semic | econocom
LIVE TECH

ACM
LOT 35

MEMÒRIA TÈCNICA

EXP.: 2024.01

notificacions@semic.es | www.semic.es

1 Índex

2 Sumari executiu

SEMIC és una empresa del sector de les Tecnologies de la Informació (TI) amb més de 40 anys d'experiència en el mercat espanyol.

SEMIC té la capacitat, els coneixements i l'equip professional necessari per cobrir totes les necessitats tecnològiques que requereixi una empresa. La finalitat de SEMIC és mantenir els seus clients productius, connectats i protegits des de qualsevol lloc on treballin, per això, basa el seu negoci en tres pilars:

- La **digitalització:** SEMIC es transforma digitalment per atendre els seus clients com vulguin i quan ho necessitin, desenvolupant i implantant plataformes online per escoltar les seves demandes, sense deixar de banda l'atenció personal, pròxima i confiable que sempre ha caracteritzat la companyia.
- La **sostenibilitat**: SEMIC és una empresa Carboni Neutral, que promou l'economia circular i està alineada amb els objectius del Pacte Verd Europeu i de l'Agenda 2030 pel Desenvolupament Sostenible (ODS).
- Els **serveis gestionats:** SEMIC aposta per la transició cap a models de serveis contractuals de TI, que garanteixen la màxima eficiència i eficàcia dels processos, aconseguint així crear solucions de gestió global, flexibles i que s'adaptin al ritme de creixement de cada empresa, mantenint la visió de principi a fi en la gestió dels serveis de IT.

SEMIC és conscient de les necessitats en TI particulars de sectors com **l'Educació, la Sanitat i les Administracions Públiques**, i és per això que té unitats de negoci especialitzades en atendre les demandes i els projectes d'aquestes tres verticals; mitjançant aquest document es presenta la proposta per al desenvolupament d'aquest projecte.

La prestació del subministrament es realitzarà segons les indicacions requerides per l'organisme contractant, tenint en compte en tot moment:

Les pautes marcades per l'organisme contractant i els procediments i controls de SEMIC, recollits en la documentació interna del sistema segons:

- La norma ISO 9001 de gestió de la qualitat.
- La norma ISO 20000-1 de gestió dels serveis TI
- La norma BS 8887-220 de remanufactura (fabricació, muntatge, desmuntatge i processament al final de la vida útil dels dispositius)
- La norma ISO 27001 de gestió de seguretat de la informació.
- L'Esquema Nacional de Seguretat (ENS) per garantir la seguretat de la informació tractada per les AAPP
- La metodologia ITIL per a la Gestió dels serveis de Tecnologies de la Informació.
- Certificació PMP® del PMI® per a la gestió de projectes.
- La norma ISO 45001 de Seguretat i Salut en el Treball
- La norma ISO 14001 de gestió del medi ambient.
- La norma ISO 50001 de gestió Energètica
- Protocol GHG (Gestió de gasos efecte hivernacle)

- Reglament EMAS de gestió ambiental de la Unió Europea
- La norma RSE-100 de Responsabilitat Social Empresarial

2.1. Localització

SEMIC és una empresa d'àmbit nacional amb 10 oficines distribuïdes per tot el territori espanyol i Andorra.

2.2. Vies de comunicació

Per tal de poder atendre de forma més eficient les incidències o peticions, les vies de comunicació establertes en horari laboral són les següents:

- Telefònica: 973 00 33 12
- Correu electrònic: supportdesk@semic.es

S' aconsella utilitzar la via de correu electrònic.

Tant si la comunicació és per via telefònica com per correu electrònic, el client haurà d' aportar la següent informació:

- Nom i cognom de la persona que realitza la trucada.
- Nom de l' empresa.
- Número de telèfon i adreça de correu de contacte perquè el nostre personal es posi en contacte amb ell/ella
- Descripció de la incidència.
- Troubleshooting realitzat pel N1

Amb l' obertura de la incidència, el nostre equip de suport, li enviarà un correu amb el número de cas assignat per la nostra eina de gestió. És important que, un cop rebut aquest correu, mantingui el contingut de l' assumpte, ja que aquest conté una etiqueta que fa que totes les comunicacions per correu electrònic s' annexin al tiquet. Si no ho fa, l'eina generarà un tiquet addicional.

És molt important que se segueixin les vies de comunicació establertes, de no fer-ho, és possible que alguna petició pugui quedar sense atendre.

3 Serveis de Ciberseguretat

Considerant l'àmbit i l'abast del servei, a continuació s'exposen les activitats que es portaran a terme per part de SEMIC durant la seva prestació.

