

Resposta a les preguntes formulades pel grup socialdemòcrata en referència a l'anunci que la pàgina web de la CASS ha permès l'accés lliure a dades confidencials

Índex

1. Dades exposades en el període crític
2. Dates crítiques
3. Nombre de consultes i usuaris afectats
4. Estudi de confidencialitat de les dades
5. Protocols de seguretat
6. Causa de la incidència
7. Responsabilitats

Dades exposades en el període crític

Quines dades personals teòricament protegides han estat exposades a la pàgina web de la CASS sense necessitat d'identificació per mot de pas?

Cal ressenyar que les dades únicament eren accessibles amb **codi d'usuari correcte** i **introduint alguna mena de contrasenya** i sota les condicions següents:

The image displays two side-by-side screenshots of the CASS user login interface, titled 'Assegurats'. Both screens show the same form with the following text: 'Si ets un assegurat (assalariat, treballador per compte propi, pensionista o indirecte) de la CASS, introdueix el teu usuari (6 números i la lletra) i clau:'. The 'Nom d'usuari' field contains '1234567X' and the 'Ex:' field shows '123456A'. The 'Contrasenya' field is highlighted with a red oval in the left screenshot and a green oval in the right screenshot. Below the password field is the text 'No recordes la teva clau?' and a button labeled 'ACCÉS USUARIS'. At the bottom, there is a section 'Assegurat, aquí podràs:' with a list of options: 'Consultar i modificar les teves dades', 'Consultar últims pagaments', and 'Consultar els teus punts de vellesa', followed by the text 'i gestionar tot el que tingui a veure amb la teva informació com a assegurat.' In the left screenshot, a red arrow points from the text 'Permetia accés' to the password field. In the right screenshot, a green arrow points from the text 'NO permetia accés' to the password field.

Permetia l'accés amb : **NO** permetia l'accés :

- **Usuari i contrasenya correcta** - Sense usuari


- **Usuari i contrasenya incorrecta** - Sense usuari i contrasenya

- **Amb usuari i contrasenya en blanc**

Cal destacar que el procés d'autenticació de l'usuari consta de dues parts:

- el número d'usuari, compostat amb 6 díigits i una lletra calculada mitjançant un algoritme matemàtic
- una contrasenya que cal informar, subjecte a unes regles definides (lletres i números, amb una longitud mínima de 8 díigits)

Respecte els entorns de tramitació del portal, la incidència **no ha afectat els tràmits efectuats amb certificat digital**; prestadors de salut, empreses i patrons domèstics.



Empreses, prestadors i patrons domèstics

Si ets **empresari, prestador o patró domèstic** de la CASS, accedeix amb certificat digital:

➔ **Accedir amb certificat digital**

Sol·licita un certificat digital:

- = **A la Cass**
- = **Tinc un certificat de Firma Professional**


Entorn NO afectat

Aquí podràs:

- = Fer la declaració de cotitzacions
- = Donar d'alta i baixa empleats

Si ets prestador podràs:

- = Tramitar remeses i fulls de prestacions
- = Baixar les llistes de metges ordenants



powerd by VeriSign

Acerca de los certificados SSL

Dades que han estat exposades durant el període crític

Tràmits de l'assegurat/ada directe/a

Dades de l'assegurat/ada directe/a

[Fitxa de l'assegurat/ada directe/a](#)

[Consulta últims pagaments](#)

Desplaçaments

[Volant de desplaçament](#)

[Volant assistència sanitària col·legial](#)

Punts de vellesa

[Extracte de punts de vellesa](#)

Volants de desplaçament a Espanya i França

Dins del formulari de desplaçament, es poden visualitzar el **codi i nom dels assegurats indirectes de l'afiliat** consultat.

En aquest cas, es pot considerar que **no hi ha dades sensibles** en aquest tràmit.

Volants d'assistència sanitària col·legial

Dins del formulari d'assistència sanitària col·legial, **no es visualitza cap dada** de l'afiliat. Aquest formulari es presenta buit de dades i cal complimentar-lo per tal de generar el volant.

En aquest cas, es pot considerar que **no hi ha cap dada sensible** en aquest tràmit.

