Junta de Andalucía

Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa

Agencia Digital de Andalucía

Consulta preliminar de mercado para la preparación de expediente de contratación de infraestructura, operación y servicios para AndalucíaCERT – Lote I – Suministro de plataforma de monitorización y servicios asociados

Agencia Digital de Andalucía
Dirección General de Estrategia Digital
T: 955061501dged.ada@juntadeandalucia.es

Sumario

1. Objeto de la consulta

Recabar información de los operadores económicos, especialistas en el sector, relativa a la Infraestructura, operación y servicios para AndalucíaCERT – LOTE I – SUMINISTRO DE PLATAFORMA DE MONITORIZACIÓN Y SERVICIOS ASOCIADOS, con el fin de que la Agencia Digital de Andalucía pueda usar, si procede, la información recabada para elaborar los pliegos del próximo expediente de contratación que, en su caso, se licite al respecto.

2. Breve descripción de las necesidades

AndalucíaCERT, como se ha indicado, presta actualmente a su grupo atendido una serie de servicios entre los que se encuentran los de detección de incidentes, apoyados en infraestructuras de monitorización desplegadas principalmente en el perímetro de la Red Corporativa de Telecomunicaciones de la Junta de Andalucía.

El objeto de este lote I es:

- El suministro, instalación, integración y servicios de apoyo de una plataforma de monitorización de eventos y detección de incidentes de seguridad en las infraestructuras TI de la Junta de Andalucía, que sustituirá y mejorará a la existente ahora mismo. Dicha plataforma tendrá la capacidad de capturar y analizar tráfico de red, recoger y normalizar eventos de seguridad y flujos de distintas fuentes, realizar correlación y generar alarmas, gestionables a través de una consola de operación integrada, con capacidad para generar informes y definir políticas de riesgo. Se pretende obtener una visión del estado de arte en las soluciones de detección de amenazas de ciberseguridad basadas en el análisis de logs, eventos de seguridad y tráfico de red. Dadas las potenciales necesidades de crecimiento, se prima una solución que facilite la escalabilidad, elasticidad y operatividad.
- La prestación del servicio de gestión de incidentes de seguridad y de peticiones, incidencias y consultas de AndalucíaCERT.

El adjudicatario, prestará, durante el tiempo de ejecución del contrato:

- Suministro de una plataforma de monitorización, y de posibles ampliaciones de la misma.
- Servicios profesionales de despliegue de la plataforma de monitorización (inicial y ampliación).
- Servicios de soporte y mantenimiento de la plataforma de monitorización.
- Suministro de electrónica de red.
- Servicios de profesionales de despliegue de la electrónica de red.
- Servicios de soporte y mantenimiento de la electrónica de red.
- Servicio de coordinación de actividades.
- Servicio de experto de la plataforma de monitorización, con objeto de lograr una capacidad de detección y respuesta a incidentes óptima, continuada en el tiempo y adaptada a la evolución del entorno tecnológico.
- Servicio de operación de la plataforma de monitorización (localizado), con objeto de monitorizar, valorar y notificar los incidentes de seguridad.

- Servicio de operación de la plataforma de monitorización (deslocalizado), con objeto de monitorizar, valorar y notificar los incidentes de seguridad desde el SOC del proveedor (en tiempo alternado con el servicio localizado).
- Servicio de gestión de incidentes de seguridad N1, con objeto de gestionar todos los incidentes de seguridad reportados a AndalucíaCERT por diversos medios.
- Servicio de gestión de incidentes de seguridad N2, con objeto de gestionar incidentes de seguridad complejos reportados a AndalucíaCERT por diversos medios.
- Servicio de administración de sistemas y redes, con objeto de administrar sistemas y redes auxiliares operadas en AndalucíaCERT.
- Servicio de formación y capacitación del personal de Junta de Andalucía.

3. Plataforma de monitorización

La plataforma de monitorización debe constar de:

- Sensores recolectores de tráfico de red (NIDS, *Network Intrusion Detection System*).
- Una solución de gestión de eventos de seguridad y generación de alarmas de seguridad (SIEM, *Security Information and Event Management*).

