FGC
Ferrocarrils
de la Generalitat
de Catalunya

Sistema de gestió d'accés i seguretat proactiva

Especificació tècnica

Àrea de Ciberseguretat
Tecnologies de la Informació i les Comunicacions
Rev. 1.0 – Desembre 2024

Ferrocarrils de la Generalitat de Catalunya, c/ Vergós 44, 08017, Barcelona

ÍNDEX

Introducció

Context i Objectius

Aquest document constitueix el Plec de Prescripcions Tècniques per establir les condicions de contractació relacionades amb el subministrament, instal·lació, configuració, integració i posada en funcionament d'una plataforma de Gestió d'Accés Privilegiat (PAM, Privileged Access Management, d'ara endavant) que permeti protegir tant la infraestructura i les aplicacions, com gestionar de manera eficient i mantenir la confidencialitat de les dades sensibles i la infraestructura crítica de FGC.

FGC, també pretén protegir de manera proactiva les seves infraestructures de possibles amenaces avançades i persistents. Per això es pretén en aquesta solució afegir tecnologies de deception per a poder generar entorns simulats i honeypots per tal d'enganyar i detectar de manera preventiva activitats malicioses. Am la implementació d'aquest tipus de tecnologies, FGC vol millorar la detecció, resposta i anàlisi dels possibles atacs, minimitzant impactes en actius crítics millorant així la resiliència operativa.

Com a part de la seva estratègia de seguretat, FGC busca incorporar una solució que protegeixi els seus sistemes crítics i ofereixi una capa essencial de seguretat informàtica per salvaguardar les dades, la infraestructura i els actius organitzacionals, així com els seus processos. A més, la solució ha d'incloure nous mecanismes per protegir els recursos TI davant ciberatacs que puguin aprofitar privilegis interns per comprometre els actius més importants de l'organització.

Aquest document defineix tots els requisits necessaris que ha de complir la solució de Gestió d'Accés Privilegiat (PAM) i les tecnologies de deception per atendre les necessitats de FGC.

Objecte del plec

L'objecte del present document té com a objectiu l'adquisició i posada en servei una plataforma de Gestió d'Accés Privilegiat (PAM) i tecnologia deception, garantint el dret d'ús d'aquestes plataformes. Això inclou la instal·lació, configuració, integració i posada en funcionament de la solució, així com el seu manteniment correctiu i evolutiu periòdic durant la durada del contracte. Aquesta durada s'estableix en tres anys.

Requeriments generals

A mode general, la eina de PAM, haurà de:

- Proporcionar avaluacions exhaustives, consistents i tècnicament adequades que permetin validar l'eficàcia de l'eina i obtenir informació objectiva sobre els serveis de seguretat que ofereix.
- Oferir un accés amb alt nivell de permisos als recursos TI de FGC. Els comptes gestionats per la plataforma PAM poden pertànyer tant a persones (internes o proveïdors) com a aplicacions que executin serveis o comandaments amb permisos especials, possibilitant la gestió d'aplicacions, programari o recursos de maquinari.
- Assegurar la protecció i el control dels accessos a comptes privilegiats que administren actius i dades crítiques, permetent als usuaris, aplicacions i administradors la flexibilitat necessària per a les seves tasques diàries.
- Prevenir l'ús indegut de comptes privilegiats en sistemes, dispositius i aplicacions TI de l'organització, permetent l'administració i monitoratge de l'ús d'aquestes comptes per part dels usuaris.
- L'administració de credencials de les comptes, amb l'objectiu de reduir risc (leak de credencials), han de ser desconegudes per l'usuari final que es connecta al recurs. A més, s'ha de poder realitzar un rotat i canvi de credencials de les contrasenyes d'accés als recursos.
- Controlar que només els usuaris autoritzats tinguin accés als recursos permesos, podent aplicar controls de ZTNA, sistemes d'aprovacions i control de comandes a cada un dels usuaris.
- Ha de permetre a FGC el compliment del ENS nivell alt per a aquesta eina.
- Monitoritzar l'activitat privilegiada: La plataforma ha de monitoritzar tots els accessos i s'haurà de poder com a mínim:
    - Visualitzar tota sessió activa
    - Visualitzar vídeo de les sessions en temps real
    - Visualitzar comandes SSH introduïdes per l'usuari
    - Auditoria post sessions