Extractes de punts

Dins del formulari de l'extracte de punts, es pot visualitzar l'**empresa** on treballa l'afiliat i el seu **salari**.

En aquest cas, considerem que **hi ha dades sensibles** en el tràmit.

Cal recordar que l'accés a les dades d'un afiliat, durant el període crític de la incidència, només ha estat possible amb la correcta introducció del codi d'usuari i un caràcter com a mínim a la contrasenya.



Número i Nom de l'assegurat:

Data d'afiliació: Data naixement: Sexe:

Data Inici Extracte: Data Fi Extracte: TOTAL PUNTS ACUMULATS ...

| PERÍODE | DECLARANT | RÈGIM | CL. | BASE IMPONIBLE | % COT. ASSEG. | VALOR COMPRA PUNTS | PUNTS PAGATS |
|---------|-------------|-------|-----|----------------|---------------|--------------------|--------------|
| | On treballa | | | Salari | | | |

Pagaments de prestacions sanitàries

En el formulari de pagaments de prestacions es pot visualitzar el moviment (capçalera) i detall del moviment (detall de la prestació).

En la capçalera, el **nom de prestador** es pot considerar **dada sensible**.

En el detall de la prestació, el **nom de prestador** i la **descripció de l'acte** es poden considerar també, **dades sensibles**.

Cal destacar que la descripció dels actes, en el cas de la **farmàcia NO suposa la visualització del detall dels medicaments**.

Consulta últims pagaments
Complimentar formulari
* Dades obligatòries:

Data inici: 01/06/2013 Exi: 03/04/2007
Data fi: 18/07/2013 Exi: 25/04/2007

Tipus de moviment: Prestacions
 Aturs
 Pensions

Consultar

Moviments

| Data | Nom prestador | Núm. document | Núm. de tiquet | Import tiquet | Data remesa | Import | Data pagament | Núm. p |
|------|---------------|---------------|----------------|---------------|-------------|--------|---------------|--------|
| | Prestador | | | | | | | |

Veure detall moviment

| Descripció | Import pagat | Import reemborsat | Data de l'acte | Nom prestador | Motiu |
|----------------------|--------------|-------------------|----------------|---------------|-------|
| Descripció de l'acte | | | | Prestador | |

Cal recordar que l'accés a les dades d'un afiliat, durant el període crític de la incidència, només ha estat possible amb la correcta introducció del codi d'usuari i un caràcter com a mínim a la contrasenya.

Pagaments d'aturs de treball

En aquest cas, l'**import del pagament** es pot considerar **dada sensible**, ja que a partir d'aquesta dada es podria **deduir el salari**.

D'altra banda, la **durada de la malaltia** podria arribar a ser una **dada sensible**, en cas que fos una **malaltia de llarga durada**.

Consulta últims pagaments [Imprimir](#)
Complimentar formulari
* Dades obligatòries:

Data inici*: 01/08/2012 Ex: 03/04/2007
Data fi*: 15/07/2013 Ex: 25/04/2007

Tipus de moviment*: Prestacions
 Altres
 Pensions

Moviments

| Inici Període | Fi període | Núm. document | Data inici atur | Import | Data pagament | Núm. pagament |
|---------------------------------------------|------------|---------------|-----------------|--------|---------------|---------------|
| No s'han trobat dades per aquesta consulta. | | | | | | |

Durada de la malaltia (circles around 'Fi període' and 'Data inici atur')
Import del pagament (circles around 'Import' and 'Data pagament')

Cal recordar que l'accés a les dades d'un afiliat, durant el període crític de la incidència, només ha estat possible amb la correcta introducció del codi

Moviments pensions


En aquest formulari, l'**import del pagament** es pot considerar **dada sensible**, però a partir d'aquesta dada seria difícil fer una estimació de la trajectòria professional en base a la pensió.

D'altra banda el **tipus de pensió** podria arribar a ser una **dada sensible**, en el cas de pensions d'invalidesa.

Cal recordar que l'accés a les dades d'un afiliat, durant el període crític de la incidència, només ha estat possible amb la correcta introducció del codi d'usuari i un caràcter com a mínim a la contrasenya.