De referencia se definen los siguientes elementos conceptuales:

- Sensor recolector de tráfico de red: será el encargado de capturar, analizar y detectar el tráfico de red malicioso de forma pasiva, incluye las funciones propias de un sistema de detección de intrusión de red (NIDS).
- Sensor recolector de logs: este elemento de la solución será el encargado de recoger información de los diferentes dispositivos de la red, sistemas y aplicaciones, así como de filtrar, consolidar y normalizar los eventos y flujos de red recogidos.
- Servidor de gestión: el servidor de gestión realizará tareas como normalizar, priorizar, recolectar, evaluar el riesgo y ejecutar el motor de correlación básica y correlación avanzada (aprendizaje máquina, análisis de comportamiento de usuarios, ...). La correlación debe alimentarse de eventos de los elementos ubicados en su mismo nivel e inferiores. Así mismo, soportará el mantenimiento y tareas externas, tales como copias de respaldo.
- Base de datos: se utilizará para el almacenamiento de los eventos representativos de seguridad recogidos, alarmas generadas, informes, inventario de activos e información útil para la gestión del sistema. Se prima la facilidad de consulta y tiempo de respuesta.
- Base de datos de logs (*logger*): se utilizará para el almacenamiento de todos los eventos recogidos. Incluye mecanismos de indexado para agilizar las búsquedas de eventos. Se prima la capacidad de almacenamiento.

- Consola de administración y operación centralizada: consola centralizada de operación, visualización y gestión de eventos, alarmas e informes.

Los anteriores elementos deben entenderse como elementos conceptuales, y no identificarse unívocamente con dispositivos físicos o módulos software. Los elementos hardware deben contar con medidas de redundancia ante fallos (discos en RAID, fuente de alimentación doble...) y de gestión remota fuera de banda (mediante protocolo IPMI o similar).

3.1. Sensores de red

Los sensores de red estarán ubicados en diversas ubicaciones (*on-premise*) para analizar los flujos de tráfico de red entrada y salida de acceso a Internet antes y después de la DMZ. Adicionalmente se analizará el tráfico de red de la red troncal y de otras sedes.

Las características principales requeridas son:

- Aplicación de fuentes de inteligencia (no gratuitas) actualizadas durante todo el período de garantía.
- Capacidad de monitorización de tráfico de red de interfaz de hasta 10 Gbps (incluyendo capa 7). Tasa de pérdida de paquetes inferior al 5%.
- Capacidad de generar flujos de red con formato *netflow*.
- Capacidad de generar flujos de red con metadatos adicionales (incluyendo capa 7).
- Capacidad de modificación de firmas de detección existentes y creación de firmas nuevas a medida.
- Capacidad de envío cifrado de eventos desde el equipo sensor al recolector de logs.
- Capacidad de reducción en la detección de falsos positivos mediante ajuste de los umbrales de detección.
- Capacidad de que no se produzcan pérdida de eventos en caso de superación puntual del límite de la capacidad máxima soportada o licenciada.
- Capacidad de configuración independiente de detección en cada sensor.
- Capacidad de captura del contenido de los paquetes de red (*payload*) que generan los eventos para análisis forense.
- Capacidad de integración con fuentes de inteligencia de AndalucíaCERT (MISP e IOC/reglas de descarga web).
- Capacidad de integración con fuentes de inteligencia de REYES (herramienta del CCN-CERT).
- El sistema debe ser compatible con reglas de detección de tráfico de red de formato SNORT.

3.1.1. Dimensionado

El tráfico total estimado a procesar es de **76Gbps**, y se estima que son necesarios 9 sensores.

La estimación de necesidades por ubicación es:

Ubicación	# de ubicaciones	Gbps (por ubicación)	# de sensores (por ubicación)
Nodo interconexión	2	20	2
Nodo troncal	2	10	1
Sede pequeña	1	1	1
Sede mediana	1	5	1
Sede grande	1	10	1
Total		76	9

3.2. SIEM

A continuación, se exponen los requisitos de la solución SIEM.

3.2.1. Características

Las características principales requeridas son:

- Aplicación de reglas de correlación (no gratuitas) actualizadas durante todo el período de garantía. La empresa adjudicataria no podrá imputar a la ADA los costes derivados de la adquisición y uso de estas reglas.
- Aplicación de fuentes de inteligencia (no gratuitas) actualizadas durante todo el período de garantía. La empresa adjudicataria no podrá imputar a la ADA los costes derivados de la adquisición y uso de estas reglas
- Capacidad de agregación y normalización de las distintas fuentes de datos.
- Capacidad de correlación empleando operaciones lógicas sobre los eventos detectados.
- Capacidad de correlación relacionando los eventos detectados y la información contenida en la base de datos de conocimiento (por ejemplo, inventario de activos e información sobre los mismos).
- Capacidad de detección por anomalías.
- Capacidad de analizar el comportamiento de usuarios y entidades (UEBA, *User and Entity Behavior Analytics*).
- Capacidad de correlación empleando técnicas de inteligencia artificial y aprendizaje máquina.

