abast

BUILDING YOUR FUTURE IT

Acord marc de subministrament d'equips informàtics i de serveis associats amb destinació a les entitats locals de Catalunya (Expedient núm. 2024.01)

Lots 34 a 41 - Serveis de ciberseguretat

Memòria tècnica

Consorci Català pel Desenvolupament Local

Contingut

1.1 Objectius

L'objectiu del present document és la descripció dels serveis de ciberseguretat per a l'homologació de les següents prestacions:

- Prestació 172. Servei d'assessoria en ciberseguretat.
- Prestació 173. Servei de formació general en ciberseguretat.

Així, a continuació es descriu com des d'Abast podem col·laborar en la prestació dels serveis que ajudin als organismes homologats a l'ACM en el seu procés de transformació digital, tenint en compte el pilar de la ciberseguretat.

1.2 Seguiment del projecte

Per tal d'establir una definició correcta i basada en les millors pràctiques ITIL dels processos de relació requerits per a la gestió del servei, es detallen, en primer lloc, els nivells funcionals i s'identifiquen els objectius i les funcions per nivell. L'avantatge d'aquesta definició serà la clarificació de rols i responsabilitats, cercant un model flexible i que aporti valor als objectius del client i seguiment del projecte, garantint una millora contínua.

Resulta necessari establir, a més a més, uns Òrgans de Gestió (Comitès) que realitzin les funcions descrites, motiu pel qual s'ha identificat, per aquest projecte, la necessitat de comptar amb tres Comitès permanents i un equip de treball de durada limitada.

És clau dotar el model de relació dels mecanismes que assegurin la bona relació entre els equips de treball, ja que la qualitat dels serveis, depèn, en gran mesura de la bona comunicació.

Comitè	**Responsabilitat**
Comitè Executiu	El Comitè Executiu vetllarà per validar i aprovar les fites marcades en les diferents bases de projecte. En la fase 1 es realitzarà una reunió a l'inici del projecte i una en finalitzar la fase per la presentació dels resultats. En situacions de risc i bloqueig serà convocat el Comitè Executiu per determinar les decisions correctes que permetin mitigar els riscos i desencallar situacions de bloqueig per tal de donar continuïtat a les diferents etapes del projecte i garantir-ne l'èxit.
Comitè Tàctic	Aquest Comitè s'ha de coordinar sempre que hi hagin riscos o bloquejos que requereixin decisions correctes per evitar-los i/o desbloquejar l'operació del servei. Es celebrarà un Comitè Tàctic entre els membres de l'equip del Client i Abast mensualment per garantir l'èxit del projecte. Els membres del Comitè Tàctic estaran coordinats amb l'equip operatiu intern setmanalment per revisar el seguiment del projecte.

Comitè Operatiu	Es celebrarà el Comitè Operatiu setmanal per fer el seguiment i revisió de l'avenç de les fites del projecte i propers passos.

El servei es prestarà majoritàriament de forma remota, deixant l'opció presencial per determinades reunions com poden ser: arrencada, aprovació dels lliuraments, situacions de risc i bloqueig i quan es planifiquin reunions per a la conscienciació i sensibilització.

S'establirà com a entorn de col·laboració un repositori documental pels entregables parcials i finals del projecte.

Addicionalment, hi haurà una comunicació àgil a través del correu electrònic i la plataforma de comunicació remota.

1.3 Servei d'assessoria en ciberseguretat

L'avenç del servei contempla una comprovació exhaustiva dels sistemes d'informació, amb l'objectiu d'identificar vulnerabilitats que podrien permetre la penetració no autoritzada d'agents maliciosos, així com l'anàlisi posterior i la proposta d'accions de mitigació sobre la base dels resultats d'aquest.

L'objectiu és proporcionar al client una proposta de serveis professionals per a la realització de proves de penetració internes i externes:

- Execució de les proves de penetració tant externes com internes.
- Presentació de resultats.
- Recomanacions per la mitigació de les vulnerabilitats identificades.