Consulta últims pagaments

Complimentar formulari

 [Imprimir](#)

* Dades obligatòries:

Data inici*:  Ex: 03/04/2007

Data fi*:  Ex: 25/04/2007


Tipus de moviment*: Prestacions

Aturs

Pensions

Moviments

| Tipus | Inici Període | Fi període | Núm. document | Data obertura | Import | Data pagament | Núm. pagament |
|---------------------------------------------|---------------|------------|---------------|---------------|--------|---------------|---------------|
| No s'han trobat dades per aquesta consulta. | | | | | | | |

 **Tipus de pensió**

 **Import del pagament**

Fitxa d'afiliat

La fitxa de l'afiliat està formada pels blocs d'informació següents:

- Dades de l'assegurat
- Dades personals
- Dades de contacte
- Història laboral
- Relacions últim assegurat directe i relacions dels assegurats indirectes
- Dades bancàries

Dades de l'assegurat/ada directe/a:

Núm. d'assegurat/ada directe/a:

Cúmul de punts:

Data d'alta:

Dades personals:

Nom i cognoms:

Sexe:

Data de naixement:

Nacionalitat:

Passaport / DNI:

Estat civil:

Dades de contacte:

Adreça:

 [Modificar dades](#)

Telèfon fix:

Telèfon mòbil:

Fax:

Correu electrònic:

Història laboral:

Règim:

Classe de vellesa:

| Núm. Empresa | Nom | Data d'alta | Data de baixa |
|--------------|-----|-------------|---------------|
|--------------|-----|-------------|---------------|

Última relació com a assegurat/ada indirecte/a:

Assegurat/ada directe/a:

Tipus d'assegurat/ada indirecte/a:

Data d'alta:

Data de baixa:

Assegurats/ades indirectes de l'assegurat/ada directe/a:**Dades bancàries:**

Entitat:

Núm. compte:

País:

 [Modificar dades](#)

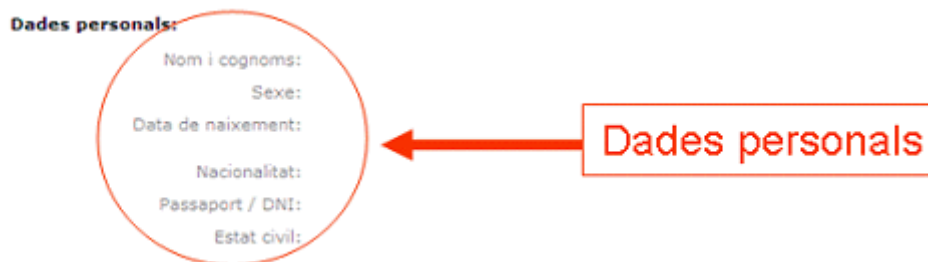
En el bloc **Dades de l'assegurat:**

El **Cúmulo de punts** es pot considerar **dada sensible**, però a partir d'aquesta dada seria difícil fer una estimació de la trajectòria professional en base al total de punts acumulats.



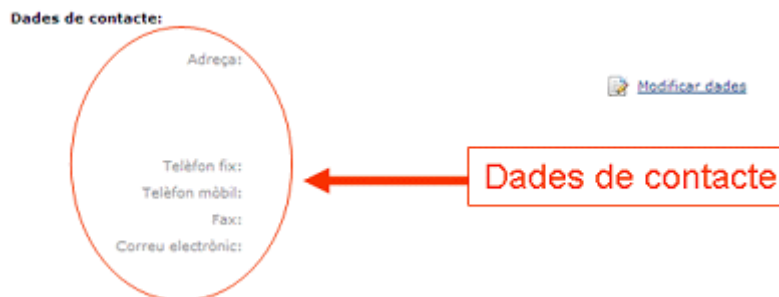
En el bloc **Dades personals:**

La **Data de naixement** es pot considerar **dada sensible**.



En el bloc **Dades de contacte:**

L'**Adreça** es pot considerar **dada sensible**.