- Capacidad de registro de fuentes de flujos de red.
- Capacidad de correlación de fuentes de flujos de red.
- Capacidad de correlación basada en datos históricos.
- Capacidad de correlación basada en vulnerabilidades.
- Capacidad de crear casos de uso mediante pasos guiados (*playbook*).
- Clasificación de los eventos y alarmas según el esquema MITRE ATT&CK.
- Disponibilidad de una librería de casos de uso alineados con el esquema MITRE ATT&CK.
- Capacidad de priorización de eventos basada en distintos criterios (valoración del activo, el tipo o taxonomía del evento, la fiabilidad del evento, reputación de la dirección IP, etc.).
- Capacidad de asignación de políticas de filtrado de eventos a grupos de activos.
- Capacidad de filtrado y aplicación de políticas en la detección de eventos según las necesidades del entorno (modificación de la prioridad, eliminación del panel de eventos, notificación de eventos, activación/desactivación de la opción de correlación, etc.) que se den en ciertos activos.
- Capacidad de que no se produzcan pérdidas de eventos en caso de superación puntual del límite de la capacidad máxima soportada o licenciada.
- Capacidad de visualización del contenido de los paquetes de red (*payload*) de los eventos de red para análisis forense.
- Capacidad de modificación y ajuste de las reglas de correlación existentes y creación de reglas de correlación nuevas a medida.
- Capacidad de reducción en la detección de falsos positivos mediante ajuste de los umbrales de detección.
- Capacidad de ofrecer información de contexto (información histórica de DNS, geolocalización, reputación de dirección IP, ...) durante el análisis del evento.
- Capacidad de espacios de trabajo (*tenant*) para la diferenciación de organismos o sedes.
- Capacidad de envío cifrado de eventos desde el equipo final al sensor recolector de logs.
- Consola de administración, configuración y operación accesible remotamente mediante protocolos seguros (por ejemplo, https) soportado en sistemas Linux.
- Control de acceso por parámetros de red (por ejemplo, rango de direccionamiento).
- La solución debe disponer de control de acceso con doble factor de autenticación, múltiples usuarios, diferentes roles para permitir el acceso a diferentes ámbitos o funcionalidades.

- Capacidad de autenticación de usuarios empleando una base de datos de usuarios externa mediante el protocolo LDAP o Active Directory. Soportar que los usuarios estén en distintas ramas de la base de datos.
- Asignación de privilegios a usuarios basada en roles que permitan asignar diferentes niveles de permiso y acceso en la herramienta. Posibilidad de creación de grupos de usuarios.
- Capacidad de restringir el acceso a la información según activos involucrados o sensores origen de los eventos basada en roles, usuarios o grupos de usuarios.
- Capacidad de registro de actividad de los usuarios.
- Capacidad de gestión de usuarios centralizada.
- Capacidad de configuración y gestión de realización de copias de seguridad de la información albergada en la solución.
- Capacidad de gestión centralizada de los elementos que componen la solución: sensores, fuentes de datos de monitorización, motores de correlación, interfaces de gestión o consulta, etc.
- Capacidad de gestión centralizada de políticas de detección y correlación, firmas, orígenes de firmas, inventario, base de datos de conocimiento, etc...
- Capacidad de actualización automática de la solución y/o los elementos que la componen (corrección de bugs, implementación de mejoras en las funcionalidades, etc).
- La información estará almacenada en servidores ubicados en la Unión Europea.
- La base de datos debe tener cualidad de *big data*.
- Capacidad de firma y sellado de tiempo de los logs y eventos almacenados en formato original.
- Capacidad de búsqueda de eventos centralizada.
- Generación de informes personalizados según distintos criterios (sensor, grupo de activos, propietario de activos, taxonomía, rangos temporales, activos, geolocalización, etc).
- Capacidad de búsquedas avanzadas que faciliten la caza de amenazas (*threat hunting*).
- Capacidad de exportar datos en diferentes formatos de salida, al menos CSV, XML, PDF, HTML.
- Capacidad de paneles informativos personalizados y configurables con datos estadísticos de los eventos y demás información sobre amenazas recogidas por la plataforma.
- Capacidad de generación de mapas de riesgo en tiempo real.
- Notificación automática de alarmas de seguridad por diversos medios: alarma en consola de operación, correo electrónico, servicio web configurable, API, *syslog*, etc.
- Capacidad de definición de políticas de notificación diferentes según distintos criterios: grupo de activos, propietario de activos, sensores de detección, taxonomías, etc.