1.3.1 Metodologia de treball

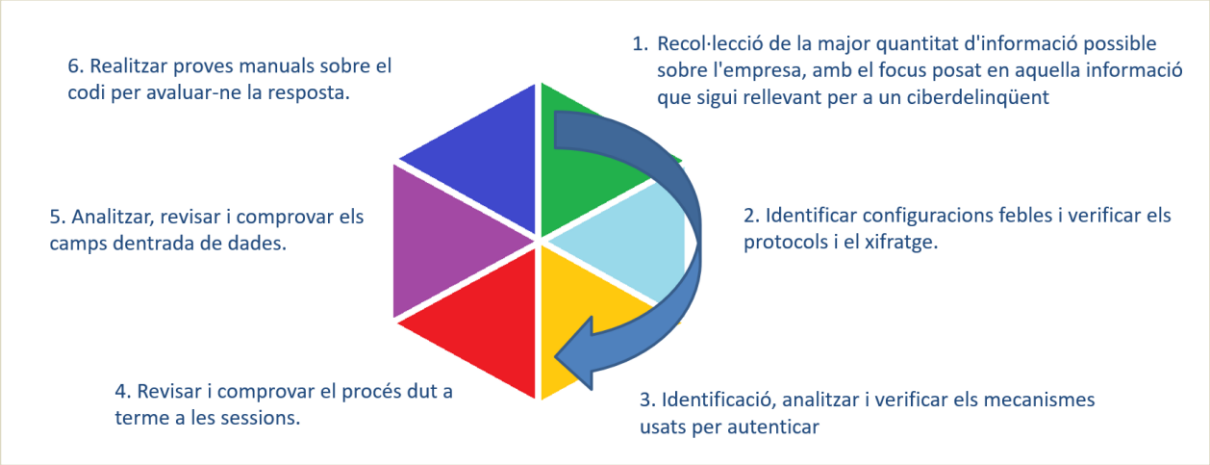
Abast, utilitzant com a referència metodologies internacionals com OWASP, i recolzant-se en les seves pròpies metodologies (basades en estàndards internacionals com MITRE ATT&CK), procedirà a:

- **Realització de proves externes:**
    - Recol·lecció de la major quantitat d'informació possible sobre l'empresa, focalitzant-se en aquella informació que sigui rellevant per un ciberdelinqüent.
    - Escaneig de la xarxa i enumeració dels dispositius connectats.
    - Identificació de ports exposats externament.
    - Identificació de serveis i versionat, per detectar vulnerabilitats associades a aquests.
    - Cerca de fitxers exposats públicament, com podrien ser fitxers de configuració o credencials d'usuaris.
    - Avaluació dels protocols de comunicació i xifratge.
    - Entendre els mecanismes de defensa, i verificar-ne la robustesa.
    - Dins l'abast acordat, explotar de manera controlada aquelles vulnerabilitats que s'hagin detectat als serveis accessibles i exposats externament.
- **Realització de proves internes:**

- Identificar la xarxa interna, la tipologia i la segmentació d'aquesta.
- Realitzar un escaneig de tots els serveis interns utilitzats per identificar-ne les versions i vulnerabilitats associades.
- Identificar rutes, fitxers o males configuracions.
- Identificar i avaluar els protocols de comunicació i xifratge utilitzats per l'empresa.
- Identificar vulnerabilitats mitjançant eines automàtiques i tècniques manuals.
- Analitzar i revisar la robustesa dels mecanismes de control i prevenció existents.
- Explotar de manera controlada les vulnerabilitats internes per aconseguir accés al sistema.
- Intentar fer salts a altres equips, escalar privilegis i imitar el comportament d'un ciberdelinqüent.

Recol·lecció d'informació a través de OSINT (Externa) o xarxa (interna)
Escanejar ports i serveis per identificar software i versions utilitzades
Identificar vulnerabilitats mitjançant proves manuals i eines automatitzades
Identificar y provar punts d'entrada com serveis FTP, SSH, SMB…
Explotació de les vulnerabilitats identificades i obtenció d'informació
Elevar privilegis i realitzar moviments laterals

Per la revisió de les aplicacions web, on s'utilitza la metodologia internacional Open Web Application Security Project (OWASP) i la metodologia desenvolupada per Abast Systems & Solutions, S.L., es defineixen les tasques següents:



Il·lustració 1: Metodologia de treball

1.3.2 Eines de treball

A més a més de les metodologies utilitzades anteriorment esmentades, l'equip de treball d'Abast utilitza eines automatitzades articulades amb tècniques manuals que permeten detectar vulnerabilitats complexes que podrien passar desapercebudes en altres eines automàtiques. Això permet simular atacs del món real, avaluar el context i la prioritat de les vulnerabilitats, així com proporcionar retroalimentació immediata i personalitzada, assegurant una cobertura més exhaustiva i adreçada a les necessitats específiques de l'organització i el context del negoci.