En el bloc **Història laboral:**

El **Nom de l'empresa** es pot considerar **dada sensible**.

| Règim: | | Classe de vellesa: | | | |
|---------------------|-----|--------------------|---------------|--|--|
| Núm. Empresa | Nom | Data d'alta | Data de baixa | | |
| Vida laboral | | | | | |

En el bloc **Relacions últim assegurat directe i relacions dels assegurats indirectes;**

En aquest bloc, es pot considerar que **no hi ha cap dada sensible**.



En el bloc **Dades bancàries**:

El **Número de compte** es pot considerar **dada sensible**.



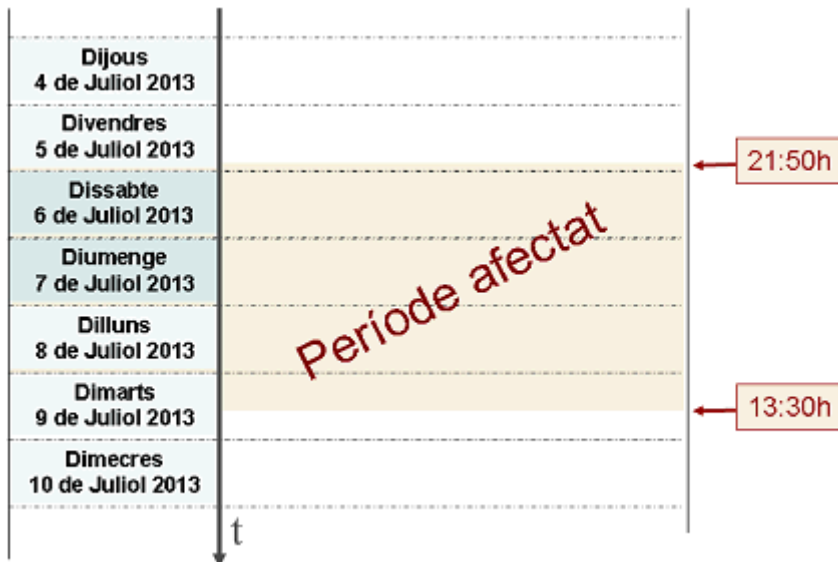
Cal recordar que l'accés a les dades d'un afiliat, durant el període crític de la incidència, només ha estat possible amb la correcta introducció del codi d'usuari i un caràcter com a mínim a la contrasenya.

Per últim cal destacar que la incidència produïda arran de la migració del portal:

- no ha afectat els tràmits efectuats amb certificat digital, que són els efectuats per prestadors de salut, per empreses i per patrons domèstics.
- no ha deixat exposades les dades relatives a l'estat de salut dels assegurats a una indeguda visualització.

2 Dates crítiques

Durant quan de temps han estat exposades les dades anteriorment mencionades i quines van ser les dates en que les dades van estar exposades?



Període de temps que han estat exposades les dades **3 dies i 15:40h**

Divendres 5 de Juliol a les 21h50 Posada en producció Portal Web

De Dissabte 6 a Dilluns 8 de Juliol Període crític d'exposició de dades

Dimarts 9 de Juliol a les 13h30 Detecció de la incidència

Dimarts 9 de Juliol a les 14h00 **Resolució de la incidència**

i restabliment del servei

3 Nombre de consultes i usuaris afectats

Quantes consultes a aquestes dades s'ha produït? Quants usuaris han tingut accés a aquestes dades?

El nombre d'usuaris que tenen accés al portal és de **11.012 afiliats**

El col·lectiu afectat és únicament de **159 usuaris diferents**, entre ells, assalariats, treballadors per compte propi, pensionistes i indirectes, amb els codis d'usuari d'aquests assegurats s'ha accedit al portal per fer modificacions de les seves dades o simplement per consultar-les.

