



# Marcs legislatius i regulatoris

**[PQ]  
[TM]** Pla de  
Qualificació en  
Tecnologia  
Mòbil

Organitza:



SOC

Servei d'Ocupació  
de Catalunya

Generalitat  
de Catalunya



Unió Europea  
Fons Social Europeu  
L'FSE inverteix en el teu futur

Imparteix:

**UOC** Universitat  
Oberta de Catalunya

Col·labora:

**MOBILE  
WORLD CAPITAL.  
BARCELONA**

# Contingut

- Esquema Nacional de Seguretat
- Estàndards de la PCI
- Protecció de la privadesa

# Esquema Nacional de Seguretat (ENS)

- Real Decret 3/2010, de 8 de gener
  - Llei estructurada en 10 capítols

Finalitat: creació de condicions necessàries de confiança en l'ús de mitjans electrònics, a través de mesures per garantir la seguretat dels sistemes, les dades, les comunicacions i els serveis electrònics, que permeti als ciutadans i a les administracions públiques l'exercici de drets i el compliment de deures a través d'aquests mitjans.

**BOLETÍN OFICIAL DEL ESTADO**  
Núm. 25 Vernes 29 de enero de 2010 Sec. I. Pág. 8089

**I. DISPOSICIONES GENERALES**  
**MINISTERIO DE LA PRESIDENCIA**

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.

La necesaria generalización de la seguridad de la información es subordinada, en gran medida, a la confianza que genera en los ciudadanos la relación a través de medios electrónicos.

En el ejercicio de las Administraciones públicas, la consecución del derecho a comunicarse con ellas a través de medios electrónicos comporta una obligación corresponsiva de las Administraciones de garantizar la confidencialidad, integridad y disponibilidad de la información que la libertad y la calidad sean reales y efectivas, y la remoción de los obstáculos que impiden o dificultan su pleno. Lo que demanda incorporar las peculiaridades que exigen una aplicación práctica de la legislación en materia de protección de datos.

A ello ha venido a dar respuesta el artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso a la información de carácter administrativo, que establece la creación del Esquema Nacional de Seguridad, cuyo objeto es el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la eficiente prestación de servicios.

La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información que genera la actividad de las administraciones, los datos, las comunicaciones, y los servicios electrónicos, que permite a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de medios electrónicos.

El Esquema Nacional de Seguridad persigue fundamentar la confianza en que los sistemas de información prestan sus servicios y custodian la información de acuerdo con las normas establecidas en la legislación de protección de datos de carácter personal, y en que la información pueda llegar al conocimiento de personas no autorizadas. Se desarrollará y establecerán las medidas necesarias para garantizar la eficiente prestación de servicios cumpliendo los requisitos de los mismos y las infraestructuras que lo apoyan.

Actualmente los sistemas de información de las administraciones públicas están fuertemente interconectados entre sí y con las empresas y las personas físicas y jurídicas que interactúan con las administraciones. De esta manera, la seguridad tiene un nuevo reto que va más allá del aseguramiento de la información que genera la actividad de las administraciones, ya que su perimetro y los responsables de cada dominio de seguridad deben coordinarse efectivamente para evitar el riesgo de males y fraudes que pudieran dañar a la información o a los ciudadanos.

En este contexto se entiende por seguridad de las redes y de la información, la capacidad de garantizar la confidencialidad, integridad y disponibilidad de los datos de nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometen la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

El Esquema Nacional de Seguridad tiene presentes las recomendaciones de la Unión Europea (Directiva 2001/54/CE CEEC, Erratum de la Comisión de 29 de noviembre de 2001, por la que se modifica su Reglamento interno y Decisión 2001/679/CE del Consejo, de 10 de diciembre, sobre la protección de las personas físicas en lo que respecta a la tratamiento de datos personales y la libertad y seguridad individual del Consejo), la situación tecnológica de las diferentes Administraciones públicas, así como

# **Esquema Nacional de Seguretat (ENS)**

- Els objectius de l'Esquema Nacional de Seguretat són:
  - Crear les condicions necessàries per a l'ús segur dels mitjans electrònics.
  - Establir la política de seguretat en la utilització de mitjans electrònics.
  - Introduir els elements comuns que han de guiar l'actuació de les Administracions públiques i els seus proveïdors en matèria de seguretat de les tecnologies de la informació.
  - Aportar un llenguatge comú per facilitar la interacció de les Administracions públiques, així com la comunicació dels requisits de seguretat de la informació a la Indústria.
  - Aportar un tractament homogeni de la seguretat.
  - Facilitar un tractament continuat de la seguretat.

# Esquema Nacional de Seguretat (ENS)

- Principis bàsics:

- 1. Seguretat integral
- 2. Gestió de riscos
- 3. Prevenció, reacció i recuperació
- 4. Línies de defensa
- 5. Revaluació periòdica
- 6. Funció diferenciada

# Esquema Nacional de Seguretat (ENS)

## ■ Principis bàsics:

- **Seguretat integral**
- Gestió de riscos
- Prevenció, reacció i recuperació
- Línies de defensa
- Reavaluació periòdica
- Funció diferenciada

La seguretat s'entén com un procés integral, amb elements tècnics, humans, materials i organitzatius.

Es prestarà la màxima atenció a les persones que intervenen en el procés i als seus responsables jeràrquics, per tal que aquests no siguin fonts de risc per a la seguretat.

# Esquema Nacional de Seguretat (ENS)

## ■ Principis bàsics:

- Seguretat integral
- **Gestió de riscos**
- Prevenció, reacció i recuperació
- Línies de defensa
- Reavaluació periòdica
- Funció diferenciada

L'anàlisi i la gestió de riscos serà part essencial del procés de seguretat i s'hauran de mantenir permanentment actualitzats.

Permetrà el manteniment d'un entorn controlat, tot minimitzant els riscos fins a nivells acceptables.