3.1. Prestació 172. Servei d'assessoria

3.1.1. Descripció del producte ofertat

El Servei d'assessoria en ciberseguretat ofert per SEMIC proporciona una cobertura completa i personalitzada per ajudar l'entitat a reforçar la seva postura de seguretat, prevenir riscos i garantir el compliment normatiu. Aquest servei inclou tant auditories tècniques com consultoria estratègica, amb l'objectiu de detectar vulnerabilitats, millorar la infraestructura i oferir un pla de millora adaptat a les necessitats específiques de l'organització.

A SEMIC oferim un ventall ampli d'auditories i serveis especialitzats, entre els quals destaquem:

- **Auditories de vulnerabilitats** (externes i internes): Identificació de configuracions incorrectes, serveis exposats i punts febles en sistemes i aplicacions.
- **Proves de penetració (Pentesting)**: Simulació controlada d'atacs per verificar si un agent extern podria comprometre els sistemes o accedir a dades sensibles.
- **Auditories de seguretat per a aplicacions i APIs**: Avaluació de vulnerabilitats en interfícies digitals i aplicacions crítiques, amb eines DAST com Burp Suite i OWASP ZAP.
- **Auditories per entorns amb Intel·ligència Artificial (IA)**: Identificació de riscos associats a l'ús de models de llenguatge i sistemes intel·ligents.
- **Anàlisi de riscos i Pla de Millora**: Avaluació contextual de les troballes i definició d'un pla d'acció per garantir el compliment de l'ENS, NIS2, ISO 27001 i altres normatives vigents.

Aquest servei està dissenyat per adaptar-se al nivell de maduresa tecnològica de l'entitat, i pot incloure assessorament inicial, revisions puntuals, o un seguiment continuat per garantir una evolució constant i segura.

A través d'aquest enfocament integral, SEMIC no només detecta les vulnerabilitats existents sinó que aporta valor estratègic ajudant a enfortir l'entorn digital del client davant les amenaces actuals i emergents.

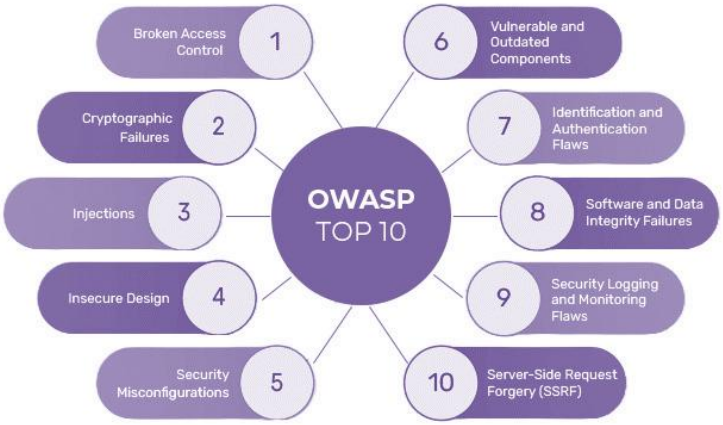
3.1.2. Eines, tècniques i procediments

SEMIC aplica un enfocament sistemàtic i estructurat per identificar, analitzar i mitigar vulnerabilitats. Es combinen eines de primer nivell com **Nessus**, **Qualys**, **Burp Suite** i **OWASP ZAP** amb comprovacions manuals i simulacions reals.

Les auditories es basen en quatre fases:

- **Descobrir**: escaneig i detecció manual de vulnerabilitats.
- **Analitzar**: avaluació segons el sistema **CVSS** per prioritzar riscos.
- **Explotar**: proves controlades per confirmar la gravetat de les vulnerabilitats.
- **Recomanar**: propostes d'accions correctores i bones pràctiques.

Es segueixen estàndards com **OWASP Top 10**, **NIST SP 800-115**, **CIS Benchmarks**, i es fa ús de referències com **CVE** i **CVSS** per assegurar una avaluació rigorosa.



3.1.3. Abast i nivell de detall de l'auditoria

Les auditories cobreixen infraestructures, xarxes, aplicacions, usuaris i actius crítics, incloent dades personals. També s'avalua la gestió de la seguretat a nivell organitzatiu segons les exigències de la **Directiva NIS2**.

L'activitat combina eines automatitzades amb anàlisi manual per detectar tant vulnerabilitats conegudes com emergents. El resultat és un informe tècnic exhaustiu i un resum executiu amb recomanacions concretes.

3.1.4. Vectors d'atac i identificació de riscos

S'avaluen escenaris reals de risc mitjançant vectors com:

- Escaneig de xarxes, fingerprinting, anàlisi de vulnerabilitats conegudes.
- Explotació de falles en aplicacions web (OWASP), accessos a APIs, escalada de privilegis.
- Simulacions d'enginyeria social i phishing, atacs a entorns cloud, accés físic i tècniques LotL.