S'ha procedit a estudiar els accessos, classificant-los segons el tipus següents:

- de Modificació
- de Consulta

Accessos de Modificació

Han estat **8 persones** que han modificat les seves dades durant el període crític, procedint a fer els següents canvis;

- 4 modificacions d'adreça

- 5 modificacions de correu electrònic o telèfon
- 3 modificacions de dades bancàries de l'assegurat

Nota: Les modificacions realitzades no mostren irregularitats, són **perfils molt heterogenis i no es detecta cap tipus de patró intrusiu.**

Accessos de Consulta

Han estat consultades les dades de **151 usuaris** durant el període crític, procedint a fer les consultes següents:

- 75 volants de desplaçament a Espanya i França
- 12 volants d'assistència sanitària col·legial
- 89 consultes extractes de punts
- 83 consultes relatives als pagaments de prestacions sanitàries
- 41 consultes relatives a pagaments d'aturs de treball
- 19 consultes moviments pensions
- 58 consultes de fitxa d'afiliat

El balanç és de **377 consultes** en total, fetes des del codi de **151 usuaris**.

Nota: Les consultes realitzades no mostren irregularitats, i són totalment **previsibles per les dates en que s'efectuen. Tampoc es detecta cap tipus de patró intrusiu.**

4 Estudi de confidencialitat de les dades

Pot assegurar la CASS que no s'ha produït un robatori de dades confidencials a causa d'aquesta situació a la seva pàgina web?

Amb els **afiliats que han procedit a modificar les seves dades**, s'ha dut a terme una trucada telefònica, **que ha permès de comprovar que han estat ells qui han efectuat els canvis.**

Resultat de les trucades realitzades als afiliats que han modificat dades

Ja que la CASS no disposa de la possibilitat de poder gravar les converses telefòniques hem demanat la col·laboració d'Andorra Telecom per fer efectiu l'enregistrament de les trucades.

El divendres 12 de juliol es va procedir a les oficines d'Andorra Telecom a les 8 trucades que calia realitzar amb les dades telefòniques de què disposa la CASS.

Obtenint els resultats següents:

- **5 trucades** han confirmat que han estat ells qui han modificat les dades
- **1 trucada** havia de confirmar amb el seu espòs si ell havia modificat les seves dades

El dimarts 23 s'ha contactat amb l'afiliada que ha confirmat la modificació de les dades.

- **2 trucades** no localitzades

S'ha enviat una carta certificada per correu ordinari per tal de ratificar la modificació de les dades. D'un afiliat es confirma la modificació de dades i queda pendent de recepció la carta de l'altra afiliat.

La única modificació pendent de confirmar correspon a un canvi d'adreça d'un assegurat.

Patrons d'accés en les Consultes

Procedim a fer un anàlisi més detallat de les consultes efectuades corresponents a 151 afiliats:

- Als **75 volants de desplaçament** han accedit **57 afiliats diferents**. S'han fet 72 peticions de volant per vacances a Espanya i 3 per França.

Els tràmits mostren un patró familiar de consulta.

- Als tràmits associats als **12 volants d'assistència sanitària col·legial** han estat efectuats per **10 afiliats diferents**. Tampoc presenta cap patró intrusiu, ja que aquest tràmit està associat a persones que estan esperant aquest volant per poder rebre la prestació sanitària.

- **68 afiliats diferents** han realitzat **89 demandes d'extractes de punts**. La gran majoria d'afiliats han efectuat un sol tràmit. Detectem que, quan un mateix usuari ha efectuat més d'una consulta, pot està relacionat amb la dificultat per visualitzar el pdf.

- **36 afiliats** han accedit a les **83 consultes relatives als pagaments de prestacions sanitàries**. Vist el context econòmic actual, sembla evident que els afiliats han efectuat aquestes consultes per comprovar si la CASS ha fet efectiu el pagament.

- **13 afiliats** han fet les **41 consultes relatives a pagaments d'aturs**. Com en el cas anterior, i vist el context econòmic actual, sembla evident que els afiliats han efectuat aquestes consultes per comprovar si la CASS ha fet efectiu el pagament.

- **12 afiliats** han efectuat les **19 consultes a moviments de pensions**. Sembla evident, al ser primers de mes, que els afiliats han efectuat aquestes consultes per comprovar si la CASS ha fet efectiu el pagament.

- **45 afiliats** han efectuat les **58 consultes de fitxa d'afiliat**. Es tracta d'una relació casi 1 a 1, per tant no podem pressuposar cap patró fraudulent.