# Esquema Nacional de Seguretat (ENS)

## ■ Principis bàsics:

- Seguretat integral
- Gestió de riscos
- **Prevenció, reacció i recuperació**
- Línies de defensa
- Reavaluació periòdica
- Funció diferenciada

La prevenció ha d'eliminar o, si més no, reduir, la possibilitat que les amenaces es materialitzin.

Les mesures de detecció han d'anar acompanyades per mesures de reacció.

Es garantirà la conservació de les dades i informacions en suport electrònic (còpies de seguretat).

# Esquema Nacional de Seguretat (ENS)

## ■ Principis bàsics:

- Seguretat integral
- Gestió de riscos
- Prevenció, reacció i recuperació
- **Línies de defensa**
- Reavaluació periòdica
- Funció diferenciada

Cal disposar d'una estratègia de protecció constituïda per múltiples capes de seguretat, disposada de manera que, quan una de les capes falli, es permeti guanyar temps per a una reacció adequada en front als incidents que no s'han pogut evitar, reduint la probabilitat que el sistema es comprometri en el seu conjunt i minimitzant l'impacte final sobre el mateix.

# Esquema Nacional de Seguretat (ENS)

## ■ Principis bàsics:

- Seguretat integral
- Gestió de riscos
- Prevenció, reacció i recuperació
- Línies de defensa
- **Revaluació periòdica**
- Funció diferenciada

Les mesures de seguretat es reavaluaran i s'actualitzaran periòdicament, per adequar la seva eficàcia a la constant evolució dels riscos i sistemes de protecció, arribant fins i tot a un replantejament de la seguretat, si aquest fos necessari.

# Esquema Nacional de Seguretat (ENS)

## ■ Principis bàsics:

- Seguretat integral
- Gestió de riscos
- Prevenció, reacció i recuperació
- Línies de defensa
- Reavaluació periòdica
- **Funció diferenciada**

Hi haurà un responsable de la informació, un responsable de servei i un responsable de la seguretat.

La política de seguretat de l'organització detallarà les atribucions de cada responsable i els mecanismes de coordinació i resolució de conflictes.

# Esquema Nacional de Seguretat (ENS)

- Tots els òrgans de les administracions públiques hauran de disposar de la seva política de seguretat, amb una sèrie de requisits mínims.
- **L'organització i el procés de seguretat**
  - La seguretat ha de comprometre a tots els membres de l'organització
  - Cal identificar clarament uns responsables.
  - La política ha de ser coneguda per tots els membres de l'organització.

# Esquema Nacional de Seguretat (ENS)

## ■ L'anàlisi i gestió de riscos

- Cal realitzar una gestió de riscos d'acord amb alguna **metodologia reconeguda internacionalment**.

## ■ Gestió de personal

- Tot el personal relacionat amb la informació i els sistemes haurà d'estar format i informat.
- Cal que estiguin supervisats per verificar que se segueixen els procediments establerts.
- Caldrà identificar el personal, per poder aplicar polítiques d'accés i registrar qui realitza cada acció relacionada amb les dades.

# **Esquema Nacional de Seguretat (ENS)**

## **■ Professionalitat**

- Cal tenir personal qualificat.
- El personal rebrà formació específica.
- Els serveis prestats han de comptar amb nivells de maduresa idonis.

## **■ Autorització i control d'accés**

- L'accés al sistema d'informació haurà de ser controlat i limitat als usuaris, processos, dispositius i altres sistemes d'informació, degudament autoritzats, restringint l'accés a les funcions permeses.

# **Esquema Nacional de Seguretat (ENS)**

- **Protecció de les instal·lacions**
  - Els sistemes d'informació es trobaran en àrees específiques, dotades d'un procediment de control d'accés, espais tancats i amb control de les claus.
- **Adquisició de productes de seguretat**
  - Es valoraran positivament aquells que tinguin certificada la funcionalitat de seguretat, d'acord amb les normes i estàndards de major reconeixement internacional.
  - Certificacions!

# Esquema Nacional de Seguretat (ENS)

Organismo de Certificación | Centro Criptológico Nacional



Buscar...



SOBRE OC PRODUCTOS CERTIFICADOS CATÁLOGO PRODUCTOS STIC TIPOS DE CERTIFICACIÓN SOLICITUDES Y FORMULARIOS

## Nuevos laboratorios acreditados



Última hora

Nuevo boletín del departamento de Productos y Tecnologías de Seguridad (PYTEC) del Centro Criptológico Nacional



Productos  
Certificados



Catálogo Productos  
STIC



Cómo certificar un  
producto

# Esquema Nacional de Seguretat (ENS)

[NUESTROS SERVICIOS](#)[QUIÉNES SOMOS](#)[NOTICIAS](#)[CARRERAS  
PROFESIONALES](#)[CONTACTO](#)

ES

[HOME](#) / [NUESTROS SERVICIOS](#) / [ÁREAS DE CONOCIMIENTO](#) / [TECNOLOGÍAS DE LA INFORMACIÓN](#)

## ESPAÑA. Certificación ENS. Compromiso de seguridad

Certifique el cumplimiento de su empresa con los principios y requisitos del Esquema Nacional de Seguridad (ENS)



SOLICITE PRESUPUESTO

DESCARGAR VERSIÓN EN PDF

# Esquema Nacional de Seguretat (ENS)

## ■ Seguretat per defecte

- El sistema d'informació ha de proporcionar la mínima funcionalitat requerida, si hi ha més funcionalitats estem generant riscos.
- L'ús ordinari del sistema d'informació ha de ser senzill i segur, de forma que **una utilització insegura requereixi d'un acte conscient per part de l'usuari.**

# **Esquema Nacional de Seguretat (ENS)**

## **■ Integritat i actualització del sistema**

- Tot element físic o lògic requerirà autorització formal prèvia a la seva instal·lació en el sistema.
- Caldrà conèixer en tot moment l'estat de seguretat dels sistemes, en relació a les especificacions dels fabricants, a les vulnerabilitats i a les actualitzacions que els afectin.

