Consorci Català pel Desenvolupament Local

Carrer València 231, 6a
08007 Barcelona
Tel. 93 496 16 16
ccdl@ccdl.cat

www.acm.cat

Annex núm. 03. LOTS 18 a 41
Sobre B

PROPOSICIÓ TÈCNICA

El/la senyor/a ..RAMON ANFRUNS BARDOLET. com ....Administrador únic... de l'empresa IP DATA SOLUTIONS BCN, SL, sota la seva responsabilitat, com a licitador/a de l'Acord marc de subministrament d'equips informàtics i de serveis associats amb destinació a les entitats locals de Catalunya (Exp. núm. 2024.01), declara que la proposta que presenta per el Lot **34**, compleix els requisits obligatoris del Plec de Prescripcions Tècniques (PPT) i normativa legal vigent

Recordem que:

*Les empreses hauran d'aportar aquest **Annex núm. 03** degudament complimentat i acompanyat de la següent documentació:*

- ***Memòria** relativa als criteris subjectes a un judici de valor*

I, perquè consti, signa aquesta declaració responsable.

(Lloc, data i signatura electrònica)

33946325G RAMON ANFRUNS (R: B64295587)

Firmado digitalmente por 33946325G RAMON ANFRUNS (R: B64295587)
Fecha: 2025.05.29 08:59:07 +02'00'

Consorci Català pel Desenvolupament Local

Carrer València 231, 6a
08007 Barcelona
Tel. 93 496 16 16
ccdl@ccdl.cat

www.acm.cat

- ***Memòria** relativa als criteris subjectes a un judici de valor*

LOT 34. SERVEIS DE CIBERSEGURETAT

Proposta de Coordinació amb l'Entitat Local Contractant

1. Objectiu i Principis Globals

Aquesta proposta estableix un **model de comunicació i coordinació** per a qualsevol entitat local adherida a l'Acord marc de serveis de ciberseguretat. L'objectiu és garantir transparència, rapidesa de resposta i traçabilitat durant tota la prestació (auditoria, consultoria, pla de millora i formació). El plantejament se sustenta en tres pilars:

1. **Canals** : correu electrònic com a via principal; telèfon per a urgències; registre de tot al sistema de tiquets a *Techservice*.
2. **Reunions estructurades i flexibles**: kick-off, seguiment periòdic, sessions extraordinàries i tancament.
3. **Procés de gestió d'incidències independent de la monitorització**: registre, priorització, resolució i lliçons apreses.

Aquest marc és **genèric** però adaptable a volum, perfil i maduresa tecnològica de cada ens local.

2. Canals de Comunicació i Responsabilitats

Canal	Ús	SLA de resposta	Responsable
Correu electrònic (suport@ipdata.es)	Consultes, informes, incidències menors	8x5xNBD	Equip Tècnic/RP
Telèfon directe (+34 93 272 12 41)	Incidències crítiques, coordinació immediata	8x5xNBD	Equip Tècnic/RP
Techservice	Creació i seguiment de tiquets	8x5xNBD	Equip tècnic/ RP

El **RP** és el punt únic de contacte amb l'entitat local; canalitza consultes, escalats i informes. Tot correu o trucada deriva en un tiquet a *Techservice* per assegurar **traçabilitat i mètrica**.

'* 8x5xNBD. Mateix dia o següent dia laborable.

Carrer València 231, 6a
08007 Barcelona
Tel. 93 496 16 16
ccdl@ccdl.cat

www.acm.cat

3. Calendari de Reunions Proposat

Fase	Quan	Format	Objectius principals
Reunió inicial (kick-off)	Primers 15 dies	Online / presencial	Presentar equips, definir abast, acordar SLA i protocols, validar calendari
Reunions de seguiment	Mensuals*	Online (40-60 min)	Revisar KPIs, estat d'accions, incidències obertes, pròximes fites
Sessions extraordinàries	Quan calgui	Online / telèfon	Tractar emergències, canvis importants o decisions urgents
Reunió de tancament	Fi del projecte/període	Online / presencial	Presentar resultats finals, lliçons apreses i recomanacions

* Freqüència adaptable (quinzenal en fases intensives; trimestral en manteniment).