Per Abast és important establir una metodologia de proves basada en l'entesa del negoci, cosa que permet fer una anàlisi amb l'enfocament i el context adequat.

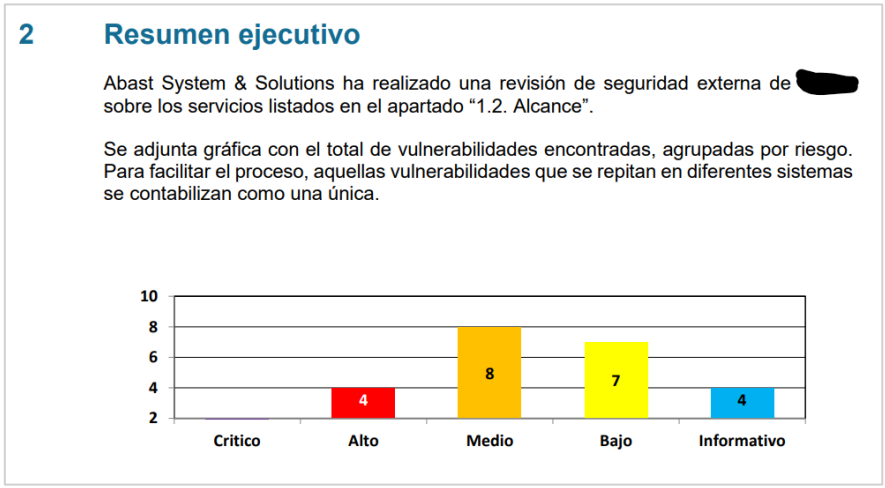
1.3.3 Informe de resultats

Es recol·lectaran i documentaran totes les evidències durant tot el procés de proves de pentesting. Els resultats seran plasmats a:

- L'informe executiu: Recollirà els resultats generals obtinguts durant l'avaluació de seguretat de l'entorn acordat, les deficiències més importants i l'impacte que podrien tenir al negoci de la companyia.
- L'informe tècnic: Recollirà el detall de cada vulnerabilitat trobada, classificada pel seu nivell de risc, i oferirà solucions per abordar-les. Dins aquest informe podem destacar:
  - Descripció de la vulnerabilitat
  - Detall de les proves realitzades
  - Nivell de risc
  - Evidències per entendre el pas a pas
  - Serveis i programari afectats
  - Recomanacions amb solucions

Els resultats es presentaran als responsables de l'àrea i, en cas que sigui necessari, es podran realitzar reunions per validar els resultats o resoldre qualsevol inquietud.

A continuació, de manera informativa, es mostren fragments d'un informe de resultats, els quals, per motius de confidencialitat, no poden ser presentats en la seva totalitat. Aquests informes poden ser lliurats en idioma espanyol o català, segons preferència.



2 Resumen ejecutivo

Abast System & Solutions ha realizado una revisión de seguridad externa de [redacted] sobre los servicios listados en el apartado "1.2. Alcance".

Se adjunta gráfica con el total de vulnerabilidades encontradas, agrupadas por riesgo. Para facilitar el proceso, aquellas vulnerabilidades que se repitan en diferentes sistemas se contabilizan como una única.

Il·lustració 2: Exemple d'informe

Título	Riesgo
Fortinet SSL VPN - Vulnerabilidad XSS	Alto
Posibilidad de fuerza bruta	Alto
Default Pages / Old / Test / Backup Files	Alto
Software sin soporte	Alto
WordPress Username enumeration	Medio
DNS Server - Amplification DDoS	Medio
DNS Server - Hostname disclosure	Medio
Certificado SSL/TLS auto firmado	Medio
Certificado SSL/TLS Expirado	Medio
Directory Listing Enabled	Medio
Métodos HTTP inseguros - TRACE	Medio
SSL/TLS Suites de cifrado medio soportados	Medio
Clickjacking	Bajo
HTTP Strict Transport Security (HSTS) Missing	Bajo
Information Disclosure - ETag Header	Bajo
Information Disclosure - HTTP Headers	Bajo
Information Disclosure - Paths del aplicativo	Bajo
SSL/TLS - Utilización de algoritmo de cifrado RC4	Bajo
SSL/TLS Diffie-Hellman Modulus <= 1024 Bits	Bajo
Métodos HTTP inseguros	INFO
TLS versión 1.0 y/o 1.1 soportado	INFO
SSL Certificate 'commonName' Mismatch	INFO
Panel de administración visible	INFO

Il·lustració 3: Exemple vulnerabilitats identificades

.