- Capacidad de integración con fuentes de inteligencia de AndalucíaCERT (MISP e IOC/reglas de descarga web).
- Capacidad de integración con fuentes de inteligencia de REYES (herramienta del CCN-CERT).
- Capacidad de integración con alarmas de seguridad de CARMEN (herramienta del CCN-CERT).
- Capacidad de integración con alarmas de seguridad de GLORIA y/o MONICA (herramientas del CCN-CERT).
- Capacidad de integración con alarmas de seguridad de microCLAUDIA (herramienta del CCN-CERT).
- Capacidad de integración con alarmas de seguridad de sensores SAT (herramienta del CCN-CERT).
- Capacidad de integración con la herramienta de *ticketing* LUCIA (herramienta del CCN-CERT).
- Capacidad de integración con fuentes de inteligencia basadas en estándares STIX/TAXII.
- Capacidad de respuesta automática (SOAR, *Security orchestration, automation, and response*).
- Capacidad de integración con eventos/alarmas de seguridad de principales fabricantes (indicados en el apartado de fuentes de eventos).
- Posibilidad de integración con otras soluciones de *ticketing* externas mediante servicios web.
- Posibilidad de integración con soluciones web externas para la consulta de informes, paneles informativos y mapas de riesgo.
- La solución debe permitir escalar ante futuras demandas (EPS y almacenamiento).
- Se está valorando exigir uno o ambos de los siguientes requisitos:
    - Que la solución esté incluida en el CPSTIC (CCN-STIC 105) en categoría ALTA.
    - En caso de solución en la nube, que la infraestructura de la consola esté certificada de conformidad con al ENS, en categoría ALTA.

3.2.2. Fuentes de eventos

El SIEM propuesto debe integrarse, para la recepción de eventos y alarmas, con las fuentes:

- Los NIDS propuestos por la solución. El SIEM debe estar especialmente adaptado a estos sensores de red para obtener el mayor de los beneficios en la correlación y contextualización de los eventos.
- Otras fuentes de eventos de la infraestructura TIC de la Junta descritas a continuación.

Las fuentes de eventos principales las componen los servicios de infraestructura de los principales fabricantes empleados por la Junta de Andalucía (las marcas indicadas no tienen carácter exhaustivo, sino que en su mayor parte reflejan las principales tecnologías actualmente en uso en la Junta de Andalucía):

- Servicios SIEM: El SIEM propuesto formará parte de una jerarquía superior sobre otros SIEM actualmente en funcionamiento en la Junta de Andalucía. Éste debe soportar la integración de alarmas de seguridad de los principales fabricantes: Alienvault, McAfee, …
- Servicio microClaudia: El SIEM propuesto debe soportar la integración de alarmas de la herramienta microClaudia del CCN-CERT.
- Servicios CASB: El SIEM propuesto debe soportar la integración de alarmas de seguridad de los principales fabricantes: Microsoft CASB, …
- Servicios de proveedores en la nube (CIPS, cloud infrastructure and platform services): El SIEM propuesto debe soportar la integración de eventos de seguridad de los principales proveedores: Azure, AWS, Google Cloud…
- Servicios de aplicaciones en la nube: El SIEM propuesto debe soportar la integración de eventos de seguridad de los principales desarrolladores: Microsoft Office 365, Microsoft Exchange, …
- Servicios de EDR: El SIEM propuesto debe soportar la integración de alarmas de seguridad de los principales fabricantes: Cytomic, Crowdstrike, Palo Alto…
- Servicios de cortafuegos: El SIEM propuesto debe soportar la integración de eventos de seguridad de los principales fabricantes: Fortinet, Forcepoint, Palo Alto…
- Servicios de NGFW/IDS/IPS: El SIEM propuesto debe soportar la integración de alarmas de seguridad de los principales fabricantes: Suricata…
- Servicios de WIFI: El SIEM propuesto debe soportar la integración de eventos de seguridad de los principales fabricantes: Aruba…
- Servicios de pasarela web (*proxy*): El SIEM propuesto debe soportar la integración de eventos de seguridad de los principales fabricantes: Bluecoat, …
- Servicios de VPN: El SIEM propuesto debe soportar la integración de eventos de seguridad de los principales fabricantes: FortiVPN, …
- Servicios de directorio: El SIEM propuesto debe soportar la integración de eventos de seguridad de los principales fabricantes: AD, LDAP, RADIUS, …
- Servicios de DNS: El SIEM propuesto debe soportar la integración de eventos de seguridad de los principales fabricantes: Infoblox, …
- Servicios de aplicaciones corporativas: El SIEM propuesto de soportar la integración de eventos de seguridad con productos de software libre y de los principales fabricantes: EXIM, ISL, … * Puede requerir desarrollo de analizadores (*parsers)*.
- Servicio de procesado de fuentes de la comunidad: IntelMQ.

Específicamente, el fabricante debe indicar el grado de integración con los sistemas en la nube de: Azure, Microsoft E365, Microsoft Exchange y Microsoft CASB.