A mode general, la solució de deception, haurà de:

- Capacitat per crear i desplegar honeypots en entorns IT/OT que simulin entorns reals (Windows, Linux, SCADA, VPN, hosts, fitxers, etc.) i que no es puguin detectar com a equips preparats.
- Exposar serveis i sistemes de manera real per tal de que els atacants interactuïn amb aquests equips per tal de poder aconseguir una detecció primerenca i precisa en produir-se aquesta interacció.
- Processar, alertar, interactuar amb altres elements de seguretat i eliminar les amenaces que es detectin o s'identifiquin de manera primerenca amb la interacció amb els sistemes parany o honeypots d'alguna manera.

Requeriments funcionals

L'eina proposada a nivell de PAM, ha de donar com a mínim compliment de les següents especificacions funcionals:

- Política d'accés centralitzada
  - **Uniformitat en l'aplicació de polítiques**: S'haurien d'implementar auditories i generació d'informes centralitzats per complir amb els mandats de compliment requerits. Cal un registre d'auditoria d'activitat a prova de manipulacions que rastregi l'activitat de l'usuari i proporcioni un control i seguretat millorats.
  - **Suport multi-plataforma**: Ha de garantir compatibilitat amb múltiples plataformes.
  - **Gestor de connexions**: Les credencials haurien d'estar completament ocultes de l'usuari.
  - **Gestor de Polítiques**: Caldria permetre la definició de polítiques granulares per assegurar l'aplicació del principi de mínim privilegi.
  - **Gestor de comandes**: Hauria de possibilitar la definició de polítiques específiques per a comandes que es poden fer servir.
- Aprovisionament d'accessos
  - **Gestió completa del cicle de vida de la gestió d'accessos**: L'eina ha de gestionar de forma automatitzada el cicle de vida dels comptes privilegiats, incloent el descobriment i la rotació de credencials.
  - **Estructura jeràrquica i funcional**: Cal establir processos d'aprovació jeràrquics per als accessos.
  - **Definició de rols i privilegis**: S'han de poder establir polítiques granulares i processos d'aprovació basats en rols jeràrquics.
  - La solució ha de permetre **diferents fluxos**: Ha de permetre definir processos d'aprovació tant jeràrquics com basats en polítiques específiques.
  - **Sincronització automàtica d'accessos**: S'hauria de garantir la sincronització automàtica de permisos via protocols com LDAP, RADIUS o SAML, a més dels usuaris locals.
- Accés Just-in-Time (JIT)
  - **Accés sota demanda:** L'accés hauria de ser concedit només per un temps predefinit, basant-se en polítiques.
  - **Expiració automàtica d'accessos:** Cal implementar mecanismes per a la creació d'usuaris amb accés limitat en el temps
  - **Fluxos d'aprovació**: Els processos d'aprovació haurien de ser jeràrquics i basats en polítiques
- Monitoratge i Auditoria en temps real
  - **Gestor d'Auditoria**: Hauria de ser possible monitoritzar, gravar i auditar activitats d'usuaris privilegiats
  - **Visualització en temps real**: Caldria incloure funcionalitats com:
    - Visualitzar totes les sessions actives
    - Visualització del vídeo de les sessions en temps real
    - Visualització de les comandes SSH introduïdes per l'usuari
    - Auditoria post sessió