ID	[redacted]
Título	Fortinet SSL VPN - Vulnerabilidad XSS
Riesgo	Alto
Descripción	Durante las pruebas realizadas ha sido posible inyectar código JavaScript en los parámetros de la aplicación web. Existe una vulnerabilidad en Fortigate CVE-2018-13380, que permite realizar ataques del tipo XSS previas a la autenticación en portal web SSL VPN a través de la explotación de los parámetros de manejo de mensajes de errores. Un atacante podría realizar un ataque de inyección de códigos maliciosos, comprometiendo la información del servicio en sus tres vectores: confidencialidad, integridad y disponibilidad.
Evidencias	[redacted] Inyección XSS relejada en el 'PopUp' en 2[redacted]
Solución	Se recomienda actualizar los servicios de Fortinet a su última versión
IPs afectadas	2[redacted]

ID	[redacted]
Título	Posibilidad de fuerza bruta
Riesgo	Alto
Descripción	Durante las pruebas realizadas ha sido posible realizar fuerza bruto sin ningún tipo de bloqueo. Un atacante podría automatizar un proceso para obtener credenciales válidas de usuarios a través de ataques de diccionario o de fuerza bruta al no haberse identificado sistemas que impidan esta automatización.

Il·lustració 4: Exemple detall d'informe

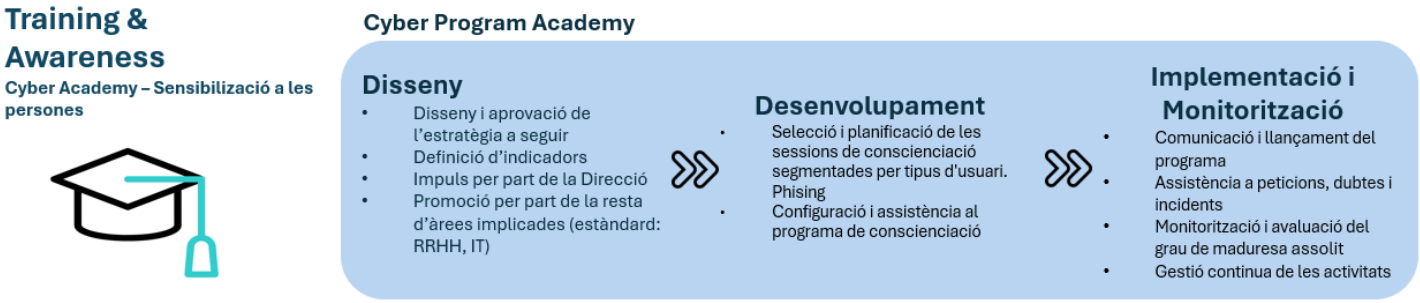
Addicionalment s'elaborarà l'anàlisi del compliment normatiu del *framework* de controls que apliqui o vulgui complir el Client (ENS, ISO 27001, NIS 2, etc.), generant el corresponent Pla Director de Seguretat que contemplarà les mesures de seguretat tècniques i organitzatives per al seu compliment.

Il·lustració 5: Exemple d'informe Pla Director de Seguretat

1.4 Servei de formació general en ciberseguretat

L'objectiu d'aquest lot és establir les pautes per:

- Mantenir els empleats i usuaris informats sobre les darreres amenaces, tècniques d'atac i bones pràctiques.
- Realitzar capacitacions periòdiques per actualitzar coneixements i reforçar la importància de la seguretat.
- Conscienciació sobre riscos reals: Mostrar exemples concrets d'atacs i les seves conseqüències perquè comprenguin la importància d'actuar amb responsabilitat, promoure una cultura de prevenció i cura en l'ús de les tecnologies, identificació d'amenaces, capacitar sobre com reconèixer correus electrònics de *phishing*, enllaços sospitosos i altres tècniques d'enginyeria social i ensenyar a reportar incidents o sospites de manera ràpida i efectiva.
- Promoure l'ús ètic i responsable de dispositius, xarxes i aplicacions.
- Simulacres i exercicis pràctics: Realitzar simulacions d'atacs perquè els usuaris practiquin com reaccionar davant d'una amenaça.
- Fomentar un ambient on la seguretat sigui una prioritat compartida i valorada per tothom.



