Junta de Andalucía
Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa
Sociedad Andaluza para el Desarrollo de las Telecomunicaciones (SANDETEL)

# PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN POR PARTE DE LA SOCIEDAD ANDALUZA PARA EL DESARROLLO DE LAS TELECOMUNICACIONES S.A. (SANDETEL) DEL SERVICIO DE CONSULTORÍA, INSTALACIÓN, IMPLANTACIÓN E INTEGRACIÓN DE UNA SOLUCIÓN PARA LA GESTIÓN DE ACCESO PRIVILEGIADO PAM (PRIVILEGED ACCESS MANAGEMENT) (EXPT23-00036)

## Definiciones, abreviaturas y acrónimos

- **CC**: Common Criteria o Criterio Común.
- **CCN-CERT**: Centro Criptológico Nacional.
- **CPSTIC**: Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones.
- **EAL**: Evaluation Assurance Level o Nivel de Garantía de Evaluación.
- **ENS**: Esquema Nacional de Seguridad
- **EPP**: Endpoint Protection Platform o Plataforma de protección de puntos finales.
- **NIAP**: National Information Assurance Partnership o Asociación Nacional de Aseguramiento de la Información
- **RFS**: Requisitos Fundamentales de Seguridad
- **SFR:** Security Functional Requirements

# 0 INTRODUCCIÓN

El presente documento es el Pliego de Prescripciones Técnicas (en adelante referido como Pliego) para determinar las condiciones para la contratación del suministro, instalación, configuración, integración y puesta en marcha de una plataforma para la Gestión de acceso privilegiado (PAM, Privileged Access Mangement) en la modalidad "Software As A Service" que permita tanto proteger la infraestructura y aplicaciones, como gestionar de manera eficiente y mantener la confidencialidad de los datos sensibles y la infraestructura crítica de **Sandetel y de la Agencia Digital de Andalucía**.

**Sandetel y la Agencia Digital de Andalucía,** como parte de su estrategia de seguridad, desean dotarse de una herramienta que proteja sus sistemas críticos y proporcione una capa de seguridad informática fundamental para proteger los datos, la infraestructura y los activos de toda la organización junto con sus procesos. Adicionalmente debe proporcionar nuevos mecanismos para proteger los recursos TI contra los ciberataques que aprovechan los privilegios internos para atacar los activos más importantes de ambas organizaciones.

El presente documento establece todos los requisitos necesarios exigidos al producto de la familia de Gestión de acceso privilegiado (PAM, Privileged Access Management) en la modalidad "Software As A Service" a cumplir para satisfacer las necesidades de **Sandetel y la Agencia Digital de Andalucía.**

# 1 OBJETO DEL PLIEGO

El objeto del contrato es la contratación del suministro y mantenimiento de una plataforma para la Gestión de acceso privilegiado (PAM, Privileged Access Mangement) en la modalidad "Software As A Service" .

Se trata de contratar el derecho de uso de una plataforma de Gestión de acceso privilegiado, en modalidad "Software As A Service" (en adelante SaaS). Se incluirá la Instalación, configuración, integración y puesta en marcha de la plataforma de Gestión de acceso privilegiado (PAM, Privileged Access Management) así como el mantenimiento correctivo y evolutivo de la propia plataforma ofertada y el soporte técnico de la misma para proteger tanto la infraestructura y aplicaciones, como gestionar de manera eficiente y mantener la confidencialidad de los datos sensibles y la infraestructura crítica de Sandetel, la Agencia Digital de Andaluacía y otros organismos de Junta de Andalucía.

- Establecer las características mínimas de seguridad que sirvan de referencia.
- Establecer por parte de Sandetel como responsable de la adquisición los criterios de evaluacion consistentes y técnicamente adecuados, que permitan contrastar la eficacia de la herramienta Gestión de acceso privilegiado (PAM, Privileged Access Management). y proporcionar información no sesgada acerca de los servicios de seguridad requeridos en la adquisición.
- Establecer los criterios que garanticen que la herramienta gestión de acceso privilegiado (PAM, Privileged Access Management). cumple su finalidad desde el punto de vista de la seguridad.

Para ello, la herramienta de Gestión de acceso privilegiado (PAM, Privileged Access Management) debe:

- Disponer de evaluaciones completas, consistentes y técnicamente adecuadas, que permitan contrastar la eficacia y proporcionar información no sesgada acerca de los servicios de seguridad que ofrece el producto.

- La herramienta de Gestión de acceso privilegiado (PAM) debe proporcionar un acceso con alto nivel de permisos a los recursos TI de la organización. Las cuentas gestionadas por el producto de Gestión de acceso privilegiado (PAM) pueden corresponder a una persona física o a cuentas que utilizan las aplicaciones para ejecutar servicios o comandos que requieren permisos especiales, permitiendo gestionar aplicaciones, software o recursos hardware.

- Debe garantizar la protección y el control de los accesos a las cuentas privilegiadas que administran activos y datos críticos, junto con la necesidad de seguir dando a usuarios, aplicaciones y administradores la flexibilidad necesaría para realizar las tareas diarias.

- La solución debe prevenir del potencial uso indebido de cuentas privilegiadas en los sistemas, dispositivos y aplicaciones TI de la organización, permitiendo administrar y monitorizar el uso de estas cuentas por parte de los usuarios.

- El producto a adquirir motivo de la licitación debe estar catalogado dentro de la familia Gestión de acceso privilegiado (PAM, Privileged Access Mangement) conforme a lo definido por el Centro Criptológico Nacional en el documento Guía de

Seguridad de las TIC CCN-STIC 105 de Noviembre de 2022 y se requiere que los usuarios finales posean una guía que facilite y garantice el uso apropiado del producto desde el punto de vista de la seguridad.

Para ello se requiere la ejecución por parte del adjudicatario, de como mínimo, las siguientes tareas:

- **Suministro, instalación, configuración, integración y puesta en marcha de una herramienta de gestión de acceso privilegiado (PAM, Privileged Access Management)** según los requisitos establecidos en este pliego.

- La oferta ha de detallar, sus características y componentes. El proveedor ha de proporcionar todo los elementos necesarios software para la puesta en marcha completa de la solución, incluyendo las licencias necesarias.

- **Mantenimiento y soporte correctivo** del software y licencias suministrados, incluyendo la gestión de incidencias, actualizaciones y generación de informes de estado.
  - Servicio de mantenimiento, soporte y mejoras.
  - Servicio de atención a incidencias y soporte técnico
  - Servicio de actualización del software
- **Configuración inicial y configuración avanzada** del software, que permita la puesta en explotación.
- **Servicios de soporte avanzado**, incluyendo consultoría sobre nuevas tecnologías, pruebas y verificación de la herramienta
- **Pruebas a ejecutar y validaciones del funcionamiento** de la herramienta, a realizar tanto en periodo de valoración de ofertas (sobre el diseño presentado), como previo a la puesta en explotación y durante la fase de ejecución del proyecto. Cualquier problema detectado sobre el incumplimiento de los requisitos solicitados podrá ser motivo de resolución del expediente.
- **Servicios de valor añadido** imputable a bolsa de horas, tanto de asistencia técnica como de capacitación.
- **Capacitación técnica y transferencia de conocimientos** relativa a la administración y operación de la solución.
- **Garantía técnica** del software y licencias suministradas, una vez finalizado el contrato.

- **La oferta ha de recoger las características mínimas de seguridad** que sirvan de referencia para su evaluación.

Los objetos anteriores deberán cumplir con las características técnicas y funcionales mínimas que se indican en los próximos apartados.
La presentación de una oferta en respuesta a este pliego de prescripciones técnicas por parte de los licitadores presupone la aceptación de todos los requerimientos incluidos en este documento.

La adjudicación de la herramienta en el presente expediente se enmarca dentro del conjunto de encargos encomendados a SANDETEL, principalmente por parte de la AGENCIA DIGITAL DE ANDALUCÍA así como de otros organismos de la Junta de Andalucía.