Adreces Internet (IP) utilitzades

Els tràmits realitzats s'han efectuat, accedint-hi des de 136 Adreces Internet (IP) diferents, destacant el següent:

- Des de cap IP s'han fet tràmits per més de 3 afiliats diferents
- Des de 3 Ip's s'han efectuat tràmits per a 3 afiliats diferents
- Des de 26 Ip's s'han efectuat tràmits per a 2 afiliats diferents
- Des de 107 Ip's s'han efectuat tràmits per a un únic afiliat
- Cap persona ha fet tràmits des de més de 2 Ip's diferents

- S'han fet tràmits de 10 afiliats des de 2 Ip's diferents.

En definitiva, dels 151 usuaris, 68 han efectuat volants de desplaçament o d'assistència sanitària col·legial.

Dels 83 afiliats restants, on consta que s'han fet altres tipus de consultes, s'ha observat que:

- Des de 1 IP s'ha efectuat tràmits per a 3 afiliats diferents.
- Des de 8 Ip's s'han efectuat tràmits per a 2 afiliats diferents: en aquests casos els 2 afiliats que han estat consultats en la mateixa IP tenen o bé una relació familiar entre ells, comparteixen adreça o consten com treballadors de la mateixa empresa.
- Des de 66 Ip's s'han efectuat tràmits per a un únic afiliat.

Podem concloure, que en base als tràmits realitzats i els accessos per les Adreces Internet (IP), que **les dades consultades no mostren irregularitats, no delectant-se patrons intrusius.**

5 Protocols de seguretat

Quina garantia pot oferir la CASS als seus afiliats que les persones que han accedit a les seves dades confidencials no en poden fer un ús malintencionat?

No s'ha detectat cap accés fraudulent, en tot cas amb els protocols de seguretat establerts podria determinar-se la procedència dels accessos fraudulents.

En el cas de detectar qualsevol ús mal intencionat de les dades, en tot moment, la CASS pot determinar, amb l'ajuda d'ANDORRA TELECOM, la procedència dels accessos fraudulents.

Arribant fins el detall de:

nom de la persona que ha fet el ús fraudulent
domicili i telèfon
adreça de correu electrònic
dades accedides

Per tal de garantir als nostres afiliats l'accés i confidencialitat de la informació, disposem dels protocols de seguiment i control següents:

Seguiment i control dels tràmits del Portal Web

A partir del protocol de traçabilitat establert, **es pot establir la procedència, origen i detall de totes les dades dels tràmits** efectuats al portal web.

· Entorn portal WEB

Disposa de dos tipus d'accés que permeten retrobar el seguiment del detall i adreces (IP) de les transaccions realitzades en el portal web.

Una transacció s'efectua a l'entrada del servidor web (Apache) on es pot fer el seguiment de la petició d'entrada al portal.

L'altra transacció s'efectua en el gestor de continguts (Liferay) on es pot fer el seguiment de la petició del tràmit.

- Entorn I/series de IBM

Les dades dels afiliats estan ubicades a l'entorn d'explotació I/series de IBM.

Les consultes o modificacions dels tràmits des del portal web s'enregistren en uns fitxers d'auditoria de l'ordinador d'explotació on es pot determinar el tipus d'operació (tràmits) i la modificació efectuada. Sempre guardant el registre d'abans i després.

Enregistrament dels canvis realitzats pels usuaris

A partir del protocol de traçabilitat establert, **es poden enregistrar tots els canvis realitzats per tots els usuaris** que han accedit a les dades de l'ordinador central I/Series de IBM.

- Entorn I/series de IBM

Totes les modificacions que efectuen els usuaris externs i interns de la CASS, a petició dels afiliats, són enregistrades i guardades en un fitxer d'auditoria. Sempre guardant el registre d'abans i després de la modificació.