4. Procés de Gestió d'Incidències (Techservice)

1. **Detecció**: per monitoratge automàtic o avís del client.
2. **Registre**: creació de tiquet amb severitat (Alta, Mitjana, Baixa) i descripció.
3. **Resposta**: diagnosi inicial dins SLA (Segons contractat).
4. **Resolució**: aplicació de mesures correctives; actualització contínua al tiquet.
5. **Tancament**: informe de causa arrel + recomanacions; confirmació del client.
6. **Revisió post-incident**: lliçons apreses i ajust del pla de millora si escau.

Escalats a N2/N3 o a tercers (p. ex. CERT-CAT) es documenten al mateix tiquet.

Prestació 172. Serveis d'assessoria

Auditoria i consultoria inicial

Objectiu de l'auditoria

- Identificar vulnerabilitats i riscos en els sistemes i la infraestructura TIC
- Avaluar la postura de seguretat actual
- Proposar mesures de mitigació o millora

Metodologia

1. Planificació i definició de l'abast

- Identificar els actius crítics (xarxes, servidors, firewalls, aplicacions...)
- Establir els límits de l'auditoria (on-prem, cloud, remot, físic...)
- Acordar amb l'equip tècnic i direcció les metodologies que s'utilitzaran
- Signar NDA o autoritzacions legals

2. Recollida d'informació (Reconnaissance)
   - Escaneig de xarxa (IP actives, ports oberts, serveis exposats)
   - Topologia de la xarxa i fluxos de dades
   - Versions de sistemes operatius i aplicacions
   - Identificació de dispositius obsolets o sense suport

3. Anàlisi de vulnerabilitats
   - Ús d'eines automàtiques
   - Identificació de CVEs coneguts
   - Avaluació de configuracions insegures, ports oberts innecessàriament, credencials per defecte
   - Revisió de *patch management*

4. Explotació controlada (opcional, si és un pentest)
   - Validació de vulnerabilitats crítiques de manera ètica i controlada
   - Tests d'accés no autoritzat, escalat de privilegis, evadir controls

5. Avaluació de riscos
   - Classificació de les vulnerabilitats per impacte i probabilitat
   - Mapatge amb referències com CVSS, NIST 800-30, ISO 27005
   - Anàlisi de riscos tècnics i de negoci

6. Informe i recomanacions
   - Resum executiu : riscos crítics, impacte, roadmap.
   - Detall tècnic : llistat de vulnerabilitats i accions concretes
   - Recomanacions de millora: configuració, actualitzacions, controls d'accés, segmentació, etc.

Bones pràctiques complementàries
- Revisar logs, polítiques de backup, i controls d'accés
- Avaluar la segmentació de xarxa i el control del trànsit
- Comprovar el desplegament de mesures com antivirus, EDR, i MFA
- Incloure sistemes cloud i serveis exposats a internet

Referències metodològiques
- OWASP Testing Guide (per apps web)
- NIST SP 800-115 – *Technical Guide to Information Security Testing*
- OSSTMM – *Open Source Security Testing Methodology Manual*
- ISO/IEC 27001 A.12.6.1 – Control de vulnerabilitats tècniques

Pla de Millora
Disseny del full de ruta (Roadmap)
Organitzar les accions en fases:

1. *Quick-Wins* (0-3 mesos)
   - Patching urgent, reforçar accés remot, MFA, desactivar serveis innecessaris.