## 2 SITUACIÓN ACTUAL

En la actualidad **Sandetel y la Agencia Digital de Andalucía** disponen de un conjunto heterogéneo de repositorios, sistemas y servicios relacionados con la gestión de identidades (a destacar, Active Directory, LDAP, entre otros).

Por este motivo, se requiere disponer de un único sistema integrado y homogéneo de gestión de accesos de los usuarios con acceso a los sistemas de información. En ese sentido se ha tomado la decisión de implantar una solución de gestión de accesos (PAM) que permita pasar del modelo actual descentralizado a un modelo centralizado.

Teniendo en cuenta esto, la solución que se presente deberá integrarse completamente con el actual LDAP corporativo, que servirá de base de datos de todos los usuarios potenciales a integrar dentro de la solución PAM.

Debido al aumento del uso de técnicas OSINT (inteligencia de fuentes abiertas) para la recopilación de información por parte de ciberdelincuentes y ciberespias, es necesario limitar la información de activos e infraestructura interna que se ofrece de manera pública, por tanto la información especifica acerca de la descripción de la versión del LDAP corporatvo de la Junta de Andalucía se entregará a las empresas licitadoras que así lo soliciten, entendiendo que este dato es primordial para garantizar la total integración con este. La solicitud de dicha documentación deberá realizarse mediante petición formal al organismo de contratación de la Junta de Andalucía mediante la cuenta de correo licitaciones.sandetel@juntadeandalucia.es

Este nuevo paradigma conllevará también un trabajo complementario de redefinición de la política corporativa en materia de gestión de identidades y privilegios de acceso a los sistemas de información.

A grandes rasgos la implantación de la solución de gestión de accesos pretende alcanzar, al menos, los siguientes objetivos y mejoras en la gestión de las TIC:

- Disponer de un único repositorio común a todas las identidades y sus respectivos atributos (roles, permisos, entre otros) que permita centralizar la gestión de accesos.
- Revisión y redefinición (simplificar y normalizar) de los distintos roles de usuarios, así como de los privilegios de acceso asociados a éstos en función de sus funciones y necesidades.
- Protocolización de los flujos de petición y de aprobación asociados a la gestión de usuarios en lo se que requiere a la gestión de accesos privilegiados.
- Aplicación inmediata y automática de los cambios de asignaciones de roles y perfiles, y por consiguiente de los privilegios asociados.

- Reducción de costes e incidencias debido a la automatización del proceso de aplicación de los privilegios en los distintos servicios, aplicaciones, servidores, elementos de red, etc.
- Minimizar los riesgos derivados de accesos no autorizados como consecuencia de asignaciones erróneas de privilegios, bajas de usuarios no gestionadas, entre otros.
- Disponer de información detallada que permita una trazabilidad exhaustiva de las modificaciones de roles/privilegios de usuarios sobre las acciones realizadas por los usuarios.
- Auditoria de accesos y control de cambios no permitidos. Disponer de registros o "grabaciones" de las acciones realizadas en las sesiones establecidas por los usuarios privilegiados.

Las solicitudes de alta, baja, modificación u otras, así como los privilegios de acceso sobre usuarios, deberán realizarse a través de la propia solución de gestión de accesos.

# 3 ESPECIFICACIONES

Estos requisitos representan las capacidades de seguridad mínimas que cualquier producto dentro de la familia de herramientas de Gestión de acceso privilegiado (PAM, Privileged Access Management) debe implementar, independientemente del fabricante y la tecnología, con el fin de proporcionar un nivel mínimo de confianza para considerarse objetivamente cualificado desde el punto de vista de la seguridad para ser empleado en los sistemas de información del sector público a los que es de aplicación el Esquema Nacional de Seguridad (ENS) Categoría MEDIA.

Estos requisitos aportan mecanismos enfocados a reducir vulnerabilidades y contrarrestar amenazas, fundamentalmente de carácter técnico, aunque también pueden ser de naturaleza física o procedimental.

## 3.1 Especificaciones técnicas de la solución

En los sucesivos apartados se enumeran las especificaciones técnicas mínimas que la herramienta de Gestión de acceso privilegiado (PAM) debe satisfacer.

a) **Almacén seguro de credenciales**, que preserva la confidencialidad e integridad de las credenciales asociadas a las cuentas privilegiadas, y las protege de accesos no autorizados.

b) **Control de acceso** a los recursos TI gestionados a través de las cuentas privilegiadas, basado en las políticas establecidas por Sandetel y la Agencia Digital Andaluza y/o configuradas por el administrador PAM.

c) **Implementación automática (Enforcement) de la política de contraseñas**, permitiendo generar, actualizar, rotar y mantener de forma automática, las contraseñas y otras credenciales de las cuentas privilegiadas.

d) **Descubrimiento automático de cuentas privilegiadas** existentes en los sistemas, dispositivos o aplicaciones de la organización, y que puedan no haber sido declaradas.

e) **Seguridad basada en roles** para grupos de usuarios que requieren el mismo nivel de acceso.

f) **Registro y monitorización de sesiones en tiempo real**, permitiendo registrar y supervisar la actividad de las sesiones de cuentas privilegiadas, incluyendo las acciones y comandos ejecutados.

## 3.2 Especificaciones funcionales de la solución

A continuación, se indican las funciones mínimas requeridas :

- **Gestor de Conexiónes:** debe permitir al recibir la solicitud de conexión por parte de los usuarios, y una vez se haya realizado la evaluación de la solicitud de conexión y sea aceptada la solicitud, establecer la conexión con el recurso TI en nombre del usuario, sin necesidad de que este conozca las credenciales privilegiadas.

- **Gestor Central:** Una vez se hayan evaluado las solicitudes de conexión de los usuarios de acuerdo con la política de seguridad vigente, permitirá rechazar o aceptar la conexión.

- **Gestor de Políticas:** debe permitir procesar las directivas procedentes de las políticas de seguridad corporativas y aplicables a las cuentas privilegiadas que gestiona con capacidad de " Policy Enforcement ", aplicando de forma automática políticas de rotación y actualización de contraseñas sobre los recursos TI.

- **Gestor de Auditoría:** que permita no solo generar registros de auditoría con los eventos de seguridad relevantes del sistema, sino que también monitorice y "grabe" las actividades que ocurren durante la sesión privilegiada, para proporcionar posteriormente una reproducción de las sesiones a los administradores autorizados. Los registros generados pueden almacenarse en un almacén de auditoría propio, o bien enviarse a un servidor de auditoría externo.

- **Gestor de Configuración:** que permita a los administradores configurar, administrar y monitorizar las políticas de seguridad, cuentas privilegiadas y, en general, todas las funciones de gestión y administración del producto. El acceso local y/o remoto a este gestor de configuración se realiza, en algunos casos, a través de interfaces de gestión.

- **Gestor de Descubrimiento:** que permite descubrir de forma automática nuevas cuentas privilegiadas en los recursos TI gestionados.

- **Gestor o Comandos:** que permite realizar un control de acceso a los recursos TI no solo a nivel de sesión, sino a nivel de comando privilegiado. Esto permite que los usuarios puedan ejecutar ciertos comandos y realizar tareas privilegiadas con su propia cuenta personal, sin necesidad de elevar sus privilegios (least privilege).

- **Gestor de Aplicaciones:** que permita facilitar el acceso privilegiado que algunas aplicaciones software requieren a ciertos recursos TI, sin necesidad de introducir las credenciales privilegiadas en el código de la aplicación o script.

- **Interfaz Web, clientes, software específico** para establecer las conexiones de administración remotas, y las conexiones de los usuarios privilegiados.

- **Doble factor de autenticación** de acceso al Interfaz Web de la solución PAM facilitando un método de control de acceso informático en el que a un usuario se le concede acceso al sistema solo después de que presente dos o más pruebas diferentes de que es quien dice ser.