# **Esquema Nacional de Seguretat (ENS)**

- **Protecció d'informació emmagatzemada i en trànsit**
  - Es prestarà especial atenció a la informació emmagatzemada o en trànsit en entorns insegurs (pendrives, tablets, mòbils, etc.)
  - Tota la informació que no estigui en suport electrònic també s'ha de protegir.
- **Prevenció envers altres sistemes d'informació interconnectats**
  - El sistema ha de protegir el perímetre si es connecta a xarxes públiques (Llei 32/2003, de 3 de novembre).
  - Cal controlar el punt d'unió.

# Esquema Nacional de Seguretat (ENS)

Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

---

Jefatura del Estado  
«BOE» núm. 264, de 4 de noviembre de 2003  
Referencia: BOE-A-2003-20253

25. Red de comunicaciones electrónicas: los sistemas de transmisión y, cuando proceda, los equipos de conmutación o encaminamiento y demás recursos, incluidos los elementos que no son activos que permitan el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, redes terrestres fijas (de conmutación de circuitos y de paquetes, incluida Internet) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada.

26. Red pública de comunicaciones: una red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público y que soporta la transferencia de señales entre puntos de terminación de la red.

# Esquema Nacional de Seguretat (ENS)

## ■ Registre d'activitat

- Es registraran les activitats dels usuaris, retenint la informació necessària per monitoritzar, analitzar, investigar i documentar activitats indegudes o no autoritzades, permetent identificar a cada moment a la persona que actua.

# Esquema Nacional de Seguretat (ENS)

## ■ Incidents de seguretat

- S'establirà un sistema de detecció i reacció envers codi maliciós.
- Es registraran els incidents de seguretat que es produixin i les accions de tractament que se segueixin. Aquests registres s'utilitzaran per a la millora contínua del sistema.

# **Esquema Nacional de Seguretat (ENS)**

## **■ Continuïtat de l'activitat**

- Els sistemes disposaran de còpies de seguretat i establiran els mecanismes necessaris per a garantir la continuïtat de les operacions en cas de pèrdua dels mitjans habituals de treball.

## **■ Millora contínua**

- El procés integral de seguretat haurà de ser actualitzat i millorat de forma continuada.

# **Esquema Nacional de Seguretat (ENS)**

## **■ Notificacions i publicacions electròniques**

- Assegurar l'autenticitat de l'organisme que les publiqui.
- Assegurar la integritat de la informació publicada.
- Deixar constància de la data i hora de la posada a disposició de l'interessat i l'accés al seu contingut.
- Aplicar procediments de firma electrònica.

# **Esquema Nacional de Seguretat (ENS)**

## **■ Auditories de seguretat**

- Com a mínim cada dos anys, amb caràcter extraordinari si es fan modificacions substancials al sistema d'informació.
- Acompliment del ENS, identificar deficiències i suggerir possibles mesures correctores.

# Esquema Nacional de Seguretat (ENS)

## ■ Compliment de requisits mínims

- L'ENS dicta uns requisits mínims, que poden ser ampliats.
- Si un sistema tracta amb dades personals s'aplicarà l'indicat a la Llei Orgànica de Protecció de Dades en vigència.
- Cal tenir en compte la categoria del sistema.

# Esquema Nacional de Seguretat (ENS)

## Annex I

### 2. Dimensiones de la seguridad.

A fin de poder determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, y de poder establecer la categoría del sistema, se tendrán en cuenta las siguientes dimensiones de la seguridad, que serán identificadas por sus correspondientes iniciales en mayúsculas:

- a) Disponibilidad [D].
- b) Autenticidad [A].
- c) Integridad [I].
- d) Confidencialidad [C].
- e) Trazabilidad [T].

# Esquema Nacional de Seguretat (ENS)

## Annex I

4. Determinación de la categoría de un sistema de información.

1. Se definen tres categorías: BÁSICA, MEDIA y ALTA.

a) Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.

b) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior.

c) Un sistema de información será de categoría BÁSICA si ninguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

# Esquema Nacional de Seguretat (ENS)

## Annex I

c) Nivel ALTO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio muy grave:

1.<sup>º</sup> La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.

2.<sup>º</sup> El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.

3.<sup>º</sup> El incumplimiento grave de alguna ley o regulación.

4.<sup>º</sup> Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.

5.<sup>º</sup> Otros de naturaleza análoga.

# Esquema Nacional de Seguretat (ENS)

- Selecció de mesures de seguretat
  - **org**: marc organitzatiu
  - **op**: marc operacional
  - **mp**: mesures de protecció

## 4. Marco operacional [op]

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

# Esquema Nacional de Seguretat (ENS)

## ■ Selecció de mesures de seguretat

| Afectadas | Dimensiones |        |        | MEDIDAS DE SEGURIDAD |
|-----------|-------------|--------|--------|----------------------|
|           | B           | M      | A      |                      |
| categoria | aplica      | =      | =      | op.pl.3              |
| D         | n.a.        | aplica | =      | op.pl.4              |
| categoria | n.a.        | n.a.   | aplica | op.pl.5              |
|           |             |        |        | op.acc               |
| AT        | aplica      | =      | =      | op.acc.1             |
| ICAT      | aplica      | =      | =      | op.acc.2             |
| ICAT      | n.a.        | aplica | =      | op.acc.3             |
| ICAT      | aplica      | =      | =      | op.acc.4             |
| ICAT      | aplica      | +      | ++     | op.acc.5             |
| ICAT      | aplica      | +      | ++     | op.acc.6             |
| ICAT      | aplica      | +      | =      | op.acc.7             |

## 4.2 Control de acceso. [op.acc].

El control de acceso cubre el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pueda, o no, acceder a un recurso del sistema para realizar una determinada acción.