El fabricante o adjudicatario debe adaptarse a la evolución de las fuentes:

- Debe llevar a cabo una actualización continuada según los cambios de los formatos de eventos, de forma que se asegure la integración de la plataforma con las diferentes evoluciones del software de los dispositivos y sistemas externos.
- Debe llevar a cabo una actualización continuada según los cambios de las bases de datos de firmas de los sistemas de seguridad, de forma que se asegure la integración de la plataforma con las diferentes evoluciones del software de los dispositivos y sistemas externos (identificadores/firmas de virus, vulnerabilidades, prevención de ataques...).

Los protocolos de intercambio de fuentes de eventos y de inteligencia deberán incluir, al menos, los siguientes:

- API REST.
- Protocolos SNMP y SYSLOG (en todas sus versiones).
- Fuentes de eventos en formatos XML, TXT, CSV, CEF o JSON.
- Fuentes de inteligencia en estándares STIX/TAXII.
- Flujos de red en formato NetFlow o IPFIX (en todas sus versiones).
- *Push*/*Pull* de ficheros de fuentes de información externas (HTTP, FTP, ...).

3.2.3. Arquitectura

Los modelos de arquitectura contemplados son:

- Centralizado. En la que todos los elementos conceptuales estén en una misma ubicación (excluyendo los sensores de red).
- Distribuido. Múltiples configuraciones en las que diversos componentes conceptuales están desplegados en las ubicaciones de los elementos de monitorización. Puede incluir además distintos niveles de jerarquía.

3.2.4. Modelos de despliegue

Modelos de despliegue contemplados:

- En las instalaciones de la Junta de Andalucía (*on-premises*): Físico o virtualizado.
- En instalaciones de terceros (*off-premises*).

En caso de servicio en nube (*cloud*), los modelos de despliegue contemplados son:

- Modelo de despliegue: Público o privado.
- Modelo de servicio: SaaS o PaaS.

3.2.5. Dimensionado

La estimación es de aproximadamente **116K** EPS de eventos.

La estimación de necesidades por ubicación es:

Ubicaciones	# de ubicaciones	# tipo de fuentes de eventos	EPS Logs (por ubicación)
Nodo central	1	-	-
Nodo interconexión	2	20	40.000
Nodo troncal	2	5	10.000
Sede pequeña	1	5	1.000
Sede mediana	1	10	5.000
Sede grande	1	15	10.000
Total			116.000

La retención de datos debe ser de 6 meses.

Para simplificar el escenario no se considera crecimiento de la demanda.

4. Electrónica de red

Para el despliegue de la nueva plataforma de monitorización es necesario disponer de nuevos *switches* de electrónica de red, debido a la insuficiencia de recursos y obsolescencia del equipamiento de red actual. Estos *switches* se utilizarán para dar servicio a la nueva plataforma de monitorización, y así como para otros servicios de AndalucíaCERT.

Es necesario instalar *switches* en las siguientes ubicaciones:

- Sala de operaciones, desde la que trabajan los técnicos del Centro.
- Nodo central, donde está ubicada la sede central de la plataforma de monitorización propuesta, y otros servicios auxiliares de AndalucíaCERT.
- Nodos de interconexión, donde están ubicados los nodos de interconexión y troncal, y otros servicios auxiliares de AndalucíaCERT.

4.1.1. Dimensionado

La estimación es de 5 switches con una capacidad de 168 puertos libres, más los puertos necesarios para dar soporte la plataforma de monitorización propuesta (lo cual depende de la solución ofertada):

Ubicaciones	# de switchs	Puertos de red libres

Sala de operaciones	1	24 1G (cobre)
Nodo central	2	24 1G (cobre) 12 10G (fibra) más las necesidades de la plataforma de monitorización
Nodo interconexión	2	24 1G (cobre) 12 10G (fibra) más las necesidades de la plataforma de monitorización

5. Servicios asociados

Se requieren servicios profesionales de soporte/mantenimiento/operación/administración de la plataforma de monitorización y de operación/administración del SOC de AndalucíaCERT.

Los servicios se prestarán en modos remoto y presencial. Los técnicos del servicio presencial se integrarán en el equipo de AndalucíaCERT y trabajarán en colaboración con el resto de técnicos del Centro.

Los servicios están descritos en los apartados siguientes.

5.1. Servicio de suministro y despliegue de la plataforma de monitorización

Servicio a desempeñar en la fase inicial del contrato (fase 1).