- Autenticació contínua i basada en risc
  - **Avaluació basada en comportament**: Hauria de permetre ajustar l'autenticació segons el comportament de l'usuari.
  - **Ajust dinàmic d'autenticació**: Cal incloure mecanismes d'autenticació adaptativa multi factor basats en el risc i el context
  - **Monitoratge de context**: Hauria de contextualitzar l'autenticació segons el dispositiu, IP i ubicació de l'usuari.
  - **Magatzem segur de credencials**: Les credencials han d'estar completament ocultes i emmagatzemades de manera segura
- Elevació i delegació de privilegis
  - **Elevació controlada de privilegis**: Les polítiques haurien d'enfocar-se en una gestió segura i controlada dels privilegis
  - **Delegació segura de tasques administratives**: Hauria d'estar previst un mecanisme per garantir aquesta funcionalitat
  - **Límits de temps i abast**: Caldria establir mecanismes per limitar els accessos en temps i àmbit
- Interfície d'usuari intuïtiva i administració centralitzada
  - **Panell centralitzat de control**: S'ha de desenvolupar un panell de control centralitzat que faciliti l'administració
  - **Experiència d'usuari intuïtiva**: Caldria treballar en una interfície que optimitzi l'experiència d'usuari
  - **Suport de configuració personalitzable**: Ha de ser possible ajustar les configuracions segons les necessitats específiques
- Informes de Compliment i Auditoria
  - **Informes de compliment**: Haurien de generar-se automàticament informes centralitzats
  - **Registre complet d'activitats**: Cal mantenir un registre complet i a prova de manipulacions de l'activitat de l'usuari
  - **Compliment amb Normatives Globals**: Hauria d'assegurar-se l'adequació a normatives globals i estàndards de seguretat que siguin d'aplicació a FGC
- Seguretat accés a la solució
  - **Filtrat per IP origen**
  - **Limitar accés en funció de l'horari**
  - **Verificar postura de seguretat** del dispositiu d'accés (ZTNA)

L'eina proposada a nivell de deception, ha de donar com a mínim compliment de les següents especificacions funcionals:

- Permetre el desplegament i configuració de manera remota i automàtica dels paranys o honeypots a desplegar.
- Permetre la creació de paranys o honeypots per a xarxes especifiques IT i també OT.
- Permetre el seguiment i rastreig de tota activitat per part dels administradors així com la correlació dels moviments laterals que hagi pogut succeir.

- Realitzar una notificació àgil i rapida, en temps real cap als responsables o administradors.
- Gestionar i desplegar de manera centralitzada aquests honeypots.
- Simular vulnerabilitats o comportaments per a atraure atacants.
- Permetre detecció primerenca, precisa i alertes que es puguin processar. Ha de permetre el rastreig, la correlació i la notificació d'aquestes alertes.
- Monitoreig i correlació d'incidents i campanyes proporcionant informació sobre:
  - Inici i tancament de sessió
  - Seguiment de moviments laterals
  - Arxius. Afegits/modificats/eliminats/executats en els honeypots
- Permetre anàlisis de malware en detall mitjançant integracions amb eines de sandboxing.
- S'ha de poder exportar i notificar els registres com a mínim per correu electrònic, SNMP i SYSLOG/CEF.
- Realització d'informes de les alertes d'incident en formats exportables (PDF/CSV).
- Capacitat per realitzar anàlisi forense de la informació, que permeti detallar moviments i moviments laterals dels atacants, i correlacionar informació d'incidents i campanyes d'atacants actives.
- Interactuar amb altres sistemes per blocar i eliminar amenaces de manera automàtica.
- S'ha de gestionar des d'una consola única el desplegament i l'anàlisi.

Requeriments tècnics

Els requeriments mínims que l'eina proposada a nivell de PAM ha de complir a nivell tècnic son els següents:

- Gestió granular d'accés
  - **Control d'accés basat en rols (RBAC):** Polítiques granulars i jeràrquiques amb aprovació requerida.
  - **Control d'accés basat en atributs (ABAC):** Polítiques personalitzades amb requisits específics.
  - **Control d'accés basat en polítiques (PBAC):** Accés jeràrquic amb polítiques definides pels administradors.
  - **Principi de mínim privilegi:** Aplicació estricta d'aquest principi per defecte.
  - **Implementació MFA:** Disposa d'un MFA adaptatiu.
- Infraestructura d'emmagatzematge de credencials segura
  - **Xifrat de credencials:** Ocultació i xifrat amb algoritmes SSH i mòduls TPM.
  - **MFA per a l'emmagatzematge de credencials:** Autenticació basada en risc i contextualitzada, amb opcions biomètriques.
  - **Control d'accés a la base de dades:** Validació contínua d'endpoints amb ZTNA abans d'atorgar accés.
- Compatibilitat d'entorn i escalabilitat
  - **Xifrat de credencials:** Ocultació i xifrat amb algoritmes SSH i mòduls TPM.
  - **MFA per a l'emmagatzematge de credencials:** Autenticació basada en risc i contextualitzada, amb opcions biomètriques.
  - **Control d'accés a la base de dades:** Validació contínua d'endpoints amb ZTNA