- **Almacén seguro de credenciales** mediante un almacenamiento seguro para las credenciales privilegiadas de los sistemas TI gestionados. Estas credenciales no se deberán nunca almacenar en texto claro, sino que irán protegidas con algún mecanismo criptográfico.

- **Almacén seguro de registros de auditoría** mediante un almacenamiento seguro para los registros de auditoría, tanto los correspondientes a los eventos de seguridad del propio sistema, como los registros o "grabaciones" de las acciones realizadas en las sesiones establecidas por los usuarios privilegiados.

- **Gestión de Backup** de toda la información necesaria para el restablecimiento de la solución completa ante cualquier incidencia.

Adicionalmente a las especificaciones descritas en este apartado, se podrá requerir al integrador la realización de una auditoría de seguridad (ya sea en primera persona con medios propios o a través de un tercero) de la infraestructura que soporta el servicio. Esta auditoría deberá incluir un análisis de vulnerabilidades y pruebas de penetración, reflejando los resultados en un informe entregable a Sandetel, y del que extraiga el cumplimiento con lo establecido por el Esquema Nacional de Seguridad (ENS) Categoría MEDIA.

# 4 REQUISITOS

En este apartado se indican algunas condiciones generales y específicas que se requieren en el entorno operativo en el que se va desplegar el producto, para garantizar su seguridad:

**a) Plataforma fortificada (hardened) y compatible:** en el caso de productos software, las plataformas hardware en las que se instale el producto deberán ser perfectamente compatibles y deben tomarse las medidas de seguridad adecuadas de fortificación para que la instalación del producto no se vea comprometida a nivel de seguridad.

**b) Entidades de terceros confiables:** en el caso de que el producto intercambie información de identidades o atributos con entidades de terceros, estas deberán ser confiables.

**c) Actualizaciones periódicas:** El producto será puesto al día conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas. También se contempla dentro del soporte la habilitación de acceso a las actualizaciones, parches y subidas de versiones software, con objeto de mejorar las prestaciones y funcionalidades o de corregir errores existentes en versiones anteriores.

**f) Se deben incluir los siguientes servicios internos** en caso de que el producto los requiera para que el entorno operacional esté completamente funcional, dentro de la red interna en la que se despliega el producto, como pueden ser:

- Servidor de credenciales (p.e Directorio Activo).
- Servidor de Auditoría.
- Fuente de tiempo fiable (reliable timestamp).
- Servidor de políticas corporativas.
- Servidor de identidades.
- Primitivas criptográficas.

## 4.1 REQUISITOS GENERALES

**Req. 1.** Solución basada en software en modelo SaaS.

**Req. 2.** La solución contará con un único entorno, que será el de producción. Cualquier otro entorno facilitado no será facturable

**Req. 3.** Solución en modalidad de alta disponibilidad en el entorno de producción.

**Req. 4.** Solución funcional desde cualquier dispositivo. (Windows, Linux, Mac, Android o IOS).

**Req. 5.** Solución basada en entorno web.

**Req. 6.**Solución compatible con la mayoría de navegadores (como mínimo Explorer, Edge, Chrome, Firefox y Safari) a la última versión disponible del mercado.

**Req. 7.** Solución basada en estándares y/o con posibilidad de integración (API, SDK, entre otros) con otros módulos/servicios, propios o de terceros, relacionados con la gestión de accesos y el control de accesos:

- Integración con LDAP
- Integración con difrentes sistemas MFA
  - TOTP
  - Radius

- Fido2
- Email Code
- DUO
- Otros

- Integración sistemas RPA
  - Acceso
  - Auditoría
- Integración API/Webservices
- Integración con soluciones de análisis de vulnerabilidades
- Integración SIEM
  - Syslog
- Integración con otras tecnologías
  - Soluciones Sandbox (mínimo Fireeye, Palo Alto, Checkpoint)
  - Soluciones Splunk

## 4.2 REQUISITOS FUNCIONALES

En este apartado se definen los requisitos funcionales, en distintos ámbitos, que como mínimo, debe satisfacer la solución de gestión de accesos:

### APROVISIONAMIENTO DE ACCESOS:

**Req. 8.** Gestión completa del ciclo de vida de la gestión de accesos: altas, bajas, modificaciones, autorizaciones, entre otros.

**Req. 9.** Gestión de los accesos en función de la estructura jerárquica y funcional.

**Req. 10.** Definición de distintos roles y privilegios en materia de gestión de accesos.

**Req. 11.** La solución debe permitir distintos flujos (solicitudes, autorizaciones, por ejemplo) siendo estos configurables en función de determinadas características de la identidad y la acción a realizar (alta, baja, modificación, entre otros).

**Req. 12.** Sincronización automática de accesos en los distintos repositorios de identidad corporativos.

**Req. 13.** Sincronización automática de la gestión de acceso para las identidades en los distintos repositorios corporativos de control de acceso.

### GESTIÓN DE ROLES/PRIVILEGIOS:

**Req. 14.** La solución debe permitir la gestión, entre otros, de atributos a nivel de gestión de accesos.

**Req. 15.** Gestión completa del ciclo de vida de los roles: altas, bajas, modificaciones, por ejemplo. Incluye la asignación de los correspondientes recursos/productos/aplicaciones/servicios a roles y la asignación de roles a identidades.

**Req. 16.** Definición de distintos roles y privilegios en materia de gestión de roles (usuarios autorizados a cursar solicitudes en función de su ámbito funcional, usuarios visadores/aprobadores dependiendo del ámbito funcional, usuario administrador de la solución, entre otros).

**Req. 17.** Sincronización automática de la asignación a identidades de los roles en los distintos repositorios corporativos de control de acceso.

**Req. 18**. Procesos de reconciliación de identidades con objeto de identificar cuentas sin correspondencia en los sistemas corporativos de control de acceso y/o cuentas sin uso.

## GESTIÓN DE CONTRASEÑAS:

**Req. 19.** Configuración de las políticas de las contraseñas. Como mínimo deberá permitir la configuración de las siguientes características:

- Establecer la longitud mínima y máxima
- Composición (forzar la combinación de dígitos, letras mayúsculas/minúsculas y/o caracteres especiales)
- Control de repetición de las últimas 5 contraseñas utilizadas
- Control de secuencias numéricas y/o patrones similares
- Alternativas a la caducidad de las contraseñas

**Req. 20.** Función de bloqueo manual de usuario (administrador de acceso) con la finalidad de bloquear/suspender acceso.
**Req. 21.** Generación aleatoria de nuevas contraseñas (en nuevas altas así como en cambios de credenciales).
**Req. 22.** Funcionalidad de autoservicio.
**Req. 23.** La solución debe admitir la sincronización de secretos con el repositorio principal del Vault (PAM) y la rotación de secretos debe sincronizarse automáticamente.
**Req. 24.** La solución debe proporcionar funcionalidades de one-time password y rotación tras uso.
**Req. 25.** La solución debe proporcionar funcionalidad de doble factor de autenticación.

## AUDITORIA Y REPORTING:

**Req. 26.** Registro (log) cronológico de todas las acciones realizadas sobre una entidad/rol: fecha, hora, usuario, acción (alta, baja, modificación, autorización, asignación de rol, entre otros), detalle del cambio realizado, por ejemplo. Este registro debe ser consultable/exportable.