2. *Millores prioritàries* (3-9 mesos)

   - Substitució d'elements crítics (firewalls antics, sistemes sense suport)
   - Implantació de SIEM o monitoratge avançat
   - Implantació d'eines i processos per al compliment de l'ENS
   - Revisió de polítiques de backup i resposta a incidents

3. *Evolució estratègica* (9-24 mesos)
   - Migració a arquitectures Zero Trust
   - Integració amb entorns cloud segurs
   - Automatització de seguretat i detecció d'amenaces tipus XDR

Recomanacions de millora (hardware + software)

Maquinari
- Substituir switches o firewalls obsolets sense suport del fabricant a nivell de seguretat i recanvi de hardware
- Consolidació de servidors amb virtualització
- Deploy de sensors de xarxa o sondes NDR
- Incorporació d'elements redundants (alta disponibilitat)

Programari

- Implantació o actualització d'EDR/XDR
- Integració de SIEM amb correcció automatitzada
- Implementació de gestors de vulnerabilitats i inventari
- Enfortiment de gestió d'identitats (IAM, SSO, PAM)
- Revisió i millora de polítiques de GPO i configuració segura

Governança i seguiment
- Establir indicadors de seguretat (KPIs)
- Crear un pla de revisió periòdica del full de ruta (cada 6 o 12 mesos)
- Alinear amb compliance (NIS2, ISO, ENS, etc.)
- Assignar responsables per accions concretes

És important destacar que segons la topologia, dimensions i actius de l'Ens públic es posarà més o menys focus en un dels apartats esmentats, i no necessariament en aquest ordre.

Per tal de poder elaborar un pla d'acció i assegurar el compliment del ENS, NIS2 i altres normatives, és imprescindible realizar un GAP Análisi. Aquest GAP Análisi ens dirà on està actualment l'entitat (Ens públic) i què li resta per arribar a complir amb la normativa requerida.

Respecte la metadologia per assegurar el compliment de l'ENS, NIS2 i altres normatives és imprescindible:

1. Conèixer l'estat actual de l'empresa
2. Identificar els processos i la cultura corporativa
3. Identificar les prioritats de l'empresa
4. Preparació del Projecte
5. Planificació i estimació inicial del calendari
6. Obtenció de la informació
7. Realització de l'anàlisi de maduresa
8. Presentació GAP anàlisi

Per a realizar aquest GAP Anàlisi es tenen un parell de reunions online amb el client on se li demana informació, i una segona reunió per presentar proposta del GAP Anàlisi, sempre que tota la informació hagi sigut suficient.

Prestació 173. Serveis de formació en ciberseguretat

Introducció.

IP DATA proposa la solució SafeUser per la prestació 173 "Servei de formació en ciberseguretat".

SafeUser és una iniciativa orientada a augmentar el nivell de seguretat dels sistemes informàtics d'empreses, administracions públiques i tota mena d'organitzacions, mitjançant l'entrenament de les persones usuàries de tecnologies de la informació que formen les plantilles respectives.

El curs SafeUser està destinat a ser altament efectiu per a usuaris no tècnics a empreses i organitzacions. Els participants aprenen a identificar els tipus d'amenaces més freqüents i practiquen hàbits de protecció efectius.

La solució de formació en ciberseguretat SafeUser és utilitzada per diverses entitats d'administracions públiques a Catalunya amb un alt grau d'efectivitat i satisfacció dels clients i usuaris.

Llistat de continguts.

Tots els continguts de SafeUser són disponibles en Català.

1. Emails maliciosos: Phishing
2. QR phishing (Quishing)
3. Emails maliciosos: Ransomware
4. Ús segur de xarxes socials
5. Smishing
6. Protecció de dades
7. Enginyeria social
8. Protecció de dades
9. Ciberdelictes financers
10. Ciberseguretat a la feina remota
11. Contrasenyes segures
12. Fitxers al núvol
13. Doble factor d'autenticació
14. Dispositius de memòria USB
15. Navegació i dominis a Internet
16. **Esquema Nacional de Seguretat**
17. Connexions wifi públiques
18. **NIS-2**
19. Ús segur de telèfons mòbils / mòbils
20. **Gestió de cibercrisi**