abans d'atorgar accés.

- Gestió de contrasenyes
  - **Polítiques configurables:** Opcions per ajustar la complexitat, rotació i altres paràmetres.
- Integració de protocols d'accés
  - **Suport per a SSH i RDP:** Oferir compatibilitat amb VNC, Telnet, MSSQL, SMB i altres protocols.
  - **Autenticació amb LDAP i AD:** Integració completa amb aquests protocols.
- Adaptació per a múltiples tipus d'autenticació
  - **Tokens d'ús únic:** Integració amb Cloud per a MFA adaptatiu i validació biomètrica.
  - **Certificats d'autenticació:** Gestió de certificats amb notificacions de caducitat.
  - **Autenticació contextualitzada:** Basada en dispositius, IP i ubicació.
- Integració amb sistemes existent
  - **Compatibilitat amb LDAP i Active Directory:** Implementació nativa.
  - **Integració amb SIEMs coneguts via syslog**.
  - **Suport d'API:** Integració amb eines de tercers
- Compatibilitat amb Infraestructures Híbrides i Multi-Cloud
  - **Suport multi-cloud:** Gestió unificada en diverses plataformes.
  - **Seguretat en entorns híbrids:** Accés segur garantitzat.
- Modes d'operació (han de ser configurables per cada recurs)
  - **Mode Proxy:** Configuració per reenviar el tot tràfic a través de la plataforma de gestió.
  - **Mode no-Proxy:** Connexió directa sense intermediari. El client rep les credencials de la plataforma de gestió.
- Compte d'emergència
  - **Break Glass i Disaster Recovery:** Sistema de comptes d'emergència i plans de recuperació. En cas d'emergència o disaster recovery, ha d'haver possibilitat de realitzar un bypass dels controles per accedir a les carpetes, recursos, sol·licitud de accés a recursos… En aquest mode, l'administrador podrà accedir a tots els recursos. Serà requisit indispensable que, durant l'activació d'aquest mode, s'enviï un email als administradors informant i que quedi la sessió gravada.
- Accés a recursos

  Es realitzarà a través de llançadors i la solució haurà de disposar de forma predefinida de llançadors web i d'aplicatius natius. Com a mínim ha de disposar dels següents:
  - Llançadors basats en Web:
    - Web-SSH
    - Web-RDP
    - Web-VNC
    - Web-SFTP
    - Web-SMB
    - Web-Telnet
  - Llançadors d'aplicatius locals:
    - Putty
    - HeidiSQL
    - Microsoft SQL CLI
    - MySQL CLI

- MySQL Shell
- PostgreSQL
- WinSCP
- SSMS (SQL Server Management Studio)
- Remote Desktop
- XShell
- MSTSC
- VNC viewer
- TightVNC
- SecureCRT
- MobaXterm

A més d'aquests llançadors, s'haurà de poder crear nous llançadors "custom" si així es necessita.