**Req. 27.** Generación de informes (a modo orientativo):

- relación de recursos/productos/aplicaciones/servicios
- relación de recursos/productos/aplicaciones/servicios por roles
- relación de identidades con acceso a determinados recursos/productos/aplicaciones/servicios resúmenes estadísticos (número de usuarios por roles)

**Req. 28.** Envío de alarmas ante el uso de cuentas no autorizadas o especiales como puede ser la cuenta de Root

## 4.3 REQUISITOS DE INTEGRACIÓN

En este apartado se definen los sistemas a integrar con la solución de gestión de accesos. La solución de gestión de accesos deberá integrarse, como mínimo, con los siguientes sistemas y servicios:

**Req. 29.** Repositorios de identidades:

- Usuarios internos
- Usuarios externos

**Req. 30.** Repositorios de control de acceso (repositorios de identidades/contraseñas):

- Microsoft Active Directory
- LDAP Corporativo
- Otros

**Req. 31.** Aplicaciones de gestión de tareas.

- Herramientas de ticketing tipo JIRA de Atlasisan, Redmine, etc

**Req. 32.** Aplicaciones de registro/auditoria.

**Req. 33.** Otros repositorios de datos

Req. 34. La comunicación entre los usuarios administradores de los servicios y la solución PAM en modelo SaaS deberá establecerse siempre mediante un canal de comunicación privado, para lo cual la adjudicataria deberá facilitar los recursos a nivel de capa de red necesarios que provean un mecanismo o control de seguridad.

**Req. 35.** La solución ha de tener compatibilidad total con los servicios e infraestructuras actuales que identifique Sandetel dentro de los servicios prestados.

Debido al aumento del uso de técnicas OSINT (inteligencia de fuentes abiertas) para la recopilación de información por parte de ciberdelincuentes y ciberespias, es necesario limitar la información de activos e infraestructura interna que se ofrece de manera pública, por tanto la información especifica acerca de las infraestructuras actuales que identifique Sandetel dentro de los servicios prestados se entregará a las empresas licitadoras que así lo soliciten, entendiendo que este dato es primordial para garantizar la total integración con este. La solicitud de dicha documentación deberá realizarse mediante petición formal al organismo de contratación de la Junta de Andalucía mediante la cuenta de correo licitaciones.sandetel@juntadeandalucia.es

## 4.4 REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

A continuación, se recogen los requisitos que debe cumplir el producto de Gestión de cuentas privilegiadas (PAM).

### PERFIL DE PROTECCIÓN COMMON CRITERIA

**Req. 36.** Los productos deberán estar certificados con alguno de los siguientes perfiles de protección o superiores en lo que a versión se refiere si procede de acuerdo a la norma Common Criteria:

| PERFIL DE PROTECCIÓN | | | |
|---|---|---|---|
| **Perfil de protección** | **Versión** | **Fecha** | **Organismo responsable** |
| *Protection Profile for Enterprise Security Management - Identity and Credential Management* [4] | *2.1* | *21/11/2013* | *NIAP* |
| *Protection Profile for Enterprise Security Management - Policy Management* [5] | *2.1* | *21/11/2013* | *NIAP* |
| *Protection Profile for Enterprise Security Management-Access Control* [6] | *2.1* | *12/11/2013* | *NIAP* |

**Req. 37.** En caso de que el producto no esté certificado contra ninguno de los perfiles anteriores, debe disponer de una declaración de seguridad ( Security Target) certificada con un nivel de confianza EAL ( Evaluation Assurance Level) EAL2 o superior. La declaración de seguridad debe implementar los SFR (Security Functional Requirements) apropiados para satisfacer, al menos, los Objetivos de Seguridad que se recogen en la siguiente tabla:

| OBJETIVO | DESCRIPCIÓN |
|---|---|
| [PROTECCIÓN DE LAS CREDENCIALES] | El producto no debe almacenar los datos de credenciales en texto claro y debe protegerlos de accesos no autorizados. |
| [CONTROL DE ACCESO] IDENTIFICACIÓN Y AUTENTICACIÓN | El producto debe identificar de forma única a los usuarios, y autenticarlos antes de permitirles acceso las funciones y datos del producto. |
| [CONTROL DE ACCESO] CONSENTIMIENTO | El producto debe permitir informar a los usuarios sobre el uso no autorizado de la sesión, antes de su establecimiento. |
| [CONTROL DE ACCESO] CONTROL DE SESIONES | El producto debe implementar mecanismos que permitan suspender o denegar el establecimiento de una sesión. |
| [GESTIÓN DE LA SEGURIDAD] FUNCIONALIDAD | El producto debe proporcionar un conjunto de funciones que permitan el control de sus funciones y datos, asegurándose de que solo los usuarios con los privilegios adecuados (administradores) puedan ejercer dicho control. |
| [GESTIÓN DE LA SEGURIDAD] PERMISOS | El producto debe permitir la definición de perfiles de administración (*roles*), y la asignación de distintas funciones de gestión a cada perfil (*separation of duties*). |
| [PROTECCIÓN DE LAS COMUNICACIONES] | El producto debe proteger la confidencialidad y la integridad de los datos transmitidos entre los componentes del producto, y entre el producto y los administradores u otras entidades IT externas. |
| [AUDITORÍA] REGISTRO DE EVENTOS | El producto debe tener la capacidad de detectar los eventos relevantes de seguridad, y registrarlos adecuadamente en los registros de auditoría. |
| [AUDITORÍA] PROTECCIÓN DE LOS REGISTROS | El producto debe proteger los registros de auditoría almacenados o trasmitidos, de accesos no autorizados. |

## ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

El estándar Common Criteria (CC) proporciona el conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TIC.

- En el ámbito de CC se elaboran unos perfiles de seguridad (Protection Profiles) que definan, para un dominio o categoría de productos, un conjunto de objetivos y requisitos de seguridad, tanto funcionales como de evaluación,independientes de la implantación.

- Los productos dentro de esta familia deberán cumplir con los RFS reflejados en el apartado 4, y con los SFR ( Security Functional Requirements) que se especifican en alguno de los siguientes perfiles de protección, certificados de acuerdo a la norma Common Criteria:

| PERFIL DE PROTECCIÓN | | | |
|---|---|---|---|
| **Perfil de protección** | **Versión** | **Fecha** | **Organismo responsable** |
| *Protection Profile for Enterprise Security Management - Identity and Credential Management* [1] | *2.1* | *21/11/2013* | *NIAP* |
| *Protection Profile for Enterprise Security Management - Policy Management* [2] | *2.1* | *21/11/2013* | *NIAP* |
| *Protection Profile for Enterprise Security Management-Access Control* [3] | *2.1* | *12/11/2013* | *NIAP* |

- En caso de que el producto no esté certificado contra ninguno de los perfiles anteriores o superiores en lo que a versión refiere si es el caso, debe disponer de una declaración de seguridad (Security Target) certificada con un nivel de confianza EAL (Evaluation Assurance Level) EAL2 o superior. La declaración de seguridad debe implementar los SFR (Security Functional Requirements) apropiados para satisfacer, al menos, los Objetivos de Seguridad que se indican en el apartado 4.1.

1. https://www.niap-ccevs.org/MMO/PP/pp_esm_icm_v2.1.pdf
2. https://www.niap-ccevs.org/MMO/PP/pp_esm_pm_v2.1.pdf
3. https://www.niap-ccevs.org/MMO/PP/pp_esm_ac_v2.1.pdf

## 4.5 REQUISITOS DE AUDITORÍA Y MONITORIZACIÓN

**Req. 38.** El producto debe monitorizar y registrar las actividades realizadas por los usuarios durante las sesiones con cuentas privilegiadas.

**Req. 39.** Los registros de auditoría de actividades se almacenarán y deberán ser protegidos de accesos no autorizados mediante el uso de un repositorio adecuado

**Req. 40.** En caso de que estos registros de auditoría de actividades se almacenen de forma remota en un servidor de auditoría externo, deberán ser enviados mediante un protocolo seguro (IPsec, TLS 1.2 o superior, SSH, etc).

## 4.6 REQUISITOS DE MÍNIMO PRIVILEGIO

**Req. 41.** El producto debe tener la capacidad de establecer las sesiones privilegiadas con el recurso TI gestionado, en nombre del usuario, de forma que este no conozca en ningún momento, las credenciales privilegiadas de acceso al recurso.