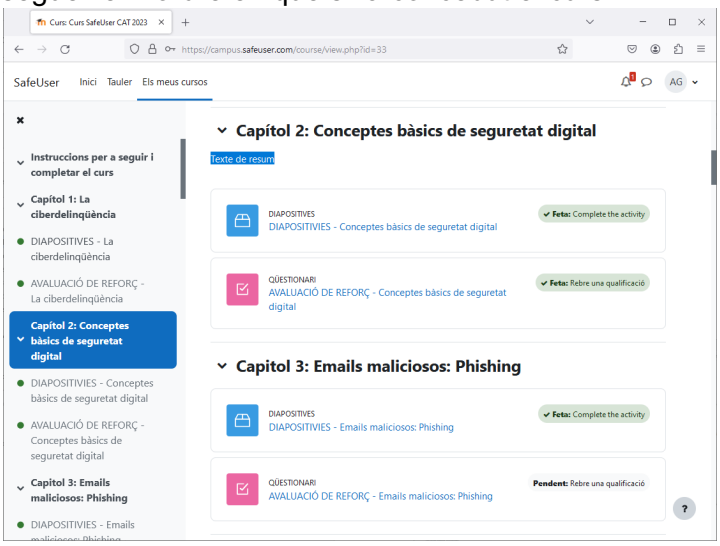
Consorci Català pel Desenvolupament Local

Carrer València 231, 6a
08007 Barcelona
Tel. 93 496 16 16
ccdl@ccdl.cat

www.acm.cat

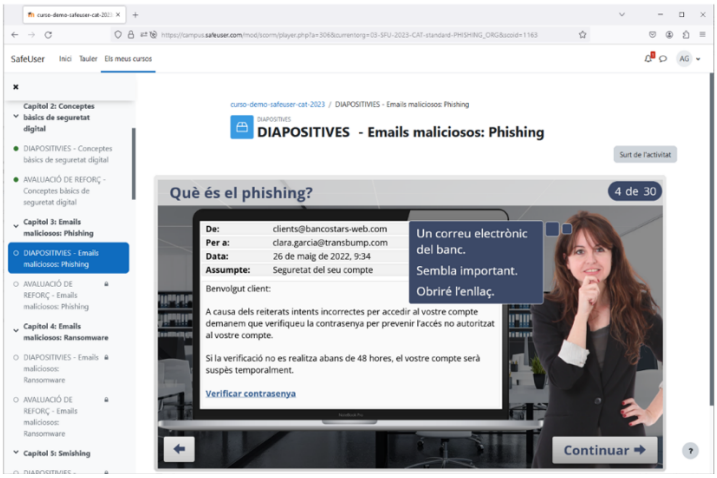
Estructura de continguts.

Cada capítol es composa de dos elements:
Diapositives interactives: entre 20 i 30 diapositives interactives per capítol (uns 15 minuts de temps d'aprenentatge).
Qüestionari: 5 preguntes d'opció múltiple orientades a estimular l'aprenentatge.
El curs està configurat de manera que és obligatori seguir l'ordre en què es presenten les diapositives i els qüestionaris. És a dir, cada activitat s'activa quan s'ha acabat l'anterior. D'aquesta manera no és possible saltar cap capítol i els participants segueixen l'ordre en què s'ha concebut el curs.



Diapositives: exemples de casos ficticis.

Les diapositives incorporen molts exemples d'amenaces de ciberseguretat. Aquests exemples es mostren en forma de casos ficticis amb base real, situacions contextualitzades i personatges.



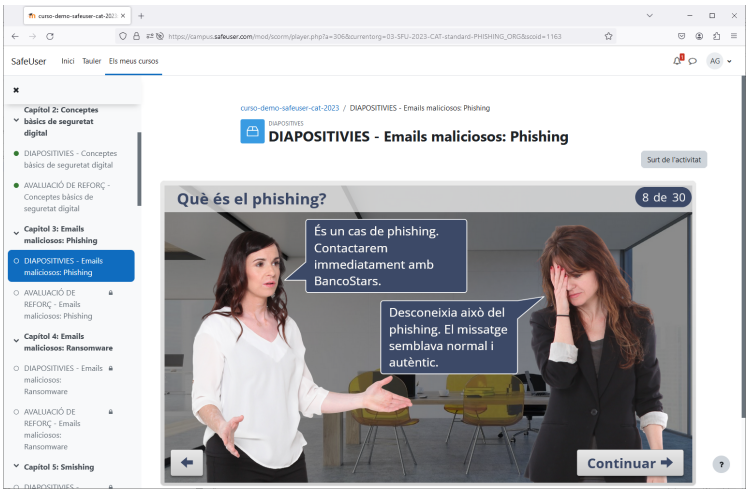
Consorci Català pel Desenvolupament Local