El control de acceso que se implante en un sistema real será un punto de equilibrio entre la comodidad de uso y la protección de la información. En sistemas de nivel Bajo, se primará la comodidad, mientras que en sistemas de nivel Alto se primará la protección.

En todo control de acceso se requerirá lo siguiente:

- a) Que todo acceso esté prohibido, salvo concesión expresa.
- b) Que la entidad quede identificada singularmente [op.acc.1].
- c) Que la utilización de los recursos esté protegida [op.acc.2].
- d) Que se definan para cada entidad los siguientes parámetros: a qué se necesita acceder, con qué derechos y bajo qué autorización [op.acc.4].
- e) Serán diferentes las personas que autorizan, usan y controlan el uso [op.acc.3].
- f) Que la identidad de la entidad quede suficientemente autenticada [mp.acc.5].
- g) Que se controle tanto el acceso local ([op.acc.6]) como el acceso remoto ([op.acc.7]).

Con el cumplimiento de todas las medidas indicadas se garantizará que nadie accederá a recursos sin autorización. Además, quedará registrado el uso del sistema ([op.exp.8]) para poder detectar y reaccionar a cualquier fallo accidental o deliberado.

Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, en los casos en que sea necesario, las medidas de seguridad locales se acompañarán de los correspondientes acuerdos de colaboración que delimiten mecanismos y procedimientos para la atribución y ejercicio efectivos de las responsabilidades de cada sistema ([op.ext]).

#### 4.2.5 Mecanismo de autenticación [op.acc.5].

| dimensiones | I C A T |       |      |
|-------------|---------|-------|------|
| nivel       | bajo    | medio | alto |
| aplica      | aplica  | +     | ++   |

Los mecanismos de autenticación frente al sistema se adecuarán al nivel del sistema atendiendo a las consideraciones que siguen.

Las guías CCN-STIC desarrollarán los mecanismos concretos adecuados a cada nivel.

##### Nivel BAJO

- a) Se admitirá el uso de cualquier mecanismo de autenticación: claves concertadas, o dispositivos físicos (en expresión inglesa »tokens») o componentes lógicos tales como certificados software u otros equivalentes o mecanismos biométricos.
- b) En el caso de usar contraseñas se aplicarán reglas básicas de calidad de las mismas.
- c) Se atenderá a la seguridad de los autenticadores de forma que:

- 1.º Los autenticadores se activarán una vez estén bajo el control efectivo del usuario.
- 2.º Los autenticadores estarán bajo el control exclusivo del usuario.
- 3.º El usuario reconocerá que los ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida.
- 4.º Los autenticadores se cambiarán con una periodicidad marcada por la política de la organización, atendiendo a la categoría del sistema al que se accede.
- 5.º Los autenticadores se retirarán y serán deshabilitados cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.

## Nivel MEDIO

- a) No se recomendará el uso de claves concertadas.
- b) Se recomendará el uso de otro tipo de mecanismos del tipo dispositivos físicos (tokens) o componentes lógicos tales como certificados software u otros equivalentes o biométricos.
- c) En el caso de usar contraseñas se aplicarán políticas rigurosas de calidad de la contraseña y renovación frecuente.

## Nivel ALTO

- a) Los autenticadores se suspenderán tras un periodo definido de no utilización.
- b) No se admitirá el uso de claves concertadas.
- c) Se exigirá el uso de dispositivos físicos (tokens) personalizados o biometría.
- d) En el caso de utilización de dispositivos físicos (tokens) se emplearán algoritmos acreditados por el Centro Criptológico Nacional.
- e) Se emplearán, preferentemente, productos certificados [op.pl.5].

*Tabla resumen de mecanismos de autenticación admisibles*

|                   |                    | Nivel |             |                |
|-------------------|--------------------|-------|-------------|----------------|
|                   |                    | BAJO  | MEDIO       | ALTO           |
| algo que se sabe  | claves concertadas | sí    | Con cautela | no             |
| algo que se tiene | Tokens             | si    | sí          | criptográficos |
| algo que se es    | Biometría          | sí    | sí          | + doble factor |

# Contingut

- Esquema Nacional de Seguretat
- **Estàndards de la PCI**
- Protecció de la privadesa

# Estàndards de la PCI

- **Payment Card Industry Data Security Standard**
  - Normes de seguretat de la indústria de les targes de pagament (PCI) es van desenvolupar per fomentar i millorar la seguretat de les **dades del titular de la targeta** i facilitar l'adopció de mesures de seguretat uniformes a nivell mundial.
  - Venedors, entitats emissores, proveïdors de servei... han de complir amb les PCI DSS.

Equips i xarxes que desen/processen informació.

- Creades a partir de les propostes de Visa, MasterCard, American Express, Discover i JCR



# Estàndards de la PCI

## ■ 6 objectius de control i 12 requisits

- 1. Desenvolupar i mantenir xarxes i dispositius segurs:
  - 1. Instal·lar i mantenir una configuració de tallafoc per protegir les dades del titular de la targeta.
  - 2. No usar els valors predeterminats subministrats pel proveïdor per a les contrasenyes del sistema i altres paràmetres de seguretat.
- 2. Protegir les dades del titular de la targeta:
  - 3. Protegir les dades del titular de la targeta que estiguin emmagatzemats.
  - 4. Xifrar la transmissió de les dades del titular de la targeta en les xarxes públiques obertes.

# Estàndards de la PCI

- **6 objectius de control i 12 requisits**
  - 3. Mantenir un programa d'administració de la vulnerabilitat:
    - 5. Protegir tots els sistemes contra malware i actualitzar els programes o software antivirus regularment.
    - 6. Desenvolupar i mantenir sistemes i aplicacions segurs.
  - 4. Implementar mesures sólides de control d'accés:
    - 7. Restringir l'accés a les dades del titular de la targeta segons la necessitat de saber que l'empresa tingui.
    - 8. Identificar i autentificar l'accés als components del sistema.
    - 9. Restringir l'accés físic a les dades del titular de la targeta.