Il·lustració 6: Metodologia de treball

Abast proposa un model per a la creació d'una consciència avançada a través d'un programa basat en la selecció i la combinació de diferents elements que permetrà planificar, mesurar i crear el material necessari per entrenar als empleats.

Cyber Academy ofereix als seus clients subscrits una varietat d'opcions per desenvolupar el seu pla de conscienciació, assegurant-se que sempre tinguin campanyes i materials de conscienciació per fomentar comportaments segurs dels empleats:

- ✓ Mòduls de formació interactius i jocs.
- ✓ Microaprenentatge animat, vídeos, etc.

1.4.1 Formació General en Ciberseguretat

Desenvolupament del material i contingut de la formació general en matèria de Ciberseguretat:

1. Introducció a la ciberseguretat

- Què és la ciberseguretat? Definició i objectius.
- Importància de la ciberseguretat en la vida quotidiana, empreses i governs.
- Evolució de les amenaces digitals i tendències actuals.

2. Conceptes bàsics de seguretat informàtica
- Confidencialitat, integritat i disponibilitat (Triada CIA).
- Autenticació, autorització i control d'accessos.
- Dades sensibles i protecció de la informació.

3. Tipus d'amenaces i atacs cibernètics
- Malware: virus, troians, ransomware, spyware.
- Phishing i enginyeria social.
- Atacs de denegació de servei (DDoS).
- Explotació de vulnerabilitats i atacs interns.

4. Bones pràctiques de seguretat per a usuaris
- Creació i gestió de contrasenyes segures.
- Ús responsable de xarxes Wi-Fi i dispositius.
- Reconeixement de correus sospitosos i enllaços maliciosos.
- Actualització regular de programari i sistemes.

5. Eines i tecnologies de seguretat
- Antivirus, tallafocs i sistemes de detecció d'intrusions.
- Autenticació en dos passos i gestors de contrasenyes.
- Encriptació de dades i comunicacions.
- Sistemes de gestió d'esdeveniments i informació de seguretat (SIEM).

6. Gestió d'incidents i resposta davant de bretxes de seguretat
- Com detectar i reportar incidents.
- Passos per contenir i erradicar amenaces.
- Importància de l'anàlisi forense digital.
- Elaboració de plans de resposta i recuperació.

7. Normatives, estàndards i bones pràctiques
- Principals regulacions (GDPR, ISO 27001, NIST).
- Polítiques internes de seguretat.
- Cultura de seguretat i sensibilització a organitzacions.

8. Seguretat al Núvol i Entorns Híbrids
- Riscos i bones pràctiques al núvol.
- Configuració segura i gestió d'accessos.

9. Tendències i futur de la ciberseguretat
- Intel·ligència artificial i automatització.
- Seguretat a l'Internet de les Coses (IoT).
- Noves amenaces i com preparar-s'hi.

1.4.1.1 Ús de material

Per desenvolupar aquest pla formatiu s'utilitzarà el material que resulti d'utilitat, com per exemple:

- Vídeos explicatius i tutorials bàsics.

- Casos d'estudi i exemples reals.
- Qüestionaris i exercicis per reforçar coneixements.
- Guies ràpides i *checklists* de bones pràctiques.

1.4.2 Formació Especialitzada per a Responsables TIC

Desenvolupament del material i contingut de la formació per al personal tècnic en matèria de Ciberseguretat:

1. Introducció a la gestió d'infraestructura de seguretat
- Conceptes bàsics d'infraestructura de TI i la importància que tenen en la seguretat.
- Arquitectura de xarxes segures i segmentació.
- Components clau: tallafocs, sistemes de detecció i prevenció d'intrusions (IDS/IPS) i sistemes de gestió d'esdeveniments (SIEM).
- Millors pràctiques en la configuració i el manteniment d'infraestructura segura.

2. Eines i tecnologies per a la gestió d'infraestructura
- Sistemes de monitorització i gestió de xarxes.
- Eines d'automatització i orquestració.
- Ús de plataformes de gestió de vulnerabilitats.
- Implementació i gestió de certificats digitals i VPNs.