Aquest enfocament permet identificar punts dèbils i planificar mesures de contenció específiques.

3.1.4.1. Vectors d'atac proposats i justificació

Els vectors d'atac cobreixen els principals àmbits de risc (digitals, físics i humans), amb un enfocament actualitzat, realista i específicament adaptat a les característiques de l'entitat. Aquests vectors permeten simular escenaris d'amenaça amb impacte potencial elevat.

S'analitzen múltiples vectors per simular escenaris d'amenaça realistes:

- **Escaneig i fingerprinting**: detecció de serveis, tecnologies i configuracions exposades.
- **Anàlisi de vulnerabilitats**: ús d'eines automàtiques i bases de dades públiques (CVE, NIST).
- **Explotació web i APIs**: proves OWASP Top 10, injeccions, manipulació de tokens.
- **Accés indegut i escalada de privilegis**: proves de força bruta i revisió de permisos.
- **Enginyeria social i phishing**: simulacions per avaluar el factor humà.
- **Persistència i backdoors**: tècniques per comprovar si un atacant pot mantenir l'accés.
- **Intercepció de comunicacions**: ARP spoofing, DNS poisoning, SSL stripping.
- **Infraestructura Cloud**: revisió de configuració en entorns com Azure, AWS, O365.
- **Seguretat física**: accés a dispositius i espais sensibles.
- **Tècniques LotL i exploits zero-day**: ús d'eines pròpies del sistema i simulació d'atacs avançats.

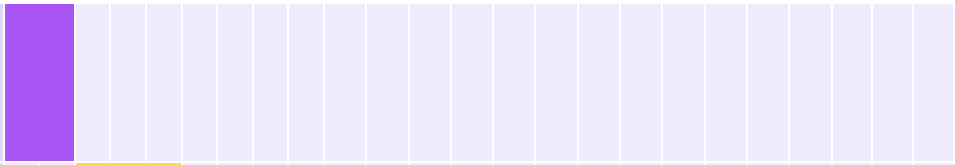
3.1.4.2. Tècniques utilitzades i anàlisi de resultats

Un cop identificades les vulnerabilitats mitjançant l'ús combinat d'**escàners automàtics** i **tècniques manuals**, aquestes són **classificades segons la seva criticitat i risc potencial** emprant el sistema **CVSS (Common Vulnerability Scoring System)**. En aquells casos en què les eines utilitzades no proporcionin una puntuació automàtica, l'equip auditor procedeix a calcular-la manualment mitjançant la **calculadora oficial de FIRST**, assegurant una valoració objectiva i estandarditzada.

3.1.4.3. Cronograma i flux de comunicació

La planificació de les actuacions es realitzarà de forma coordinada amb l'entitat, assegurant la traçabilitat i minimitzant l'impacte en els serveis. El flux de comunicació es divideix en tres fases: reunió inicial per definir l'abast i els canals; seguiment periòdic durant l'execució; i entrega final d'informes amb sessió de presentació de resultats. Les proves s'ajustaran a franges horàries de baixa activitat per garantir la continuïtat operativa.

		Duració estimada (dies)																					
15	**Activitats**	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

Planificació i Kick-off	Reunió inicial, definició d'abast, calendarització i coordinació	
Recollida d'informació	Entrevistes, anàlis documental, inventari de sistemes i usuaris	
Execució tècnica	Escaneig de vulnerabilitats, proves manuals i explotació controlada	
Anàlisi i elaboració d'informes	Classificació de troballes, redacció d'informe tècnic i executiu	
Presentació de resultats	Sessió de lliurament i expliació de resultats i recomanacions	

3.1.4.4. Mesures per evitar interrupcions i pla de recuperació

Per evitar afectacions als serveis durant les proves, SEMIC aplica mesures com l'ús d'entorns de preproducció, la coordinació d'horaris amb l'entitat, l'ús de tècniques de baix impacte i la disponibilitat d'un pla de contenció i recuperació davant incidències imprevistes.

3.1.5. Entregables

L'entregable és un informe que conté un apartat d'**Informe Executiu**, amb un resum no tècnic de les vulnerabilitats detectades, i un apartat d'**Informe Tècnic** amb el detall de les incidències, així com les recomanacions per corregir-les.

A l'apartat de l'Informe Tècnic s'indica quin control de seguretat de l'OWASP ha fallat per a cada vulnerabilitat trobada, respectant el codi de control d'OWASP (per exemple, OTG-INFO-001), per facilitar al client la gestió del cicle de vida de la vulnerabilitat.