- Tecnologia Deception
  - La solució PAM ha de permetre **integrar-se amb capacitats d'altres solucions que facin servir la tecnologia Deception.** Aquestes capacitats son:
    - Identificar atacs dirigits, moviments laterals i activitats sospitoses dins d'una xarxa interna.
    - Complementar a solucions com EDR, NDR, SIEM i SOC per oferir una detecció més primerenca.
    - Simular sistemes, serveis i dispositius per atreure els atacants.
    - Generar paranys que imiten estacions de treball, servidors, IoT/OT i bases de dades sensibles.
    - Operar dins de la xarxa per monitoritzar activitats malicioses que aconsegueixen evadir les defenses externes.
    - Permetre estudiar les tàctiques, tècniques i procediments (TTPs) dels atacants.
    - Integrar frameworks com MITRE ATT&CK per correlacionar l'activitat detectada
    - Ajuda els equips de SOC i CERT a reaccionar ràpidament, recopilant evidències i generant alertes específiques.
- Transferència segura de fitxers
  - La solució ha de permetre securitzar les transferències de fitxers des dels dispositius client cap als recursos crítics (WinSCP o SMB) aplicant perfils de seguretat d'antivirus i/o polítiques DLP.

Els requeriments mínims que l'eina proposada a nivell de deception ha de complir a nivell tècnic son els següents:

- Aquests honeypots han de poder desplegar-se en entorns virtuals i Cloud més comuns (vmWare, Hyper-V, AWS, Azure, etc.).
- S'han de permetre com a mínim el següents tipus de tecnologies, sistemes operatius i serveis en els honeypots:
  - Sistemes operatius
    - Windows 7, 10
    - Windows Server 2016, 2019

    - Ubuntu 16, 18
    - CentOS
    - Redhat 7, 9
- Serveis
    - SMB
    - SAMBA
    - RDP
    - RADIUS
    - GIT
    - FTP
    - ESXi
    - TCP Port Listener
    - SQL Server
    - MySQL
    - ELK
    - SQL ODBC
    - SMTP
    - Connexions de xarxa simulades
    - SAP Connector
    - Documents Office, PDF
- Aplicacions
    - SAP
    - ERP
    - POS
- IoT
    - Cisco Routers
    - IP Cam
    - Impressores
    - UPS
    - SIP
    - XMPP
    - MQTT
- OT SCADA
    - HTTP
    - FTP
    - TFTP
    - MODBUS
    - S7COMM
    - IPMI
    - Ethernet/IP
    - DNP3
    - Triconex

- Permetre personalitzar o configurar a mida els honeypots (Windows/Linux) per actuar com un equip més (pero sent un parany), permetent accions com unirse a un AD, fer servir

BBDD pròpies amb dades, aplicacions i servidors Web, servidors d'arxius, servidors SCADA, etc.

Requeriments de instal·lació i posada en servei

La solució proposada per donar compliment a aquesta licitació (subministrament, instal·lació i posada en servei de solució de PAM i deception), ha de ser un projecte "claus en mà", això vol dir que s'ha d'incloure:

- Subministrament i instal·lació de tot el maquinari virtual requerit, realitzar la instal·lació i configuració adient de tot el programari necessari.
  - Tant en la part de PAM com deception, s'ha de poder-se desplegar-se en els entorns virtuals locals i Cloud més comuns (vmware, hyprevisor, Azure, AWS, etc.)
  - Per la part de PAM, donada la criticitat d'aquest tipus de sistemes de gestió de credencials de recursos crítics:
    - S'ha disposar d'alta disponibilitat la solució entregada
    - La plataforma ha de poder permetre mínim configuració de clúster actiu/passiu.
    - Addicionalment, si es permet configurar més de 2 equips, el tercer, s'hauria de poder considerar 'Disaster Recovery' estant instal·lat/configurat en una ubicació remota (amb nivell 3 diferent que la resta del clúster).

- S'hauran d'incloure totes les llicencies per complir els requeriment definits al llarg d'aquest document així com el suport del fabricant pel període de durada del contracte (3 anys).
  - Per la part del PAM, s'han de poder gestionar un mínim de 65 comptes privilegiades, i aquestes poden ser d'usuaris interns o proveïdors (amb les mateixes condicions).
  - Per la part de deception, s'han de poder crear i gestionar de manera complerta mínim 2 honeypots.

- S'hauran d'efectuar proves/demostracions de funcionament, rendiment i operativitat per tal de poder validar l'acceptació de la instal·lació i del projecte per part de FGC.

- El projecte s'entregarà a punt per operar-lo. S'entregarà una guia d'operació complerta.