## 4.7 REQUISITOS DE SOPORTE CRIPTOGRÁFICO

**Req. 42.** En caso de que el producto utilice algoritmos y funciones criptográficas, debe soportar el uso de aquellas aceptadas para nivel Alto del ENS según la guía CCN-STIC-807, así como proporcionar capacidades de configuración que permitan obligar al uso de estos algoritmos exclusivamente.

**Req. 43.** El producto debe usar longitudes de clave que proporcionen una fortaleza equivalente a 256 bits o superior en el que caso de interconexiones e intercambio de información entre todos los elementos integrantes o integrados en la solución PAM.

## 4.8 REQUISITOS MÍNIMOS ANTE AMENAZAS

Los recursos necesarios a proteger mediante el uso del PAM, incluyen:

**a) Datos críticos almacenados:**

- Credenciales que permiten el acceso privilegiado a los recursos TI de la organización, gestionados por el producto PAM.
- Datos de configuración del producto.
- Datos de auditoría relativos a las acciones que el usuario haya llevado a cabo durante la sesión privilegiada, o a las acciones realizadas por los administradores sobre la configuración del producto.
- Claves y otros parámetros críticos de seguridad (Critical Security Parameters, CSPs) utilizados para las funciones criptográficas.

**b) Datos críticos intercambiados entre los distintos componentes del producto, o entre el producto y otras entidades o recursos TI autorizados:**

- Datos de administración, configuración y gestión del producto intercambiados a través de las interfaces de gestión.
- Datos de identidad y credenciales de acceso privilegiado a los recursos TI gestionados.
- Datos de autenticación intercambiados con servidores externos de autenticación (AAA servers).
- Datos de auditoría intercambiados con servidores externos de auditoría (Audit servers).

**c) Recursos TI de la organización a los que los usuarios pueden acceder, a través del producto, con cuentas privilegiadas.**

Como mínimo el producto debe ser capaz de hacer frente contra las amenazas detalladas a continuación:

- **Compromiso de los datos críticos:** un usuario malintencionado puede intentar acceder a los datos críticos almacenados en el producto o transmitidos entre las distintas partes del mismo o con otras entidades externas, para modificarlos, destruirlos u obtener credenciales que podría reproducir para hacerse pasar por otro usuario autorizado.

- **Compromiso de los registros de auditoría:** un usuario o proceso malintencionado puede acceder de forma no autorizada a los registros de auditoría, y provocar la pérdida o la modificación de los mismos, o intentar enmascarar sus acciones, causando con ello que los datos de auditoría se registren incorrectamente o que nunca se registren.

- **Acceso no autorizado:** un usuario malintencionado podría saltarse los mecanismos de identificación, autenticación o autorización del producto para obtener acceso ilícito a sus funciones o recursos.

- **Errores de administración:** un administrador podría instalar o configurar el producto incorrectamente, aunque de forma no intencionada, provocando la falta de efectividad de los mecanismos de seguridad

## 4.9 MONITORIZACIÓN Y ADMINISTRACIÓN

El sistema de gestión de accesso PAM ha de disponer de un software propio y herramientas de monitorización en la que se puedan comprobar los KPI principales con datos históricos de al menos un año de antigüedad, además se deberá incluir el software necesario y sus correspondientes licencias que permita todas las funcionalidades que se exponen a continuación:

- Ha de disponer de herramientas con capacidad de monitorización y diagnóstico del estado y rendimiento de los sistemas.
- Enviar alertas vía correo electrónico, traps SNMP y debe ser monitorizable mediante la herramienta Nagios / Centreon o mediante API
- Ejecutar scripts con comandos externos
- Personalizar las entradas y mensajes de alerta
- Interfaz gráfico y por consola para la administración del entorno
- Posibilidad de examinar con detalle todos los componentes y la actividad del sistema, identificar y resolver cuellos de botella, y conseguir que el sistema tenga un mejor rendimiento.
- Capacidad de envío de alarmas relativas a incidencias de cualquier componente y problemas de rendimiento del sistema.
- Deberá proporcionar un sistema de monitorización con alertas que permitan rápidamente la detección de cualquier problema en el sistema y elementos asociados.
- Se deben establecer las métricas necesarias que se tendrán en cuenta a la hora de aplicar la monitorización de la solución las cuales deberán estar basadas como mínimo en métricas de uso del entorno: consumo de CPU (MHz), consumo de memoria RAM (GB), etc.

### 4.10 SEGURIDAD Y CONFIDENCIALIDAD DE LA SOLUCIÓN

La solución deberá permitir la realización de copias de seguridad y su recuperación acorde con los procedimientos y sistemática establecida por Sandetel.
La responsabilidad en la realización y/o mantenimiento de dichas copias de seguridad, recaerá en el proveedor de Outsourcing contratado.

El sistema de asignación de roles y control de los usuarios administradores, deberá de garantizar la seguridad lógica de la información, eliminando cualquier posibilidad de accesos incontrolados y no autorizados. La solución dispondrá de un modulo de auditoría que permitirá la trazabilidad de las acciones del usuario, en especial aquellas que impliquen mayor riesgo para la integridad de la base de datos.

Durante la fase de personalización de la solución, el equipo de implantación e integración de la empresa adjudicataria, deberá tomar todas las precauciones y medidas necesarias para que el servicio resultante sea robusto, minimizando el riesgo de perdida de integridad.

Todos los miembros de los equipos de implantación, integración y soporte de la empresa adjudicataria están obligados a guardar secreto profesional y estricta confidencialidad sobre toda la información a la que tengan acceso durante el desarrollo del proyecto de personalización y su posterior mantenimiento, por tiempo indefinido desde la finalización del contrato

## 5 SERVICIOS A OFRECER POR EL ADJUDICATARIO

A continuación se indican los requisitos mínimos que deberá cumplir la propuesta del licitador:

Se deberá contemplar una serie de tareas de distinta temática y alcance que se dividen en:

- Suministro, Instalación, configuración, integración y puesta en marcha de la solución de gestión de accesos.

En los siguientes apartados se describen con mayor detalle los trabajos a realizar por el adjudicatario.

### 5.1 ANÁLISIS PREVIO

Se abordará, con carácter general, una revisión y análisis de la política de gestión de accesos actual. Durante esta primera fase de análisis y revisión se mantendrán las reuniones de trabajo que se consideren oportunas con las áreas funcionales y técnicas implicadas, tanto de Sandetel y la Agencia Digital Andaluza como del Proveedor TIC. Sandetel y la Agencia Digital Andaluza facilitará el acceso a la información que en todo momento pueda requerirse.

Fruto de esta fase de revisión y análisis se propondrá el modelo de gestión de accesos más acorde a las particularidades y necesidades de Sandetel y la Agencia Digital Andaluza. Para ello se tendrán en cuenta los aspectos funcionales, organizativos y tecnológicos actuales y futuros de ambas entidades.

También se detallarán las especificaciones técnicas y el diseño de la infraestructura necesaria para la solución de gestión de accesos.

Para ello se tendrán en cuenta, al menos, los siguientes factores:

- El diseño de la solución tendrá en cuenta unas condiciones de explotación de la misma de 24 horas al día y siete días a la semana.
- La solución ha de ser escalable, en términos que permita el crecimiento del sistema de forma horizontal, tanto en número de usuarios como en funcionalidad y volumen de datos.
- Se utilizarán tecnologías y productos contrastados, teniendo en cuenta el resto de productos y tecnologías con los que tendrán que relacionarse.
- El sistema ha de tener capacidad para procesar el número de operaciones requeridas en un tiempo determinado así como realizarlo cuando los usuarios lo requieran.
- El sistema ha de garantizar la continuidad del servicio con un número de operaciones elevado, garantizando la tolerancia del sistema a fallos, sin necesidad de intervención manual y de forma transparente al usuario.
- El sistema estará dimensionado para soportar como mínimo el trabajo de los usuarios que actualmente tienen acceso concurrente a los sistemas de gestión y administración de usuarios y roles garantizando el mismo para un mínimo de 250 usuarios.