# Estàndards de la PCI

- **6 objectius de control i 12 requisits**
  - 5. Supervisar i avaluar les xarxes amb regularitat:
    - 10. Rastrejar i supervisar tots els accessos als recursos de xarxa i a les dades del titular de la targeta.
    - 11. Provar periòdicament els sistemes i processos de seguretat.
  - 6. Mantenir una política de seguretat de la informació:
    - 12. Mantenir una política que abordi la seguretat de la informació per a tot el personal.

## Desarrolle y mantenga redes y sistemas seguros.

### Requisito 1: Instale y mantenga una configuración de *firewall* para proteger los datos del titular de la tarjeta

Los *firewalls* son dispositivos que controlan el tráfico computarizado entre las redes (internas) y las redes no confiables (externas) de una entidad, así como el tráfico de entrada y salida a áreas más sensibles dentro de las redes internas confidenciales de una entidad. El entorno de datos de los titulares de tarjetas es un ejemplo de un área más confidencial dentro de la red confiable de una entidad.

El *firewall* examina todo el tráfico de la red y bloquea las transmisiones que no cumplen con los criterios de seguridad especificados.

Todos los sistemas deben estar protegidos contra el acceso no autorizado desde redes no confiables, ya sea que ingresen al sistema a través de Internet como comercio electrónico, del acceso a Internet desde las computadoras de mesa de los empleados, del acceso al correo electrónico de los empleados, de conexiones dedicadas como conexiones entre negocios mediante redes inalámbricas o a través de otras fuentes. Con frecuencia, algunas vías de conexión hacia y desde redes no confiables aparentemente insignificantes pueden proporcionar un acceso sin protección a sistemas clave. Los *firewalls* son un mecanismo de protección esencial para cualquier red de computadoras.

Otros componentes del sistema pueden funcionar como *firewall*, siempre que reúnan los requisitos mínimos correspondientes a *firewalls*, según se especifica en el Requisito 1. En las áreas que se utilizan otros componentes del sistema dentro del entorno de datos de los titulares de tarjetas para proporcionar la funcionalidad de *firewall*, es necesario incluir estos dispositivos dentro del alcance y de la evaluación del Requisito 1.

| Requisitos de la PCI DSS  | Procedimientos de prueba   | Guía  |
|---|--|---|
| 1.1 Establezca e implemente normas de configuración para <i>firewalls</i> y routers que incluyan lo siguiente:                                    | 1.1 Inspeccione las normas de configuración de <i>firewalls</i> y routers y otros documentos especificados a continuación para verificar el cumplimiento e implementación de las normas.   | Los <i>firewalls</i> y los routers son componentes clave de la arquitectura que controla la entrada a y la salida de la red. Estos dispositivos son unidades de software o hardware que bloquean el acceso no deseado y administran el acceso autorizado hacia dentro y fuera de la red. Las normas y los procedimientos de configuración ayudarán a garantizar que la primera línea de defensa de la organización en la protección de sus datos mantenga su solidez. |
| 1.1.1 Un proceso formal para aprobar y probar todos los cambios y las conexiones de red en la configuración de los <i>firewalls</i> y los routers | 1.1.1.a Revise los procedimientos documentados para corroborar que existe un proceso formal para aprobar y probar lo siguiente: <ul style="list-style-type: none"><li>• Conexiones de red</li><li>• Cambios en las configuraciones de <i>firewalls</i> y routers</li></ul> | La implementación y la documentación de un proceso para aprobar y probar todas las conexiones y cambios de los <i>firewalls</i> y los routers ayudarán a prevenir problemas de seguridad causados por una configuración errónea de la red, del router o del <i>firewall</i> .   |

## **Requisito 2: No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad**

Las personas malintencionadas (externas e internas a una entidad), por lo general, utilizan las contraseñas predeterminadas por los proveedores y otros parámetros que el proveedor predetermine para comprometer los sistemas. Estas contraseñas y parámetros son conocidos entre las comunidades de hackers y se determinan fácilmente por medio de información pública.

| Requisitos de la PCI DSS   | Procedimientos de prueba  | Guía  |
|--|---|---|
| <p><b>2.1 Siempre cambie los valores predeterminados por el proveedor y elimine o deshabilite las cuentas predeterminadas innecesarias <b>antes</b> de instalar un sistema en la red.</b></p> <p>Esto rige para TODAS las contraseñas predeterminadas, por ejemplo, entre otras, las utilizadas por los sistemas operativos, los software que prestan servicios de seguridad, las cuentas de aplicaciones y sistemas, <i>los terminales de POS</i> (puntos de venta), las aplicación de pago, las cadenas comunitarias de SNMP (protocolo simple de administración de red), etc.</p> | <p><b>2.1.a</b> Escoja una muestra de los componentes del sistema e intente acceder a los dispositivos y aplicaciones (con la ayuda del administrador del sistema) con las cuentas y contraseñas predeterminadas por el proveedor y verifique que se hayan cambiado TODAS las contraseñas predeterminadas (incluso las de los sistemas operativos, los software que prestan servicios de seguridad, las cuentas de aplicaciones y sistemas, los terminales de POS [puntos de ventas], las cadenas comunitarias de SNMP [protocolo simple de administración de red]). (Utilice los manuales y las fuentes de los proveedores que se encuentran en Internet para encontrar las cuentas y las contraseñas proporcionadas por estos).</p> <p><b>2.1.b</b> Para la muestra de los componentes del sistema, verifique que todas las cuentas predeterminadas innecesarias (incluso las cuentas que usan los sistemas operativos, los software de seguridad, las aplicaciones, los sistemas, los terminales de POS [puntos de ventas], SNMP [protocolo simple de administración de red], etc.) se hayan eliminado o deshabilitado.</p> <p><b>2.1.c</b> Entreviste al personal, revise la documentación de respaldo y verifique lo siguiente:</p> <ul style="list-style-type: none"><li>• Se cambian todos los valores predeterminados por proveedores (incluidas las contraseñas predeterminadas de sistemas operativos, software que presta servicios de seguridad, cuentas de aplicaciones y sistemas, terminales de POS, cadenas de comunidad de protocolo simple de administración de red [SNMP], etc.) antes de instalar un sistema en la red.</li></ul> | <p>Las personas malintencionadas (externas e internas a la organización), por lo general, utilizan configuraciones predeterminadas por los proveedores, nombres de cuentas y contraseñas para poner en riesgo el software del sistema operativo, las aplicaciones y los sistemas donde están instalados. Debido a que estos parámetros predeterminados suelen publicarse y son conocidos en las comunidades de hackers, cambiar estas configuraciones contribuirá a que el sistema sea menos vulnerable a los ataques.</p> <p>Incluso si una cuenta predeterminada no se creó para usarse, cambiar la contraseña predeterminada por una contraseña única y sólida y, después, deshabilitar la cuenta, evitará que personas maliciosas vuelvan a habilitar la cuenta y accedan con la contraseña predeterminada.</p> |