- S'haurà de realitzar una fase de formació i traspàs de coneixements. Aquesta formació s'haurà de fer en dos vegades per tal de cobrir tot el personal assistent.

- S'entregarà documentació complerta de tot el projecte (arquitectura dissenyada, implementació feta, configuració detallada realitzada als equips, regles de seguretat aplicades, etc.).

Roadmap de desplegament i tasques

Com a guia de les tasques que s'han d'anar complimentant dintres de la planificació que es proposa tenim el següent:

1. Planificació	
OBJECTIU	**Establir els fonaments del projecte i definir els requisits tècnics i funcionals.**
ACTIVITATS A REALITZAR DURANT LA FASE	
1. DISSENY DEL PROJECTE	Definir clarament els objectius del projecte, l'abast i els lliurables.
	Establir un cronograma detallat de tasques, amb dates de lliurament per a cada fase.
	Assignar responsabilitats clares als membres de l'equip del projecte i establir una cadena de comunicació eficaç entre totes les parts implicades.
	Establir les prioritats del projecte segons els actius més crítiques que requereixen un accés privilegiat.
2. AUDITORIA PRÈVIA DE COMPTES PRIVILEGIATS	Realització d'una auditoria exhaustiva per identificar tots els comptes privilegiats existents en els sistemes de FGC. Això inclou comptes de superusuari, administradors de sistema, bases de dades, aplicacions crítiques, etc. Analisi i proposta de eina deception segons millor convingui a FGC.
	Anàlisi de les bases de dades de comptes i permisos per garantir que només les persones autoritzades tinguin accés a recursos crítics.
	Identificació de possibles riscos derivats de comptes obsolets o no controlats.
3. DISSENY DE L'ARQUITECTURA DE LA SOLUCIÓ PAM	Establir quines solucions seran necessàries, així com les eines complementàries per a la integració (IAM, SIEM, etc.).
	Crear un model d'arquitectura detallat que inclogui les eines i components que es desplegaran per a la gestió d'accés privilegiat (per exemple, bastionament de servidors, rotació de contrasenyes, etc.) i l'eina de deception.
	Determinar la infraestructura necessària per al desplegament, com servidors, emmagatzematge, xarxes i connexions segures.
LLIURABLES (com mínim)	• Document de disseny del projecte • Informe d'auditoria de comptes privilegiats • Proposta de desplegament de honeypots • Pla d'arquitectura de la solució PAM i decepcion

2. Execució	
OBJECTIU	**Implementar la solució en entorns pilot i escalar a la producció.**
ACTIVITATS A REALITZAR DURANT LA FASE	
1. PREPARACIÓ DE LA INFRAESTRUCTURA	Configuració dels sistemes que donaran suport a la solució PAM i deception, incloent-hi la preparació d'entorns (servidors, bases de dades, xarxes).
	Instal·lació de la solució PAM en un entorn de prova per validar la seva integració amb els sistemes existents. Instal·lació de la solució deception en un entorn de prova per validar la seva integració amb els sistemes existents.
	Configuració de les interfícies d'integració amb altres eines de seguretat com IAM, SIEM o Active Directory, segons sigui necessari.
2. DESPLEGAMENT PILOT	Seleccionar un grup reduït de sistemes o usuaris (per exemple, un departament o grup de treballadors amb privilegis crítics) per provar la solució PAM i deception en un entorn controlat.
	Configurar l'accés privilegiat per al grup pilot, incloent-hi la rotació de credencials i l'autenticació multifactor (MFA).
	Validar que la solució PAM realitza una gestió eficaç dels comptes privilegiats, amb auditories i alertes de seguretat funcionant correctament. Validar que la solució deception desplegada es operativa i simula realment un entorn productiu.
	Realitzar proves de seguretat, com la detecció d'accés no autoritzat, per garantir que la solució ofereix la protecció desitjada. Realitzar proves de intrusió en la eina de deception.
3. DESPLEGAMENT COMPLET	Ampliar la implementació de la solució PAM a tots els usuaris demanats, incloent-hi tots els sistemes i comptes que necessiten una gestió d'accés privilegiat. Desplegar tots el honeypots contractats.
	Configuració final de l'eina PAM per garantir una rotació automàtica de contrasenyes, controls de MFA i monitorització en temps real dels accessos privilegiats. Configuració final de l'eina de deception i garantir alertes i monitoreig.
	Ajustar els permisos d'usuari per garantir que només les persones autoritzades tinguin accés als sistemes crítics.
LLIURABLES (com mínim)	• Informe de preparació d'infraestructura • Informe de desplegament pilot