## 5.2 PUESTA EN MARCHA

La empresa adjudicataria deberá realizar los siguientes trabajos:

- Configuración del software de gestión de acceso y definición de los parámetros necesarios para su puesta en pleno funcionamiento según las especificaciones de este pliego y las directrices del Director del proyecto.
- Configuración de cualquier otro software que se suministre según las especificaciones de este pliego y las directrices del Director del proyecto.
- Definición del procedimiento a seguir para la migración de los servicios actuales a los nuevos sistemas.
- Con objeto de validar el procedimiento anterior, se ejecutará dicho procedimiento para un caso particular definido por el Director del proyecto. Se deberá poder acceder a sus datos/aplicaciones de la misma forma en la que lo hace con los sistemas actuales.
- La ejecución del procedimiento de migración a este nuevo software que afecte a otros servicios y/o sistemas será realizada por el proveedor, siendo valorable la bolsa de horas ofertada por la empresa adjudicataria para asistencia y así solventar cualquier problema que se presente durante el proceso. En general estas horas se emplearán para tareas de consultoría, configuración, actualización a nuevas versiones, cambios de plataforma y en general cualquier actuación relacionada con la incorporación de los servicios o sistemas.

- El perfil de los técnicos será el adecuado para la ejecución de los procedimientos de migración definidos por la empresa y será Sandetel la que determine las tareas y los períodos de intervención necesarios.

Será condición necesaria para dar por buenas la instalación y puesta en marcha de la herramienta software PAM, la **certificación completa por parte de Sandetel**. Sin esta, se entenderá que aún no se ha concluido y no podrán darse por cerrada.

Sin perjuicio de incluir aquella documentación complementaria que se considere necesaria, se generarán, como mínimo, los siguientes entregables:

- Identificación de las distintas tipologías de usuarios, perfiles, roles y privilegios de acceso actuales y propuesta de modelización/redefinición/simplificación de los mismos.
- Planificación detallada de la ejecución del proyecto que contemple la evolución/transición de la situación actual hacia el modelo futuro basado en la solución de gestión de identidades.
- Inventario de los recursos/productos/aplicaciones/servicios que requieren medidas de control de acceso lógico y sus correspondientes roles asociados.
- Definición de la política de asignación de privilegios por puestos de trabajo, perfiles y roles.

- Documento de instalación del software y sus componentes incluyendo:
  - Una descripción detallada de las versiones de software instaladas y sus componentes.

- Procedimiento de soporte.
  - Medios y recursos disponibles para el soporte.
  - Información relativa al soporte y el software asociado (n.º de contrato, acceso por web, acceso por correo, n.º de teléfono, etc).
  - Horario de atención, tiempos de respuesta, diagnóstico, presencia "in situ" y procedimientos de tramitación de incidencias y consultas, y de descarga de actualizaciones.

- Plan de pruebas del software desplegado
- Durante la ejecución de los trabajos objeto del contrato el adjudicatario deberá facilitar a las personas designadas por Sandetel, la información y documentación necesaria para conocer el desarrollo de los trabajos, así como la actuación ante diferentes incidencias.

- Elaboración de una matriz en la que se detallen los roles de los distintos recursos/productos/aplicaciones/servicios que correspondan en función de los distintos tipos y perfiles de usuario.

- Definición formal y documentación detallada del modelo de gestión de accesos: circuito de gestión de solicitudes, funcionalidades autoservicio, asignación de privilegios por perfiles/roles, entre otros.

- Especificaciones funcionales y técnicas en materia de diseño e integración de la solución de gestión de accesos con los sistemas necesarios. El modelo futuro de gestión de accesos tendrá la consideración de hito del proyecto. Éste será revisado y aprobado formalmente por Sandetel y la Agencia Digital Andaluza.

### 5.2.1 Equipo de trabajo

El adjudicatario designará un Jefe de Proyecto y aportará los recursos humanos y materiales necesarios, para la adecuada prestación de los servicios establecidos en el presente Pliego.
La responsabilidad del Jefe de Proyecto consiste en asegurar la prestación de los servicios indicados y será el interlocutor único entre el adjudicatario y Sandetel. Entre sus responsabilidades estarán:

- Dirigir, representar y coordinar el equipo de trabajo que está prestando los servicios por parte del adjudicatario.
- Atender cualquier tipo de petición por parte del equipo de Sandetel.
- Ser el único interlocutor válido con el equipo de Sandetel.
- Asegurar el nivel de calidad de los trabajos y de la documentación producida, así como garantizar el cumplimiento de los plazos acordados.
- Presentar los resultados de la realización del servicio.

Respecto al equipo de trabajo, estará formado por el Jefe de Proyecto ya mencionado, y por los técnicos y personal necesario que la empresa adjudicataria aporte para la prestación del servicio.

Cabe destacar que no se permitirá que cualquier miembro del equipo de trabajo disponga de dos o más roles asignados. Además, la dedicación de estas personas para el proyecto de esta licitación, deberá ser total y de forma exclusiva dentro de su jornada laboral, evitando su colaboración en otros proyectos de forma paralela.

### 5.2.2 Plazo de ejecución e instalación

El plazo de ejecución para la puesta en marcha de la solución, que dispondrá el adjudicatario, será el siguiente:

La empresa suministradora asegurará la plena operatividad del conjunto una vez instalado.

- Instalación de todo el software para que funcione correctamente según las especificaciones de este pliego y las directrices del Director del proyecto.
- Se garantizará que la solución quedará plenamente operativa para su uso una vez finalizado el plazo de instalación.

Plazo máximo de 4 meses para la entrega de la solución, instalación, configuración, integración, puesta en marcha, realización de la formación y entrega definitiva del proyecto. El cómputo del plazo para ambas tareas, se iniciará a partir de la firma del contrato, es decir, el plazo total NO es acumulativo y ambas tareas deberán trabajarse de forma paralela. Dicho plazo puede quedar interrumpido

en aquellos casos en los que por motivos ajenos al adjudicatario éste no pueda avanzar en las tareas de ejecución del servicio propuesto. Aunque se indica que la planificación se realizará una vez adjudicado el contrato, se valorará la presentación de los diferentes apartados que tendrá dicha planificación y donde como mínimo se indicarán las tareas y subtareas, alcance de cada una de ellas y entregables relacionados. Y la información respecto a los plazos de tiempo implicados. El adjudicatario deberá entregar, a la finalización de la actividad de puesta en marcha de la solución, unos manuales de usuario personalizados para las diferentes tipologías de usuario descritas. Éstos se entregarán en formato digital.

### 5.2.3 Formación

Se debe incluir formación para el personal de Sandetel y la Agencia Digital Andaluza dividida en los siguientes aspectos:

- Administración, parametrización y mantenimiento, al objeto de poder administrar, modificar y/o ampliar las distintas funcionalidades de la solución PAM ofertada.
- Operación de la herramienta que contenga el flujo de trabajo completo de altas, bajas y modificaciones de nuevos usuarios dentro de la herramienta PAM, y del alta de nuevos sistemas hardware dentro del control de la solución PAM.

La formación tendrá una duración mínima de 14 horas para el curso de administración y 7 horas para el correspondiente a operación.

La empresa adjudicataria proporcionará un plan completo de formación desarrollando en detalle el alcance anteriormente citado, todo ello tras la firma del contrato y con carácter previo a su impartición.

Los cursos serán con carácter presencial, si bien SANDETEL y la Agencia Digital Andaluza podrá autorizar de forma extraordinaria la impartición parcial de forma remota.

