidos
- Dirección y profesorado
- Información general
- Colaboradores
- Testimonios
- Videos y noticias

CYBERSECURITY MANAGEMENT

MÁSTER PRESENCIAL.

PRESENTACIÓN



INCIBE ofrece un programa de becas para cursar el máster y los posgrados sobre ciberseguridad de la UPC School.



Certificaciones profesionales: ISACA, NISDL, ...



[INICI](#)

[QUI SOM ▾](#)

[CERTIFICACIONS ▾](#)

[FOTOGRAFIES](#)

[CALENDARI ▾](#)

Barcelona Chapter



CURS OFICIAL ONLINE DE PREPARACIÓ A L' EXAMEN CISA
Inici: 15 octubre 2015



La ciberseguridad a un clic de tu empresa



Oficina
de Seguridad
del Internauta

[¿Quiénes somos?](#) [Encuesta de valora](#)

[Ponte al día](#) [¿Cuánto sabes?](#) [¿Qué deberías saber?](#) [¿Cómo protegerte?](#) [¿Necesitas ayuda?](#)



Unifying the Global Response to Cybercrime

Home

Report Phishing

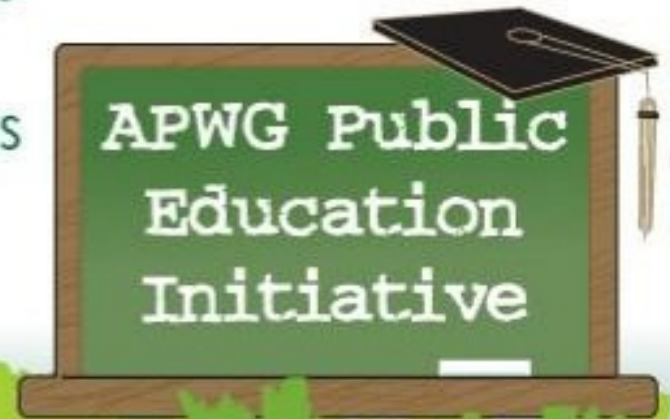
Collaborator Solutions

Resources

Events

APWG.EU Ne

APWG crafts end-user education schemes for both consumers and enterprise users, through warning systems and public-awareness campaigns





PARA | PIENSA | CONÉCTATE®

Consejos y recomendaciones



Mantenga Limpia su Computadora



Proteja su Información Personal



Conéctese con Cuidado



Manténgase Informado sobre la Web



Sea un Buen Ciudadano Virtual

**Pienso
ANTES de
hacer clic.**

PARA | PIENSA | CONÉCTATE

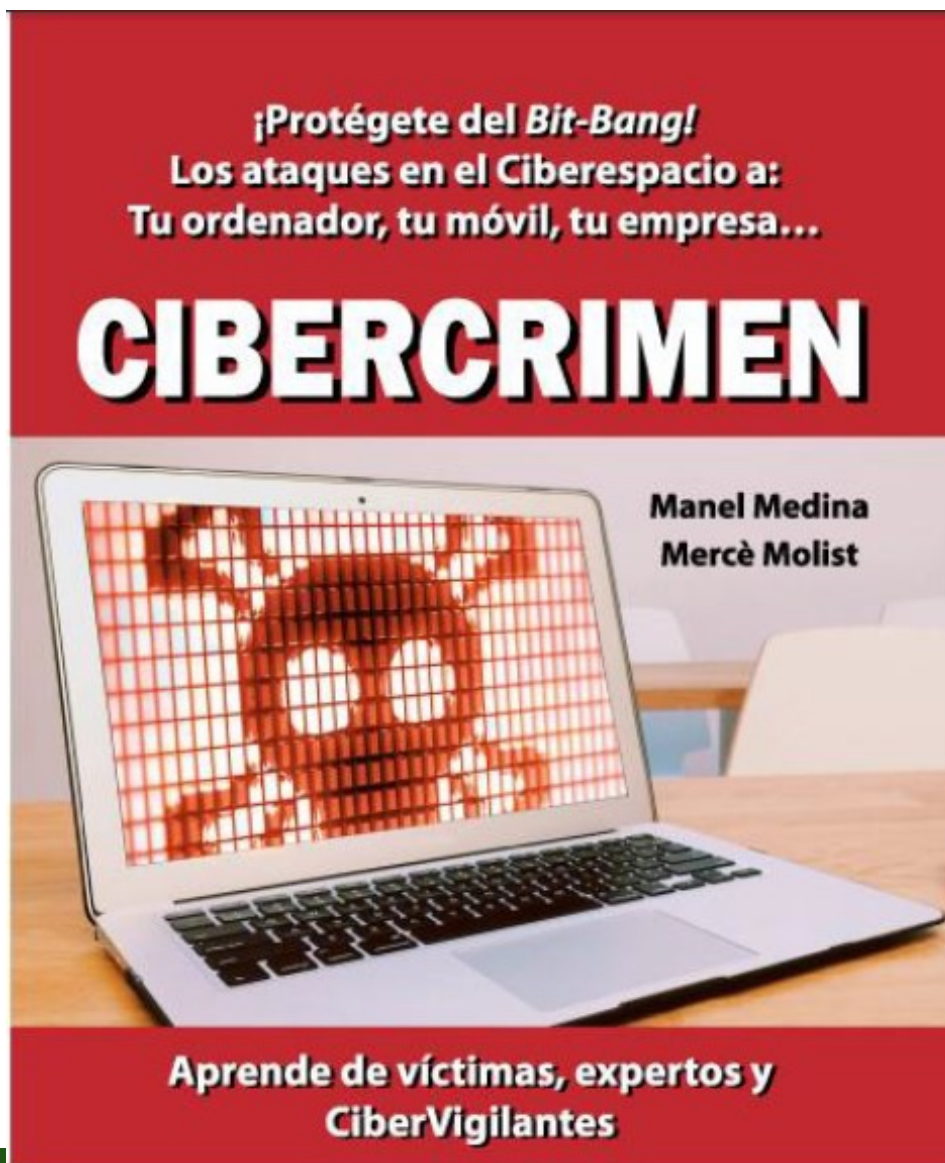
www.consumidorsicilia.es | www.consumer.es | www.consumer.es

**MI CONTRASEÑA MEZCLA
LeTrAs,
#númerOs
y
\$ímbol!#**

PARA | PIENSA | CONÉCTATE

www.consumidorsicilia.es | www.consumer.es | www.consumer.es





○ ○ ●

Conclusiones:

- **Riesgos** conocidos:
Mira donde te metes!
- **Ataques** publicados:
Aprende de los errores ajenos!
- **Defensas** aplicables:
Elige el que más te conviene!
- **Protectores** disponibles:
Pide ayuda cuando la necesitas!