	• Informe de desplegament

3. Seguiment i Control	
OBJECTIU	**Monitoritzar el rendiment de la solució, assegurar la seva correcta implementació i adaptar-la a les necessitats de seguretat de FGC.**
ACTIVITATS A REALITZAR DURANT LA FASE	
1. SEGUIMENT DE LA IMPLEMENTACIÓ	Monitoritzar contínuament l'activitat dels comptes privilegiats per detectar anomalies o accessos no autoritzats. Monitoritzar el correcte funcionament dels honeypots desplegats.
	Analitzar les alertes generades pel sistema PAM i honeypots i identificar possibles incidents o vulnerabilitats.
	Realitzar auditories periòdiques per verificar que la solució segueix les millors pràctiques i les polítiques de seguretat de FGC.
2. GESTIÓ i ADMINISTRACIÓ	Revisar i ajustar les polítiques d'accés privilegiat per adaptar-les a canvis en l'organització o l'estructura tecnològica.
	Configurar els mecanismes d'automatització (rotació de contrasenyes, accessos temporals, etc.) per garantir l'eficiència del sistema i minimitzar la intervenció manual.
	Establir un procés de revisió periòdica de permisos per garantir que no hi hagi comptes privilegiats obsolets o no autoritzats.
3. PLA DE CONTINGÈNCIA	Crear i validar un pla de recuperació de desastres per garantir la disponibilitat de la solució PAM en cas de fallades o incidents.
	Establir mecanismes de resposta ràpida en cas d'incidents, com el bloqueig automàtic de comptes compromesos o l'aïllament de sistemes vulnerables.
LLIURABLES (com mínim)	• Informe de seguiment de la implementació • Pla de gestió i administració • Pla de contingència i recuperació de desastres

4. Tancament i pas a manteniment	
OBJECTIU	**Formalitzar la implementació de la solució i garantir que la solució sigui efectiva a llarg termini.**
ACTIVITATS A REALITZAR DURANT LA FASE	
1. DOCUMENTACIÓ FINAL	Crear documentació tècnica detallada de la solució PAM i deception, incloent-hi guies operatives, manuals d'administrador, procediments de

	seguretat i informes d'auditoria.
	Incloure un pla de gestió per a l'administració contínua de la solució PAM i deception, així com recomanacions per a l'optimització futura.
	Lliurar un informe de tancament del projecte, detallant els resultats, les lliçons apreses i les possibles millores per a futures implementacions.
2. FORMACIÓ	Proporcionar un pla de formació a l'equip de seguretat, administradors i usuaris amb accés privilegiat, assegurant que tots els implicats comprenguin les seves responsabilitats i l'ús correcte de la solució PAM i deception.
	Incloure una formació pràctica sobre la gestió de les eines, l'autenticació multifactor (MFA) i l'administració de permisos.
3. TRANSFERÈNCIA DE CONEIXEMENT I SUPORT POST-IMPLEMENTACIÓ	Realitzar un pla de transferència de coneixement a l'equip intern de FGC per garantir que poden mantenir i gestionar la solució PAM de manera independent.
	Passar la solució a manteniment, incloent-hi actualitzacions, millores de seguretat i suport en cas de necessitar assistència tècnica.
LLIURABLES (com mínim)	• Manual d'administrador que inclou instruccions detallades sobre la gestió de la solució PAM i deception. • Guia operativa sobre l'ús correcte de la solució i recomanacions per mantenir la seguretat a llarg termini. • Informe de tancament del projecte • Pla de formació