## 5.3 GARANTÍA, SOPORTE Y MANTENIMIENTO

Las empresas licitadoras deberán presentar en su oferta la metodología del servicio técnico como de atención al cliente para el tratamiento de las incidencias, a partir de su reporte y hasta su finalización. El servicio de mantenimiento deberá contemplar tanto su aspecto correctivo como la asistencia técnica a los usuarios. Para la resolución de incidencias sobre el funcionamiento y procedimientos operacionales que formen parte del proyecto se utilizará la asistencia telefónica o correo electrónico así como cualquier otra comunicación que el licitador provea vía web.

### 5.3.1 Atención técnica al usuario

Se incluirá en la oferta, la atención al usuario vía telefónica, vía e-mail y/o vía remota, en la que se resolverán las dudas que estos pudieran tener acerca del funcionamiento del servicio. La atención al usuario será:

- Funcionamiento del servicio: 24x7, 365 días al año.

- Tiempo de respuesta: El más breve posible con el fin de garantizar la participación del licitador y teniendo en cuenta los plazos estipulados en la tabla adjuntada en el apartado "Incidencias" de este Pliego de Prescripciones Técnicas.
- Tiempo de resolución: El más breve posible con el fin de garantizar la participación del licitador y teniendo en cuenta los plazos estipulados en la tabla adjuntada en el apartado "Incidencias" de este Pliego de Prescripciones Técnicas.

### 5.3.2 Mantenimiento

La empresa adjudicataria deberá mantener actualizada la solución propuesta, conforme a las mejoras o nuevas versiones de la misma. Estas acciones no podrán implicar ningún coste relacionado. La incorporación de estas actualizaciones/mejoras no deberá, en la medida de lo posible, afectar al funcionamiento normal de la solución, por lo que antes de su instalación la empresa adjudicataria garantizará que se realizarán las pruebas oportunas, de manera previa a la incorporación de estas actualizaciones en el servicio.

Dentro del precio de adjudicación del contrato, y durante toda la vigencia del contrato, se incluirá el mantenimiento correctivo así como la asistencia técnica remota o presencial, sin límite de horas, en caso de mal funcionamiento de la solución.

### 5.3.3 Mantenimiento correctivo

El servicio de mantenimiento correctivo incluirá la resolución de aquellos errores específicos de la solución y el posible mal funcionamiento por motivos ajenos a Sandetel y que sean derivados por el diseño, arquitectura, desarrollo, configuración, integración, funcionamiento habitual, por ejemplo, así como de los flujos o desarrollos establecidos por Sandetel y que hayan sido implementados por el adjudicatario. Los tiempos de resolución de las incidencias se adaptarán a los especificados en el apartado "Incidencias" de este Pliego de Prescripciones Técnicas.

El mantenimiento correctivo incluirá la generación de la nueva versión de la solución, su prueba exhaustiva y su puesta en marcha acorde con los procedimientos de Sandetel. Como paso previo a su puesta en marcha siempre se deberá contar con la aprobación del personal de Sandetel, que autorizara el cambio correctivo.

### 5.3.4 Condiciones de las actualizaciones de la solución

Determinadas gestiones relacionadas con la instalación de actualizaciones de la solución, serán realizadas por el proveedor de Outsourcing TI contratado por Sandetel o bien, en colaboración con éste. Cualquier instalación o despliegue de las actualizaciones de la solución, deberá cumplir los siguientes requisitos:

a. Previa a la aplicación de la actualización de la solución, el adjudicatario velará por la realización de una copia de seguridad de todos los datos pertenecientes a Sandetel, evitando la pérdida de información.
b. Antes de ejecutar la actualización de la solución, será necesario disponer de la conformidad de Sandetel

c. Las actualizaciones de la solución, deberán ser realizadas preferiblemente entre las 0:00 y 6:00 horas, aunque podría darse el caso que Sandetel solicite que el cambio de versión o actualización sea realizado en un horario diferente durante las 24 horas del día.
d. Si se produjera una degradación del rendimiento de la solución como consecuencia de la puesta en marcha de algún cambio o actualización, el adjudicatario deberá tratarlo como un error de la misma.

Este sistema ha de poder actualizarse a las últimas versiones disponibles a lo largo del fin de vida útil :

- La actualización ha de poder realizarse en caliente, y sin disrupción del servicio.
- El adjudicatario deberá suministrar dentro del precio ofertado todas las licencias necesarias para el correcto funcionamiento del sistema.
- Se deberá incluir el software necesario y sus correspondientes licencias que permitan tener activas todas las funcionalidades de la solución, siendo estas todas las necesarias para monitorización y administración del sistema, así como todas las licencias necesarias para el correcto y pleno funcionamiento de todo el software instalado.
- Cualquier reposición de elementos o actualizaciones de software será a cargo del adjudicatario sin implicar ningún coste para Sandetel.
- Se han de proponer las actualizaciones y recomendaciones de actualización de parches de forma proactiva junto con notas de la versión previa validación de la compatibilidad de la la actualización sobre la infraestructura ,sistemas y servicios afectados.

### 5.3.5 Incidencias, peticiones y consultas

INCIDENCIAS:

Para resolver las incidencias planteadas por los distintos usuarios de la solución, en la puesta en servicio de la misma se deberá entregar un plan de soporte y resolución de incidencias que sirva como complemento a la fase de formación, que permita la tutela y acompañamiento a los usuarios en la tramitación de los primeros trámites. Recogerá los protocolos de actuación, medios disponibles para el soporte e igualmente podrá contemplar herramientas que permitan el reporte de consultas o errores.

Las incidencias se clasificaran en función de la gravedad, y se exigirá un nivel de servicio mínimo en cuanto a tiempo de respuesta y tiempo de resolución tal y como se muestra en la siguiente tabla, en base a las siguientes consideraciones:

- **Tiempo de respuesta:** Tiempo transcurrido desde que se comunica la incidencia al Servicio de Mantenimiento propuesto, hasta que dicho servicio se pone en contacto con el usuario o cliente.
- **Tiempo de resolución:** Tiempo transcurrido desde el instante en el que se ha notificado por el cliente un aviso de avería/incidencia, hasta el momento en que el servicio, se ha restablecido a su normal funcionamiento.

- **Tipo de incidencia 1-PRIORITARIA:** Fallo en la solución impidiendo la ejecución de las funcionalidades claves sin que el aplicativo permita un camino alternativo para el desarrollo de la misma funcionalidad.
- **Tipo de incidencia 2-ALTA:** Fallo en la solución impidiendo la ejecución de funcionalidad clave aunque el programa permite un camino alternativo para el desarrollo de la misma funcionalidad o fallo en la solución impidiendo la ejecución de funcionalidad no clave pero que afecta a un elevado número de usuarios.
- **Tipo de incidencia 3-NORMAL:** Fallo en la solución impidiendo la ejecución de funcionalidad no clave y que no afecta a un elevado número de usuarios.

| Incidencia | Tiempo de respuesta | Tiempo de resolución |
|---|---|---|
| Tipo 1 - Prioritaria | 1 hora | 8 horas |
| Tipo 2 - Alta | 4 horas | 24 horas |
| Tipo 3 - Normal | 8 horas | 72 horas |

Cabe la posibilidad de que Sandetel contacte con el proveedor externo de servicios TIC para informarle de la avería o incidencia relacionada y sea el proveedor externo de servicios TIC quien contacte con el servicio de soporte para solucionar o dar la respuesta que corresponda.

El adjudicatario deberá disponer del personal y medios necesarios para proporcionar:

- Diagnóstico y Soporte Técnico Especializado.
- Disponibilidad de los técnicos de campo para garantizar presencia "in situ" si fuese necesario.

Para el envío y tramitación de incidencias deben ponerse a disposición de SANDETEL los siguientes métodos de consulta y notificación:

- Número de teléfono.
- Cuenta de correo electrónico.

- Sitio web de comunicación y seguimiento de incidencias.

PETICIONES:

Este apartado incluye aquellas solicitudes de cambio de configuración, adaptación y funcionalidades adicionales a la puesta en marcha, que sean necesarias durante la ejecución del contrato, por ejemplo la integración de la solución de un nuevo fabricante del mercado que haya sido adquirida por Sandetel.