Incluye el suministro, diseño, instalación y configuración de la plataforma de monitorización propuesta, la integración de fuentes y con otros sistemas. El proyecto de implantación puede requerir, entre otras tareas:

- Diseño del plan técnico de despliegue.
- El análisis y selección de las fuentes a integrar en la solución, la confección de guías de configuración de las fuentes y asesoramiento en las labores de configuración de los equipos monitorizados.
- El desarrollo para la integración de las fuentes no soportadas nativamente (o*ut-of-the-box*) por la plataforma.
- El desarrollo de reglas de correlación y cuadros de mando específicos.
- El análisis y selección de las fuentes a integrar en la solución, asesoramiento y confección de guías de configuración de las fuentes
- La documentación de los casos de uso.
- Realizar un ajuste fino y subsanación de falsos positivos en la post-implantación.

5.2. Servicio de suministro y apoyo a nuevos despliegues de la plataforma de monitorización

Servicio a desempeñar en la fase 2.

Incluye el suministro y ampliación de la plataforma de monitorización para la integración de fuentes de los sistemas de monitorización de eventos pertenecientes a otros organismos o entidades, para cada una de las tres sedes (pequeña, mediana y grande). El proyecto de implantación puede requerir, entre otras tareas:

- Diseño del plan técnico de despliegue.
- El análisis y selección de las fuentes a integrar en la solución, la confección de guías de configuración de las fuentes y asesoramiento en las labores de configuración de los equipos monitorizados.
- El desarrollo para la integración de las fuentes no soportadas nativamente (o*ut-of-the-box*) por la plataforma.
- El desarrollo de reglas de correlación y cuadros de mando específicos.
- El análisis y selección de las fuentes a integrar en la solución, asesoramiento y confección de guías de configuración de las fuentes
- La documentación de los casos de uso.
- Realizar un ajuste fino y subsanación de falsos positivos en la post-implantación.

5.3. Servicio de soporte y mantenimiento de la plataforma de monitorización

Servicios deslocalizados a prestar en el SOC del proveedor en modalidad 24x7.

Incluye las licencias y suscripciones de los productos requeridos para el funcionamiento de la plataforma, de las fuentes de inteligencia, de las librerías de casos de uso y de otros productos ofertados. Así como los servicios de garantía del soporte y mantenimiento de la plataforma.

Las tareas principales son:

- Soporte hardware 24x7.
- Monitorización de la disponibilidad de la plataforma.
- Atención a las incidencias de indisponibilidad de la plataforma.
- Administración de la plataforma de monitorización: gestión de incidencias, gestión de cambios, gestión de parches, gestión de usuarios, … Incluyendo actualizaciones de versiones de software semestrales y aplicación de parches de seguridad de la plataforma.

5.4. Servicio de suministro y despliegue de la electrónica de red

Servicio a desempeñar en la fase inicial del contrato.

Incluye el suministro, diseño, instalación y configuración de la electrónica de red propuesta.

5.5. Servicio de soporte y mantenimiento de la electrónica de red

Servicio a prestar en modalidad 24x7.

Incluye las licencias y suscripciones de los productos requeridos para el funcionamiento de los *switches*. Así como los servicios de garantía del soporte y mantenimiento de los *switches*.

Las tareas principales son:

- Soporte hardware 24x7.

5.6. Servicio de coordinación de actividades

Servicio remoto a prestar en modalidad 8x5.

Este servicio engloba las labores de organización, coordinación y control para una ejecución eficaz y eficiente de los servicios localizados y deslocalizados del contrato, así como de la interlocución y del reporte a la ADA.

5.6.1. Dimensionado

La estimación es de un (1) recurso humano con una dedicación al 50%.

El puesto debe contar con un suplente para cubrir indisponibilidades temporales.

5.7. Servicio de soporte experto de la plataforma de monitorización

Servicios presenciales a prestar en la sede de AndalucíaCERT en modalidad 8x5.

Las tareas principales son:

- Ajuste fino continuo en la detección de incidentes de seguridad de la plataforma. Corrección de posibles falsos positivos.
- Gestión de fuentes de ciberinteligencia.
- Integración de nuevas fuentes de eventos.
- Monitorización de incidentes de seguridad basados en las señales débiles disponibles en la plataforma de monitorización
- Creación de procedimientos de pasos guiados (*runbook*) de casos de uso.

5.7.1. Dimensionado

La estimación es de un (1) recurso humano, ampliable con un (1) recurso adicional en la fase 2.

El puesto debe contar con un suplente para cubrir indisponibilidades temporales.

5.8. Servicio de operación de la plataforma de monitorización (localizado)

Servicios presenciales a prestar en la sede de AndalucíaCERT en modalidad 12x5.

Este servicio engloba principalmente la monitorización de incidentes de seguridad basados en las señales fuertes (alarmas) generadas por la plataforma de monitorización, así como labores propias de la operación de la plataforma.