La previsió i possible estimació en temps del projecte es la següent, tot i que pot estar subjecta a canvis aprovats per FGC:

Fase	Duració	Mes	Setmana
Planificació	4 setmanes	Mes 1	Setmanes 1-4
Execució	8 setmanes	Mesos 2-4	Setmanes 5-12
Seguiment i Control	4 setmanes	Mes 5	Setmanes 13-16
Tancament	4 setmanes	Mes 6	Setmanes 17-20

Equip de treball

L'equip de treball que es considera imprescindible per a assolir aquest projecte amb èxit per a FGC, és el que es detalla a continuació:

Equip professional	Coneixements i experiència acreditables
Un Coordinador del Projecte Un tècnic de nivell 2 pel procés d'instal·lació i configuració del equips Un tècnic de Nivell 3 especialista en tecnologia de Ciberseguretat	**- Experiència de l'equip:** 10 anys d'experiència en el sector de la ciberseguretat - Titulació universitària de grau superior en informàtica o titulació d'enginyer (grau en enginyeria) o titulació universitària que asseguri la competència en la matèria, o titulació homologada a l'estat espanyol. **- Certificacions tècniques mínimes (o equivalents):** PMP (Project Management Professional) ECC – CEH (Certified Ethical Hacker) CompTIA Security+

Requeriments de suport i manteniment

L'adjudicatari, donarà un suport especialitzat que contemplarà coma mínim les següents tasques durant tota la durada del contracte:

- Resoldre consultes o incidents relacionats amb l'operació i administració dels dispositius de seguretat subministrats que puguin sorgir. S'haurà d'ajudar a resoldre dubtes d'administració sobre les funcionalitat dels equips objecte d'aquest contracte, així com donar suport necessari en cas d'incidència que requereixi coneixement expert sobre la tecnologia i/o el fabricant.
- Donar suport, resoldre dubtes i aconsellar en les tasques de manteniment i actualitzacions a realitzar als equips.
- Realitzar les actualitzacions periòdiques recomanades pel fabricants (un o dos, segons solució proposada).

Per tal de poder requerir suport especialitzat a l'adjudicatari, aquest haurà de proporcionar una eina de tiquets, portal web o procediment per tal de garantir la correcta gestió i resposta sobre els incidents o consultes realitzades. Periòdicament l'empresa adjudicatària enviarà un informe del número d'incidents, peticions i consultes gestionades, en quin estat es troben i agrupades per severitat/criticitat durant el període d'enviament definit.

L'equip que es requereix perquè durant tota la durada del contracte doni el suport especialitzat de configuracions, resolució de consultes i problemes, així com el manteniment de les versions recomanades pel fabricant ha te complir el següents requeriment:

Equip professional del servei continu	Coneixements i experiència acreditables de l'equip del servei continu
Servei Certificat en ENS categoria Alta Nivell de partnership alt amb el fabricant/fabricants de la solució proposada	2 x Certificacions oficials del fabricant/fabricants ofertat en el seu nivell expert 2 x Certificacions oficials del fabricant/fabricants ofertat en el seu nivell professional 4 x Certificacions oficials del fabricant/fabricants ofertat en el seu nivell bàsic

Per al correcte compliment del servei, s'estableixen els següents SLA's que s'han de complir durant tota la durada del contracte:

Atenció incident:

Nivell de Severitat	Resposta
CRÍTIC	30 min
ALT	60 min
MIG-BAIX	90 min

Resolució de l'incident:

Nivell de Severitat	Resposta
CRÍTIC	4 hores
ALT	8 hores
MIG-BAIX	72 hores

Actualitzacions:

Nivell de Severitat	Resposta
CRÍTIC (CVSS: 9/10)	4 hores

ALT (CVSS: 7/8.9)	8 hores
MIG-BAIX (6.9/0)	72 hores

Catalogació:

Nivell de Severitat	**Definició**
CRÍTIC	Incidències que impliquen tall de Servei.
ALT	Incidències que impliquen degradació de Servei.
MIG-BAIX	Incidències amb impacte al Servei.