Estas horas de ejecución de la petición irán con cargo a las 150 horas de bolsa de trabajo descritas en el apartado 6 de este PPT.

| Peticiones | Tiempo de respuesta |
|---|---|
| Tipo 1 - Normal | 24 horas |

CONSULTAS:

Se establece como consultas aquellas dudas ocasionadas durante la operativa del proyecto y que no puedan ser resueltas de forma autónoma por Sandetel, y que tengan que ser resueltas para garantizar el buen funcionamiento del servicio.

| Consultas | Tiempo de respuesta | Tiempo de resolución |
|---|---|---|
| Tipo 1 - Normal | 24 horas | 72 horas |

Asimismo durante el periodo de garantía se ofrecerá soporte telefónico y, de ser necesario, asistencia en las instalaciones SANDETEL, para la resolución de los problemas que se planteen y tengan su origen en los trabajos realizados con objeto del presente pliego.

El adjudicatario debe indicar en su oferta los medios y recursos de que dispone para dar cumplimiento al soporte solicitado.

### 5.3.6 Modificación de las Capacidades

Una vez surge la necesidad de modificación de la capacidad de las licencias contratadas ya sea por uso o por demanda, se establecen las siguientes pautas para solicitar el aumento o disminución del número de licencias, teniendo en cuenta que nunca se podrá bajar del número mínimo comprometido de 150 licencias.

La ampliación o disminución deberá realizarse mediante solicitud por el medio que se designe al proveedor del servicio por parte de Sandetel, mediante el responsable/s que se marque al principio del contrato para este tipo de solicitudes.

Para llevar a cabo estas modificaciones, el licitador deberá presentar un procedimiento que incluya instrucciones completas del proceso de solicitud de modificación de las capacidades:

- Solicitud (Teléfono, Email, Aplicación de gestión, ....)
- Aceptación
- Ejecución o implantación

Teniendo en cuenta que la facturación se ha establecido de forma mensual, la solicitud de aumento o disminución deberá realizarse entre los días 10 y 20 del mes, para que surja efecto la solicitud en el mes siguiente. Si no existiera solicitud alguna de aumento o disminución por parte de Sandetel, se entiende que se debe extender el número de licencias contratadas al mes siguiente.

## 6 BOLSA DE SERVICIOS DE APOYO

Se deberá proveer por parte del licitador una bolsa de horas técnicas para servicios de adaptación, integración y configuración de nuevas necesidades que surjan durante la ejecución del proyecto. Se establece un mínimo de 150 horas anuales para este apartado.

## 7 CONDICIONES DEL PROYECTO

Por parte de Sandetel, se asignará un Responsable del proyecto el cual tendrá las siguientes funciones:

- Verificar el correcto desarrollo del proyecto y de la ejecución del contrato.
- Certificar la conformidad a las tareas entregadas/finalizadas por el adjudicatario, dando el visto bueno a su ejecución, funcionamiento o acción que corresponda.
- Comunicar y aplicar las penalizaciones al adjudicatario, en caso que sea necesario. o Confirmar o solicitar los posibles cambios del equipo de trabajo.

El Responsable asignado por Sandetel, podrá delegar sus funciones en una o más personas de Sandetel. En ese caso, dicho Responsable lo comunicará por escrito al adjudicatario informando de los datos de la/s persona/s que corresponda e indicando las tareas delegadas. Durante el desarrollo del proyecto, Sandetel podrá solicitar, como parte de las tareas de seguimiento y control, entregas intermedias que permitan tanto la verificación del trabajo realizado, como evitar y reducir riesgos en los hitos especificados.

Como condición general del proyecto, se establece que tras la finalización del contrato se deberá suministrar a Sandetel una copia completa de todo el almacen de credenciales seguras en el formato exportable que se requiera, así como de elementos integrados, y cualquier información o dependencia adicional que sea necesaria para trasladar el servicio prestado a otra solución PAM o similar.

# 8 CONDICIONES GENERALES

## 8.1 PROPIEDAD DE LOS RESULTADOS DE LOS TRABAJOS

Todos los estudios y documentos, así como los productos y subproductos elaborados por el contratista como consecuencia de la ejecución del presente contrato serán propiedad de SANDETEL quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el adjudicatario autor material de los trabajos.

El adjudicatario renunciará expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del presente contrato pudiera corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este pliego de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa de SANDETEL.

Específicamente todos los derechos de explotación y titularidad de las aplicaciones informáticas y programas de ordenador desarrollados al amparo de esta contratación, corresponden únicamente a SANDETEL.

La presente cláusula no será de aplicación a los productos y herramientas preexistentes empleados para la ejecución del contrato protegidos por derechos industriales o de propiedad intelectual.

## 8.2 SEGURIDAD Y CONFIDENCIALIDAD

La información a la que tenga acceso la empresa como consecuencia del contrato tendrá un carácter confidencial. No podrá transferir información alguna sobre los trabajos a terceras personas o entidades sin el consentimiento expreso y por escrito de SANDETEL.

La empresa adjudicataria, en cumplimiento de la "Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal", únicamente tratará los datos de carácter personal a los que tenga acceso en el marco del presente contrato conforme a las instrucciones de SANDETEL , y no los aplicará o utilizará con un fin distinto al estipulado, ni los comunicará, ni siquiera para su conservación, a otras personas.

Además, deberá cumplir las medidas técnicas y organizativas estipuladas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. En el caso de que la empresa, o cualquiera de sus miembros, destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será responsable de las infracciones cometidas. Una vez finalizada la relación

contractual, los datos de carácter personal tratados por la adjudicataria, así como el resultado del tratamiento obtenido, deberán ser destruidos o devueltos a SANDETEL en el momento en que ésta lo solicite.

## 8.3 PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

En todo lo relativo a la implementación de la funcionalidad de gestión de usuarios y control de accesos del sistema de información a desarrollar, se tendrán en cuenta las estipulaciones que sobre seguridad hace la legislación vigente en materia de tratamiento de datos personales (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) así como de la legislación nacional vigente en materia de protección de datos, y el Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad, modificado por el Real Decreto 951/2015, de 23 de octubre.

En particular, se perseguirá:

- la correcta identificación de los usuarios (medida op.acc.1 del anexo II del ENS).
- la adecuada gestión de derechos de acceso (medida op.acc.4).
- la correcta selección e implantación de los mecanismos de autenticación (medida op.acc.5).

En virtud de lo establecido en el artículo 14.4 del Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad, modificado por el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso y de qué tipo son éstos.

El certificado electrónico podrá utilizarse como medio de autenticación de usuarios, si bien no de modo exclusivo, debiéndose disponer de un medio de autenticación alternativo a su utilización, de acuerdo a las consideraciones establecidas en el anexo II del ENS.

## 8.4 ESQUEMA NACIONAL DE SEGURIDAD

Las propuestas deberán garantizar el cumplimiento de los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información que constituyen el Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010 de 8 de enero, modificado por el Real Decreto 951/2015, de 23 de octubre. En concreto, se deberá asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que son objeto de la presente contratación.

Para lograr esto se aplicarán las medidas de seguridad indicadas en el anexo II del ENS, en función de los tipos de activos presentes en el sistema de información y las dimensiones de información relevantes, considerando que el sistema de información recae en la categoría de seguridad MEDIA conforme a los criterios establecidos en el anexo I del ENS.

Se atenderá también a la normativa interna de SANDETEL en materia de Seguridad TIC.

Además, se deberá atender a las mejores prácticas sobre seguridad recogidas en las series de documentos CCN-STIC (Centro Criptológico Nacional-Seguridad de las Tecnologías de Información y Comunicaciones), disponibles en la web del CERT del Centro Criptológico Nacional (http://www.ccn-cert.cni.es/), así como a las recomendaciones de Andalucía-CERT, como centro especializado en la materia en el ámbito andaluz.