| Requisitos de la PCI DSS   | Procedimientos de prueba   | Guía   |
|--|--|--|
| <p><b>3.2.3</b> Despues de la autorización, no almacene el PIN (número de identificación personal) ni el bloqueo de PIN cifrado.</p>   | <p><b>3.2.3</b> En el caso de la muestra de los componentes del sistema, revise las fuentes de datos, incluido, a modo de ejemplo, lo siguiente y verifique que los PIN y los bloques de PIN cifrados no se almacenen despues de la autorización:</p> <ul style="list-style-type: none"> <li>• Datos de transacciones entrantes</li> <li>• Todos los registros (por ejemplo, transacciones, historiales, depuración, error)</li> <li>• Archivos de historial</li> <li>• Archivos de seguimiento</li> <li>• Esquemas de bases de datos</li> <li>• Contenidos de bases de datos</li> </ul>   | <p>Sólo el propietario de la tarjeta o el banco emisor de la tarjeta deben conocer estos valores. Si se hurtan estos datos, personas malintencionadas pueden efectuar transacciones de débito basadas en PIN fraudulentas (por ejemplo, retiros de cajeros automáticos).</p>   |
| <p><b>3.3</b> Enmascare el PAN (número de cuenta principal) cuando aparezca (los primeros seis o los últimos cuatro dígitos es la cantidad máxima de dígitos que aparecerá), de modo que solo el personal con una necesidad comercial legítima pueda ver más que los primeros seis o los últimos cuatro dígitos del PAN.</p> <p><b>Nota:</b> Este requisito no reemplaza los requisitos más estrictos implementados para la presentación de los datos del titular de la tarjeta (por ejemplo, requisitos legales o de las marcas de las tarjetas de pago para los recibos de POS [puntos de venta]).</p> | <p><b>3.3.a</b> Revise las políticas y los procedimientos escritos para ocultar las vistas de PAN (número de cuenta principal) para verificar lo siguiente:</p> <ul style="list-style-type: none"> <li>• Se documenta una lista de las funciones que necesitan acceso a más que los primeros seis o los últimos cuatro dígitos (incluye el PAN completo), junto con la necesidad empresarial legítima que justifique dicho acceso.</li> <li>• Se debe ocultar el PAN cuando aparezca para que solo el personal con una necesidad comercial legítima pueda ver más que los primeros seis y los últimos cuatro dígitos del PAN.</li> <li>• Todas las demás funciones que no estén específicamente autorizadas para ver PAN completos solo deben ver PAN ocultos.</li> </ul> <p><b>3.3.b</b> Revise las configuraciones del sistema y verifique que las vistas del PAN (número de cuenta principal) estén disponibles solo para aquellos usuarios/funciones que tengan una necesidad comercial legítima y que el PAN (número de cuenta principal) esté oculto para el resto de las solicitudes.</p> | <p>La presentación de un PAN completo en pantallas de computadoras, recibos de tarjetas de pago, faxes o informes impresos puede facilitar la obtención y uso fraudulento de estos datos por parte de personas malintencionadas. Asegurarse de que solo aquellas personas que tengan una necesidad comercial legítima puedan ver el PAN (número de cuenta principal) completo minimiza el riesgo de que personas no autorizadas tengan acceso a los datos del PAN (número de cuenta principal).</p> <p>El enfoque de ocultamiento siempre deberá garantizar que solo se muestre el número mínimo de dígitos necesario para realizar una función comercial específica. Por ejemplo, si solo se necesitan los últimos cuatro dígitos para realizar una función comercial, enmascare el PAN para que las personas que realizan esa función solo puedan ver los últimos cuatro dígitos. A manera</p> |

# Estàndards de la PCI

- **Vídeo resum**

<https://www.youtube.com/watch?v=szVmMxWORBc>

- **Problemes?**

- Les empreses emissores de targes poden multar o impedir que es continuïn usant els productes.
- Cal recordar que les dades d'una targeta són protegides per la LOPD...

# Estàndards de la PCI

## ■ PA-DSS (Payment Application)

- De forma similar, la PCI té uns requeriments per als desenvolupadors d'aplicacions que usin dades de targes bancàries:
  - No retenir totes les dades (per exemple, incloent PIN)
  - Protegir les dades
  - Mecanismes d'autentificació
  - Registre de les activitats de pagament
  - Les dades no s'han de desar en un servidor connectat a Internet
  - etc.

# Contingut

- Esquema Nacional de Seguretat
- Estàndards de la PCI
- **Protecció de la privadesa**

# Protecció de la privadesa

- Protecció de dades personals
  - Abans de maig 2018
    - **Directiva 95/46/CE** transposada a LODP 15/1999 i el reglament 1720/2007
    - S'hi definien dades especialment sensibles, amb nivells de protecció bàsic, mitjà, alt. S'hi definien actors com ara el responsable, l'encarregat i el cap de seguretat. S'implanta l'**Agència de Protecció de Dades**, i també l'**Autoritat de Protecció de Dades**. Les persones tenen els drets **ARCO** (accés, rectificació, cancel·lació i oposició).