Carrer València 231, 6a
08007 Barcelona
Tel. 93 496 16 16
ccdl@ccdl.cat

www.acm.cat

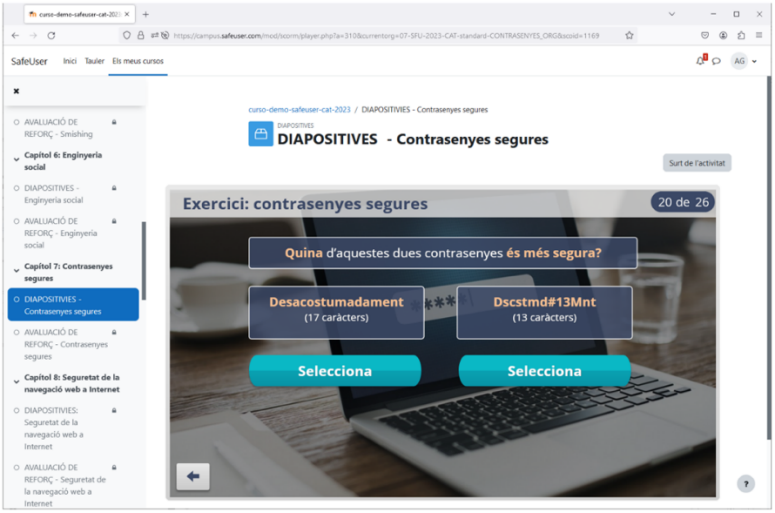
Diapositives: diàlegs entre personatges.

Les diapositives també inclouen diàlegs entre persones expertes i usuaris no tècnics. Hi ha una gran varietat de personatges per garantir l'equilibri de gènere. Per exemple, la figura del expert s'alterna entre una dona i un home entre els capítols al 50%.



Diapositives: activitats i exercicis.

Les diapositives també incorporen nombroses activitats i exercicis pràctics en què les persones participants han de prendre decisions com a part de la seva preparació. Segons les ciències de l'educació, està demostrat que la participació activa incrementa l'efectivitat de l'aprenentatge.



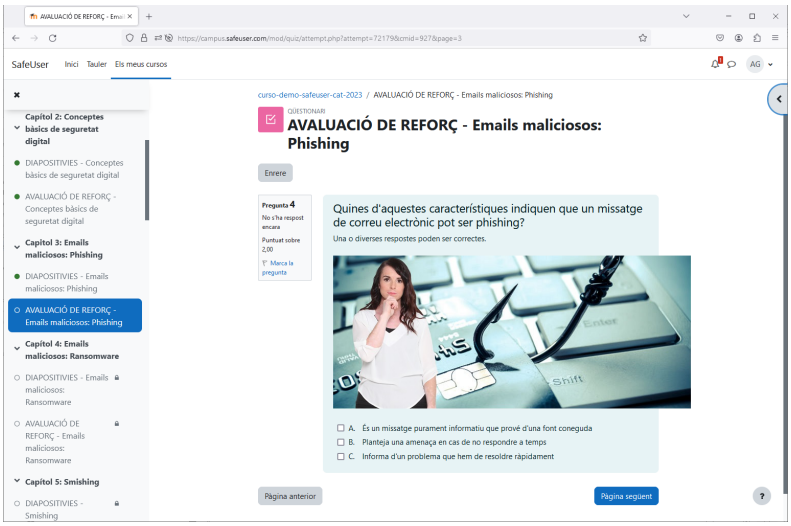
Consorci Català pel Desenvolupament Local

Carrer València 231, 6a
08007 Barcelona
Tel. 93 496 16 16
ccdl@ccdl.cat

www.acm.cat

Qüestionaris amb preguntes de resposta múltiple.