En aquest fitxer d'auditoria consta:

§ nom de conversa

§ nom de l'arxiu modificat

§ data de l'acció

§ hora de l'acció

§ número d'afiliat

§ usuari que ha efectuat l'acció

§ tipus d'acció

§ registre abans

§ registre després

Seguiment i control de dades sensibles

La CASS per preservar la confidencialitat, i fer un **seguiment i control exhaustiu de les dades sensibles de major incidència** dels seus afiliats, disposa dels programaris **QJRN/400 i CONTROLLER**, que compleixen els reglaments internacionals SOX, HIPAA, BALE II, PCI, 21-CFR. **Garantint així la seguretat i integritat de les dades.**

Aquest programari permet marcar els camps en els fitxers que són més sensibles i guardar totes les consultes i modificacions que s'han efectuat amb aquestes dades.

A més controla el accessos intrusius (adreces IP) i possibles còpies de dades que es puguin efectuar.

6 Causa de la incidència

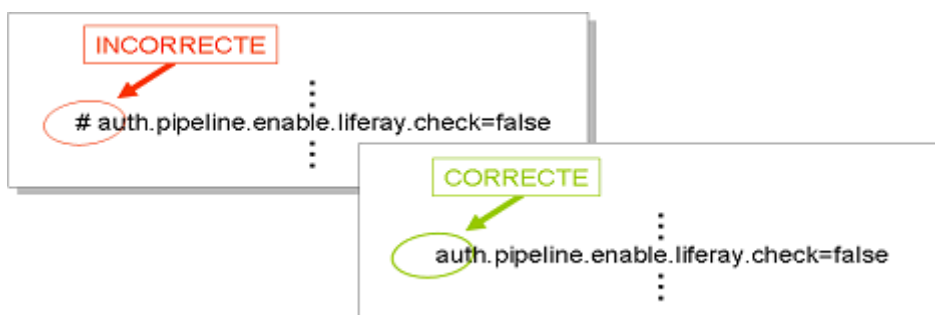
Quina ha estat la causa que ha permès la possibilitat d'accedir a les dades personals protegides sense necessitat de mot de pas?

Cal ressenyar que les dades únicament eren accessibles amb codi d'usuari correcte i introduint alguna mena de contrasenya.

Durant el procés de migració, l'empresa LEM va procedir a restaurar els paràmetres i adreces (URL) per poder posar el portal en producció. **Aquest va ser l'error que va produir la incidència.**

Després d'analitzar el codi dels programes, es determinà que **la causa de la incidència era conseqüència de la incorrecta restauració dels paràmetres, efectuada per l'empresa LEM S.L.** després de l'execució del procés de migració dels continguts.

El fitxer `/opt/liferay6/jboss-ports02/deploy/ROOT.war/WEB/classes/ext-portal.properties` a la línia 87 tenia el següent paràmetre mal configurat.



Aquest paràmetre és el que permet comprovar la validesa de la contrasenya de cada codi d'usuari, **al posar el coixinet davant la validació**, aquesta no s'executa i **la línia de codi es tracta com un comentari**.

El Protocol de la CASS no ha permès detectar aquest incident concret, s'han efectuat verificacions i validacions a pre-producció, però no s'ha efectuat una verificació i validació a producció.

7 Responsabilitats

Està govern disposat a exigir responsabilitats als responsables d'aquesta greu situació?

El Consell d'Administració de la CASS, com a òrgan competent en un afer que afecta la entitat, ha actuat de la manera següent:

- 1) Amb l'objectiu de vetllar pel bon funcionament del portal web, es va acordar en primer lloc que s'estabilitzés el procés de migració amb l'empresa LEM.
- 2) Posteriorment s'ha contractat una empresa que assegurí el manteniment correctiu i evolutiu del portal fins al desembre de 2013.
- 3) El 31 de juliol s'ha notificat a l'empresa LEM la voluntat de la CASS de resoldre el contracte de serveis de referència, suspentent l'accés als sistemes informàtics de la CASS.
- 4) S'ha advertit a la Directora General que es prenguin les mesures escaients perquè un fet com aquest no es pugui reproduir.
- 5) S'ha qualificat com a falta greu del Director de Sistemes d'informació, les mancances en el protocol establert, essent la sanció imposada de suspensió de feina i sou de 7 dies.
- 6) S'ha qualificat com a falta lleu del cap de l'àrea de Sistemes d'informació i del tècnic informàtic que tenien encomanades tasques de supervisió, essent la sanció imposada la d'una amonestació escrita.