# Protecció de la privadesa

- A partir de maig 2018
  - **Reglament 2016/679** del Parlament Europeu i del Consell, 27 d'abril de 2016.
  - **Llei Orgànica 3/2018**, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD)

# Protecció de la privadesa

- Actors
  - **Responsable del tractament de dades.** Persona física o jurídica que decideix sobre el tractament de les dades, que se'n farà, si es conservaran, etc.
  - **Encarregat del tractament.** Persona física o jurídica que tracta les dades personals per compte del responsable del tractament.
  - **Responsable de seguretat, delegat de protecció de dades.**

# Protecció de la privadesa

- Actors
  - **Responsable del tractament de dades**
    - Haurà de fer una avaluació de l'impacte (Privacy Impact Assessment), que ve a ser una anàlisi de riscos sobre el sistema d'informació que desarà les dades personals.
  - **Delegat de protecció de dades**
    - Podrà ser intern o extern, persona física o jurídica. És obligatori per a
      - empreses públiques
      - tractament de dades a gran escala
      - empreses de més de 250 treballadors

Informa i assessorà al responsable, supervisa el compliment, coopera amb autoritats de control.

# Protecció de la privadesa

- Es demana una **responsabilitat proactiva** en el sentit que són les organitzacions qui tenen l'obligació de complir amb els principis, garanties i drets establerts.
- La privacitat serà per defecte i per disseny (*privacy by design*).
  - Adoptar mesures tècniques i organitzatives per aplicar de forma efectiva els principis de protecció de dades.
  - Només s'han de tractar aquelles dades que siguin necessàries segons la finalitat del tractament.
- S'ha de controlar l'accés a les dades.
- Cal vetllar pel termini de conservació de les dades.
- Transparència a l'hora de donar informació, senzillesa.

# Protecció de la privadesa

- GSuite, Google Cloud

<https://cloud.google.com/security/gdpr/>

- Un debat interessant...

Gsuite vs. eines gratuïtes respecte LOPDGDD

<https://ayudaleyprotecciondatos.es/2018/02/12/rgpd-google-g-suite/>

# Protecció de la privadesa

## ■ General Data Protection Regulation (2016)

L 119/48

EN

Official Journal of the European Union

4.5.2016

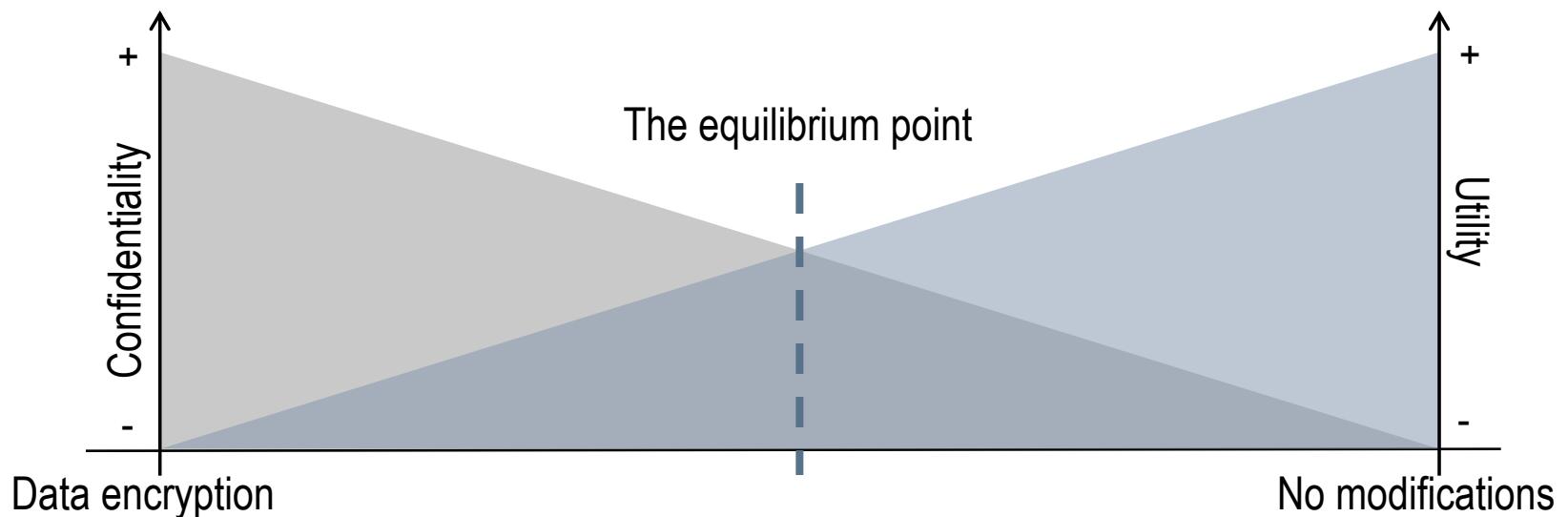
### *Article 25*

#### **Data protection by design and by default**

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

# Protecció de la privadesa

- Protegir les dades...
  - Cal protegir les dades, però aquestes han de ser útils. Si les dades es desen xifrades, els servidors no poden fer càlculs, a no ser que les sàpiguen desxifrar...