Las actividades propias a desarrollar serán las siguientes:

- Interlocución con el servicio de operación deslocalizado.

Adicionalmente se desarrollan las siguientes actividades compartidas con el Servicio de operación de la plataforma de monitorización (deslocalizado), reflejadas en el apartado siguiente. Estas actividades tendrán un desborde al servicio deslocalizado (ver el apartado siguiente) para dar una cobertura en 24x7:

- Atención a las detecciones y alarmas en la consola de plataforma.
- Notificación de los incidentes de seguridad en la plataforma LUCÍA de AndalucíaCERT. Se debe incluir un plan de respuesta al incidente.
- Identificación de posibles falsos positivos.
- Interlocución con el servicio de soporte y mantenimiento del fabricante.
- Atención de consultas técnicas.

5.8.1. Dimensionado

La estimación es de tres (3) recursos humanos, ampliable con dos (2) recursos adicionales en la fase 2. El equipo debe estar lo suficientemente dimensionando para permitir una cobertura 12x5; con un mínimo de dos (2) técnicos durante el turno de mañana en jornada laboral, y un mínimo de un (1) técnico por la tarde.

5.9. Servicio de operación de la plataforma de monitorización (deslocalizado)

Servicios deslocalizados a prestar en el SOC del proveedor en el horario complementario al del Servicio de operación de la plataforma de monitorización (localizado) para garantizar una cobertura 24x7 del servicio los 365 días del año.

Las actividades a desarrollar serán las indicadas como actividades compartidas en el apartado anterior.

5.9.1. Dimensionado

La estimación es del equivalente a un (1) recurso humano al 50%. El equipo debe estar lo suficientemente dimensionando como para permitir una cobertura 24x7 los 365 días del año (excluyendo la ventana de 12x5 del servicio localizado); con un mínimo del equivalente de un (1) técnico al 50% durante la prestación.

5.10. Servicio de gestión de incidentes de seguridad de Nivel 1 (N1)

Servicios presenciales a prestar en la sede de AndalucíaCERT en modalidad 24x7.

La labor principal es la gestión de los incidentes de seguridad de AndalucíaCERT.

Las actividades a desarrollar serán las siguientes:

- Atención a los canales de entrada:
  - Buzón de correo electrónico
  - Línea telefónica.
  - La herramienta LUCIA.
  - Búsqueda proactiva de incidentes de seguridad en sistemas auxiliares.
  - Cualquier otra vía de entrada que sea habilitada o solicitada por el Jefe de Proyecto.

- Atención de los incidentes de seguridad que lleguen a AndalucíaCERT. Análisis, tratamiento, seguimiento y resolución. Interlocución con terceros: grupo atendido y otros equipos de respuesta.
- Atención de las consultas, peticiones, incidencias que lleguen a AndalucíaCERT.
- Tareas de apoyo a la gestión interna y a los sistemas de calidad. Generación de informes de servicio.

5.10.1. Dimensionado

El volumen aproximado de incidentes de seguridad gestionados en el año pasado fue de 600 incidentes al mes.

La estimación es de siete (7) recursos humanos, ampliable con dos (2) recursos adicionales en la fase 2. El equipo debe estar lo suficientemente dimensionando para permitir una cobertura 24x7 los 365 días del año; con un mínimo de tres (3) técnicos durante el turno de mañana en jornada laboral, y un mínimo de un (1) técnico en el resto del tiempo.

5.11. Servicio de gestión de incidentes de seguridad de Nivel 2 (N2)

Servicios presenciales a prestar en la sede de AndalucíaCERT en modalidad 12x5 con disponibilidad de guardias telefónicas en 24x7.

El equipo de segundo nivel es un equipo de mayor especialización que el equipo N1 y desarrolla las capacidades de resolución de incidentes complejos, de detección de amenazas avanzadas y de soporte y mejora continua de los procedimientos.

5.11.1. Dimensionado

El volumen aproximado de incidentes de seguridad gestionados en el año pasado fue de 600 incidentes al mes. El volumen estimado de intervenciones en la guardia es de doce (12) al año.

La estimación es de tres (3) recursos humanos, ampliable con un (1) recurso adicional en la fase 2. El equipo debe estar lo suficientemente dimensionando para permitir una cobertura 12x5; con un mínimo de dos (2) técnicos durante el turno de mañana en jornada laboral, y un mínimo de un (1) técnico por la tarde.

5.12. Servicio de administración de sistemas y redes

Servicios presenciales a prestar en la sede de AndalucíaCERT en modalidad 8x5 con disponibilidad de guardias telefónicas en 24x7.