3.1.6. Pla de millora

A partir dels resultats de l'auditoria inicial, SEMIC elaborarà un **Pla de Millora Estratègic** per reforçar la seguretat de l'entitat i reduir l'exposició a riscos crítics.

El pla inclourà:

- **Millores d'infraestructura:** accions prioritzades per reforçar servidors, xarxes i dispositius, amb propostes com EDR, segmentació de xarxa, xifrat i monitoratge centralitzat.
- **Prevenció d'amenaces:** mesures específiques contra ransomware, phishing i altres vectors habituals, a més de revisions de contrasenyes, privilegis i pràctiques d'autenticació.
- **Compliment normatiu:** accions per alinear-se amb l'ENS, la NIS2 i la norma ISO 27001, incloent millores en rols, documentació i protocols de seguretat.

Les accions es planificaran amb un **cronograma**, assignació de **responsables** i sistema de **seguiment**, adaptat a la realitat operativa del client i amb l'objectiu d'obtenir una millora sostinguda i mesurable.

3.2. Prestació 173. Servei de formació en ciberseguretat

3.2.1. Descripció del producte ofertat

El servei proposat ofereix una solució integral de **formació i sensibilització en ciberseguretat** dirigida als treballadors d'una organització. L'objectiu principal és **elevar el nivell de consciència i coneixement dels usuaris** davant de les principals amenaces cibernètiques, millorant així la capacitat de resposta de l'organització i reduint els riscos associats als ciberatacs.

El servei de formació en ciberseguretat proposat per SEMIC s'estructura en dues fases complementàries:

1. Una **formació inicial diferenciada**, adaptada als perfils dels usuaris.
2. Un servei continu de **píndoles formatives mensuals**, dirigit a tot el personal.

Aquest plantejament permet generar una base de coneixement sòlida i, alhora, mantenir la sensibilització activa al llarg del temps.

3.2.2. Formació inicial

La formació inicial es realitza en dues modalitats:

- **Formació General**: adreçada al conjunt de treballadors de l'entitat. Inclou formació sobre phishing, correus sospitosos, contrasenyes segures, gestió de dades i dispositius, i exemples reals de ciberatacs per augmentar la consciència i capacitat de resposta.
- **Formació per a Responsables TIC**: dirigida a perfils tècnics i de responsabilitat en sistemes d'informació. Aprofundeix en temes com la gestió d'infraestructures segures, resposta davant incidents i implantació de mesures avançades de protecció. Aquesta sessió inclou també una **actualització sobre les normatives vigents** que apliquen a l'entitat, com ara:
    - **LOPDGDD i RGPD**: protecció de dades personals, principis de licitud, responsabilitat proactiva i registre d'activitats.
    - **ENS (Esquema Nacional de Seguretat)**: requisits mínims de seguretat per a entitats públiques, classificació de sistemes i controls tècnics i organitzatius.
    - **NIS2**: responsabilitats i mesures per a entitats essencials i importants en sectors crítics.

- **ISO/IEC 27001**: estàndard internacional per a sistemes de gestió de la seguretat de la informació (SGSI), controls annexos i auditories internes.

Aquesta actualització normativa ajuda els responsables TIC a interpretar els requeriments aplicables, identificar desviacions i planificar actuacions correctores.

3.2.3. Servei de pildores formatives mensual

Un cop realitzada la formació inicial, es posa en marxa un servei de píndoles formatives, basat en l'enviament de **píndoles mensuals per correu electrònic** a tots els treballadors. Aquestes píndoles tenen com a objectiu consolidar hàbits segurs i mantenir una cultura de ciberseguretat activa dins de l'organització.

Funcionament del servei:

- Cada mes es lliura una píndola amb un **tema específic i actualitzat**, en format breu i comprensible.
- El contingut inclou recomanacions pràctiques, exemples reals i consells per prevenir riscos.
- L'enviament es fa de forma controlada, amb seguiment de la participació mitjançant informes.
- S'inclouen **dues avaluacions durant l'any** per mesurar l'impacte formatiu i el grau de conscienciació dels usuaris.

Temàtiques mensuals de les píndoles:

1. Identificació de correus phishing
2. Contrasenyes segures i gestors
3. Actualitzacions de sistemes
4. Autenticació de doble factor
5. Ús segur de dispositius USB
6. Ús de dispositius personals
7. Xarxes segures
8. Gestió de dades sensibles
9. Missatgeria segura
10. Navegació segura per Internet
11. Conscienciació sobre malware
12. Notificació d'incidents
13. Seguretat en el teletreball