# Protecció de la privadesa

## ■ RGPD i pseudonimització

'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

# Protecció de la privadesa

- RGPD i pseudonimització

Pseud.  
↓

| Row | Name       | SS Num.     | City      | Job     | AIDS |
|-----|------------|-------------|-----------|---------|------|
| 1   | H. Simpson | 123-45-6789 | Barcelona | Baker   | NO   |
| 2   | R. Smith   | 987-65-4321 | Reus      | Plumber | NO   |
| 3   | M. Stephen | 124-35-1111 | El Rouell | Doctor  | YES  |
| 4   | D. Garcia  | 133-35-2829 | Reus      | Farmer  | NO   |
| 5   | M. Ngu     | 424-25-6272 | Barcelona | Teacher | NO   |
| 6   | F. Torra   | 924-95-3839 | Reus      | Teacher | YES  |
| ... | ...        | ...         | ...       | ...     | ...  |

# Protecció de la privadesa

## ■ RGPD i pseudonimització

Remove      Pseud.      Remove      Categorise

| Row | Name       | SS Num.     | City      | Job     | AIDS |
|-----|------------|-------------|-----------|---------|------|
| 1   | H. Simpson | 123-45-6789 | Barcelona | Baker   | NO   |
| 2   | R. Smith   | 987-65-4321 | Reus      | Plumber | NO   |
| 3   | M. Stephen | 124-35-1111 | El Rouell | Doctor  | YES  |
| 4   | D. Garcia  | 133-35-2829 | Reus      | Farmer  | NO   |
| 5   | M. Ngu     | 424-25-6272 | Barcelona | Teacher | NO   |
| 6   | F. Torra   | 924-95-3839 | Reus      | Teacher | YES  |
| ... | ...        | ...         | ...       | ...     | ...  |

# Protecció de la privadesa

- RGPD i pseudonimització

|  | Name       |  | City     | Job     | AIDS |
|--|------------|--|----------|---------|------|
|  | da8767asda |  | Big city | Baker   | NO   |
|  | s87d97a9   |  | City     | Plumber | NO   |
|  | cc898cd98  |  | Hamlet   | Doctor  | YES  |
|  | dada787a   |  | City     | Farmer  | NO   |
|  | j7dj9d0s   |  | Big city | Teacher | NO   |
|  | 8djdu8dj   |  | City     | Teacher | YES  |
|  | ...        |  | ...      | ...     | ...  |

# Protecció de la privadesa

ayudaleyprotecciondatos.es

The screenshot shows the homepage of the website. At the top, there is a dark blue header bar with the logo 'AYUDA LEY PROTECCIÓN DATOS' on the left. To the right of the logo are several navigation links: 'LOPDGDD PARA EMPRESAS', 'CIUDADANOS', 'BLOG DE PROTECCIÓN DE DATOS', and a search icon. Below the header, a large white text area contains the heading 'Sección de recursos gratuitos para cumplir la LOPDGDD'.



# Protecció de la privadesa

## LOS DERECHOS QUE TIENES PARA PROTEGER TUS DATOS PERSONALES

EL 25 DE MAYO DE 2018 SE APLICA EL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS Y ES IMPORTANTE QUE CONOZCAS CUÁLES SON TUS DERECHOS

1

### DERECHO A CONOCER

#### \* PARA QUÉ UTILIZAN TUS DATOS

- Quién los tiene
- Para qué los tienen
- A quién los pueden ceder
- Quiénes son sus destinatarios

#### \* EL PLAZO DE CONSERVACIÓN DE TUS DATOS o Hasta cuándo van a ser utilizados

#### \* QUE PUEDES PRESENTAR UNA RECLAMACIÓN ANTE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

#### \* LA EXISTENCIA DE DECISIONES AUTOMATIZADAS, LA ELABORACIÓN DE PERFILES Y SUS CONSECUENCIAS



2

### DERECHO A SOLICITAR AL RESPONSABLE

#### \* LA SUSPENSIÓN DEL TRATAMIENTO DE TUS DATOS

- Si impugnamos la exactitud de los datos, mientras se verifica dicha exactitud por parte del responsable
- Si hemos ejercitado nuestro derecho de oposición al tratamiento de datos, mientras se verifica si los motivos legítimos del responsable prevalecen sobre tus derechos

#### \* LA CONSERVACIÓN DE TUS DATOS

- Si el tratamiento es ilícito y nos oponemos a la supresión de los datos solicitando la limitación de su uso
- Si los datos se necesitan para la formulación, ejercicio o defensa de reclamaciones

#### \* LA PORTABILIDAD DE TUS DATOS A OTROS PROVEEDORES DE SERVICIOS

- En un formato estructurado, de uso común y lectura mecánica, siempre que sea técnicamente posible para su portabilidad y cuando los hayan utilizado/tratado con tu consentimiento o por existir un contrato

3

### DERECHO A RECTIFICAR TUS DATOS

#### \* CUANDO SEAN INEXACTOS

#### \* CUANDO ESTÉN INCOMPLETOS



4

### DERECHO A SUPRIMIR TUS DATOS

#### \* POR TRATAMIENTO ILÍCITO DE DATOS

- POR LA DESAPARICIÓN DE LA FINALIDAD QUE MOTIVÓ EL TRATAMIENTO O RECOPILADA
- CUANDO REVOCAS TU CONSENTIMIENTO
- CUANDO TE OPONES A QUE SE TRATEN



5

### DERECHO DE OPOSICIÓN AL TRATAMIENTO DE TUS DATOS

#### \* POR MOTIVOS PERSONALES SALVO QUE QUIEN TRATA TUS DATOS ACREDITE UN INTERÉS LEGÍTIMO

#### \* CUANDO EL TRATAMIENTO TENGA POR OBJETO EL MARKETING DIRECTO



# Protecció de la privadesa



## Autoritat Catalana de Protecció de Dades

Inici

Autoritat

Drets i obligacions

Documentació

Actualitat

Contacte

Seu electrònica

[Inici](#) > [Documentació](#) > [Guies bàsiques de protecció de ...](#) > Guies APDCAT



### ≡ Guies APDCAT

Pautes de protecció de dades per als centres educatius

Pautes centres educatius: preguntes freqüents

Guia sobre l'avaluació d'impacte relativa a la protecció de dades al RGPD (2.0)

Guia sobre l'encarregat del tractament al RGPD

Guia per al compliment del deure d'informar al RGPD