Els qüestionaris de cada capítol presenten cinc preguntes de resposta múltiple. Les preguntes obliguen a reflexionar sobre la matèria d'aprenentatge gràcies al fet que més d'una resposta pot ser correcta.
La configuració de sèrie permet fins a tres intents que mai no presenten exactament les mateixes preguntes pel fet que cada capítol disposa d'un banc de preguntes amb 15 preguntes de mitjana. Aquestes configuracions es poden modificar en funció de les necessitats i els criteris de cada client.



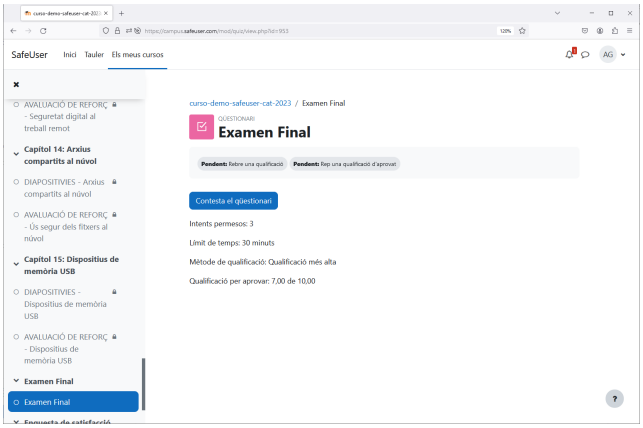
Examen Final.

Un cop finalitzats els capítols, s'activa l'Examen final. En la configuració estàndard, l'examen final consta de 20 preguntes amb un temps límit de 30 minuts.
Aquestes 20 preguntes es prenen de forma aleatòria entre les 150 preguntes del curs. Per tant, cada participant tindrà un examen totalment diferent de la resta de participants. Gràcies al fet que l'ordre de les respostes també és aleatori, és pràcticament impossible que uns participants ajudin la resta del grup a superar l'examen. El resultat aprovatori està fixat en un 70% d'encert. Tots aquests paràmetres es poden configurar segons els criteris de cada client.

Consorci Català pel Desenvolupament Local

Carrer València 231, 6a
08007 Barcelona
Tel. 93 496 16 16
ccdl@ccdl.cat

www.acm.cat

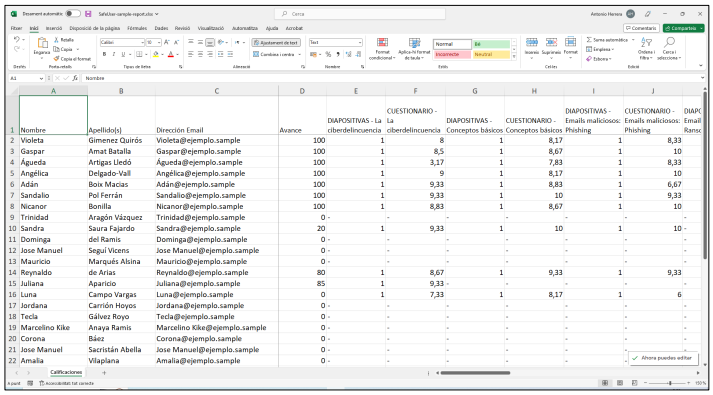


Enquesta i certificat de superació del curs.

Un cop superat l'examen final, s'activa l'enquesta de satisfacció. Després d'emplenar l'enquesta, es genera automàticament el certificat de superació del curs.

Informes d'activitat.

La plataforma permet consultar per pantalla i exportar a l'Excel o CSV els informes d'activitat de cada participant al curs. D'aquesta manera es pot disposar en qualsevol moment de la informació relativa al seguiment del curs, tant del col·lectiu com de cada persona a nivell individual.