Es el encargado de administrar la infraestructura común propia de AndalucíaCERT (excluyendo la plataforma de monitorización propuesta), incluyendo:

- Entorno de virtualización.
- Almacenamiento de virtualización.
- Electrónica de red.
- Cortafuegos.
- Sistemas operativos, servidores web, bases de datos y aplicativos.

Las labores principales de este perfil senior son:

- Administración de los sistemas (principalmente de software libre): gestión de cambios, gestión de parches, gestión de usuarios...
- Asegurar el funcionamiento correcto de los sistemas.
- Atender las incidencias de disponibilidad de los sistemas.
- Diseñar y desplegar nuevos sistemas requeridos en AndalucíaCERT.

El puesto puede requerir el desplazamiento a los CPD ubicados en Sevilla.

5.12.1. Dimensionado

El número de equipos y sistemas a administrar es del orden de 75, aproximadamente.

La estimación es de un (1) recurso humano. El volumen estimado de intervenciones en la guardia es de dos (2) al año.

El puesto debe contar con un suplente para cubrir indisponibilidades temporales.

5.13. Servicio de formación y capacitación

Se incluirán en la contratación servicios de formación iniciales y periódicos, para personal de la Junta de Andalucía sobre la plataforma desplegada, sus características y operación en la detección de amenazas.

La formación se puede prestar de forma telemática.

5.13.1. Dimensionado

La estimación es de una sesión formativa inicial y posteriormente una sesión en cada uno de los semestres siguientes. Capacidad para un mínimo de 20 asistentes.

5.14. Resumen de los servicios profesionales

La siguiente tabla muestra los servicios y de forma resumida la estimación de recursos humanos dedicados.

Servicio	**Modo**	**Recursos**	**Total**
Servicio de suministro y despliegue de la plataforma de monitorización			
Servicio de soporte y mantenimiento de la plataforma de monitorización	24x7	Servicio de soporte hardware del fabricante. Servicio de administración de la plataforma prestado desde el SOC del proveedor.	
Servicio de suministro y apoyo a nuevos despliegues de la plataforma de monitorización	24x7	Servicio de soporte hardware del fabricante. Servicio de administración de la plataforma prestado desde el SOC del proveedor.	
Servicio de suministro y despliegue de la electrónica			

de red			
Servicio de soporte y mantenimiento de la electrónica de red	24x7	Servicio de soporte hardware del fabricante.	
Servicio de coordinación de actividades	**8x5**	**Un (1) recurso humano con una dedicación al 50%.**	**0,5**
Servicio de soporte experto de la plataforma de monitorización	**8x5**	**Un (1) recurso humano con una dedicación al 100%, ampliable con un (1) recurso adicional en la fase 2.**	**1 (hasta 2)**
Servicio de operación de la plataforma de monitorización (localizado)	**12x5**	**Tres (3) recursos humanos con una dedicación al 100%, ampliable con dos (2) recursos adicionales en la fase 2.**	**3 (hasta 5)**
Servicio de operación de la plataforma de monitorización (deslocalizado)	24x7 alternado	Equivalente a un (1) recurso humano con una dedicación al 50%. Alternado con el servicio localizado. Servicio prestado desde el SOC del proveedor.	0,5
Servicio de gestión de incidentes de seguridad de Nivel 1 (N1)	**24x7**	**Siete (7) recursos humanos con una dedicación al 100%, ampliable con dos (2) recursos adicionales en la fase 2.**	**7 (hasta 9)**
Servicio de gestión de incidentes de seguridad de Nivel 2 (N2)	**12x5 + guardia**	**Tres (3) recursos humanos con una dedicación al 100%, ampliable con un (1) recurso adicional en la fase 2.**	**3 (hasta 4)**
Servicio de administración de sistemas y redes	**8x5 + guardia**	**Un (1) recurso humano con una dedicación al 100%.**	**1**
Servicio de formación y capacitación			

5.15. Acuerdos de nivel de servicio

Al menos, se está pensando introducir en la licitación el siguiente conjunto de ANS:

- Disponibilidad de la plataforma
- Resolución de incidencias
- Atención a peticiones
- Respuesta a consultas
- Comunicación de alarmas de nivel alto/muy alto/crítico
- Respuesta a incidentes de seguridad

6. Dimensionamiento general

En la descripción de cada servicio se incluye el dimensionamiento inicial/estimado de los servicios de cara al modelado de los mismos.

El ámbito de actuación de la posible contratación sería la Administración de la Junta de Andalucía y sus entidades instrumentales, así como los consorcios a los que se refiere el artículo 12.3 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía. Esto suma aproximadamente 85 organismos que forman el grupo atendido principal de AndalucíaCERT.

La duración del contrato sería de cuatro (4) años.