3. Detecció i resposta a incidents de seguretat
- Tipus d'incidents i impacte.
- Cicle de vida de l'incident: detecció, anàlisi, contenció, erradicació, recuperació i aprenentatge.
- Ús de sistemes SIEM per a correlació i anàlisi d'esdeveniments.
- Tècniques d'anàlisi forense digital i recopilació d'evidències.

4. Procediments i protocols de gestió d'incidents
- Planificació i elaboració de plans de resposta a incidents.
- Rols i responsabilitats de l'equip tècnic.
- Comunicació interna i externa durant un incident.
- Documentació i informe d'incidents.
- Exercicis pràctics i simulacions d'incidents.

5. Anàlisi de vulnerabilitats i gestió de *patches* (pegats)
- Identificació i priorització de vulnerabilitats.
- Estratègies de *patches* (pegats) i actualització de sistemes.
- Avaluació de riscos associats a vulnerabilitats.

6. Seguretat a la infraestructura al núvol i entorns híbrids
- Consideracions específiques per a entorns al núvol.
- Configuració segura i gestió d'incidents al núvol.

7. Normatives i bones pràctiques
- Compliment estàndards i regulacions (ISO 27001, NIST, GDPR, etc.).
- Polítiques internes i procediments de seguretat.

1.4.2.1 Ús de material

Per desenvolupar aquest pla formatiu s'utilitzarà el material que resulti d'utilitat, com per exemple:

- Guies ràpides i *checklists* per a la gestió d'incidents.
- Casos d'estudi i anàlisi d'incidents reals.
- Simulacions i exercicis pràctics amb escenaris ficticis.
- Vídeos explicatius i tutorials pas a pas.

1.4.3 Preparació de la formació

Format de la formació en ciberseguretat *Online:*

1. **Preparació prèvia**

- Definir objectius clars de la formació.
- Seleccionar i preparar el contingut i els materials didàctics (presentacions, vídeos, casos pràctics).
- Escollir la plataforma de videoconferència (Zoom, Teams, Google Meet, etc.) i verificar compatibilitat.
- Enviar invitacions amb enllaços, agenda i requisits tècnics als participants.
- Preparar recursos addicionals: qüestionaris, exercicis, fòrums de discussió.

2. **Estructura de la sessió**

- **Inici (10-15 minuts)**
  - Benvinguda i presentació de l'instructor i dels participants.
  - Presentació dels objectius i agenda del dia.
  - Dinàmica ràpida per trencar el gel (preguntes, enquestes, etc.).

- **Desenvolupament (60-90 minuts)**
  - Explicació teòrica amb suport visual (diapositives, vídeos).
  - Ús d'exemples pràctics i de casos reals per contextualitzar.
  - Demostracions en viu o simulacions, si és possible.
  - Espais per a preguntes i aclariments a cada secció.

- **Activitat pràctica (30-45 minuts)**
  - Exercicis interactius, com ara anàlisi d'incidents, simulacions o resolució de problemes.
  - Ús de plataformes de laboratori virtual o entorns controlats.
  - Discussió en petits grups (sales de *breakout*) per fomentar la participació.

- **Tancament (15-20 minuts)**
  - Resum dels punts clau.
  - Avaluació ràpida (enquestes, qüestionaris).
  - Espai per a dubtes finals.
  - Informació sobre recursos addicionals i propers passos.

- **Metodologia i recursos**
  - Ús de metodologies actives: aprenentatge basat en problemes, estudis de casos, debats.
  - Incorporació de recursos multimèdia per mantenir interès.
  - Fomentar la participació mitjançant preguntes obertes i enquestes en viu.
  - Proveir materials descarregables (guies, *checklists*, resums).

- **Seguiment i avaluació**
  - Enviar un qüestionari de satisfacció i avaluació de l'aprenentatge.
  - Proporcionar certificats de participació, si s'escau.
  - Oferir recursos de suport i contacte per a dubtes posteriors.
  - Programar sessions de reforç o actualització, si cal.

abast

BUILDING YOUR FUTURE IT

www.abast.es

BARCELONA
C/Equador 39-45
08029 Barcelona
Tel. 933 666 900

MADRID
C/ de la Basílica, 19 9ºB
28020 Madrid
Tel. 914 061 601

PALMA
C/ Fluvià 1, Baixos dreta
Despatx 25 07009 Palma
Tel. 971 706 882