Nombre	Apellido(s)	Dirección Email	Avance	DIAPOSITIVAS - La ciberdelincuencia	CUESTIONARIO - La ciberdelincuencia	DIAPOSITIVAS - Conceptos básicos	CUESTIONARIO - Conceptos básicos	DIAPOSITIVAS - Emails maliciosos: Phishing	CUESTIONARIO - Emails maliciosos: Phishing	DIAPOSITIVAS - Emails maliciosos: Ransomware
Violeta	Gimenez Quirós	Violeta@ejemplo.sample	100	1	8	1	8,17	1	8,33	
Gaspar	Amat Batalla	Gaspar@ejemplo.sample	100	1	8,5	1	8,67	1	10	
Águeda	Artigas Lledó	Águeda@ejemplo.sample	100	1	3,17	1	7,83	1	8,33	
Angélica	Delgado-Vall	Angélica@ejemplo.sample	100	1	9	1	8,17	1	10	
Adán	Boix Macías	Adán@ejemplo.sample	100	1	9,33	1	8,83	1	6,67	
Sandalio	Pol Ferrán	Sandalio@ejemplo.sample	100	1	9,33	1	10	1	9,33	
Nicanor	Bonilla	Nicanor@ejemplo.sample	100	1	8,83	1	8,67	1	10	
Trinidad	Aragón Vázquez	Trinidad@ejemplo.sample	0	-	-	-	-	-	-	
Sandra	Saura Fajardo	Sandra@ejemplo.sample	20	1	9,33	1	10	1	10	
Dominga	del Ramis	Dominga@ejemplo.sample	0	-	-	-	-	-	-	
Jose Manuel	Seguí Vicens	Jose Manuel@ejemplo.sample	0	-	-	-	-	-	-	
Mauricio	Marqués Alsina	Mauricio@ejemplo.sample	0	-	-	-	-	-	-	
Reynaldo	de Arias	Reynaldo@ejemplo.sample	80	1	8,67	1	9,33	1	9,33	
Juliana	Aparicio	Juliana@ejemplo.sample	85	1	9,33	-	-	-	-	
Luna	Campo Vargas	Luna@ejemplo.sample	0	1	7,33	1	8,17	1	6	
Jordana	Carrión Hoyos	Jordana@ejemplo.sample	0	-	-	-	-	-	-	
Tecla	Gálvez Royo	Tecla@ejemplo.sample	0	-	-	-	-	-	-	
Marcelino Kike	Anaya Ramis	Marcelino Kike@ejemplo.sample	0	-	-	-	-	-	-	
Corona	Báez	Corona@ejemplo.sample	0	-	-	-	-	-	-	
Jose Manuel	Sacristán Abella	Jose Manuel@ejemplo.sample	0	-	-	-	-	-	-	
Amalia	Vilaplana	Amalia@ejemplo.sample	0	-	-	-	-	-	-	

Consorci Català pel Desenvolupament Local

Carrer València 231, 6a
08007 Barcelona
Tel. 93 496 16 16
ccdl@ccdl.cat

www.acm.cat

Plataforma d'aprenentatge en línia.

Els continguts es posen a disposició dels clients mitjançat la plataforma d'aprenentatge en línia de SafeUser, basada en la tecnologia Moodle. Aquesta tecnologia de codi obert ofereix un conjunt de característiques de funcionalitat, efectivitat i seguretat molt adients pel servei de formació en ciberseguretat.

La plataforma és multi idioma incloent el Català, Castellà, entre d'altres.

La plataforma SafeUser és altament escalable i pot donar servei a colectius de milers d'usuaris totals i cents d'usuaris concurrents.

Els servidors es troben a la Unió Europea en compliment de les lleis de protecció de dades personals.

La combinació de la plataforma i els continguts de SafeUser permeten una total traçabilitat i control del procés d'aprenentatge.

Tutorització dels cursos.

IP DATA inclou processos de tutorització dels cursos com a part del servei de formació de ciberseguretat.