

Enpresa-Garapenerako Euskal Agentzia  
Agencia Vasca de Desarrollo Empresarial  
Business Development Basque Agency

[www.spri.eus](http://www.spri.eus)



SPRI-AGENCIA VASCA DE DESARROLLO EMPRESARIAL

PLIEGO PRESCRIPCIONES TECNICAS:**2024044 armonizado**

**SUMINISTRO E IMPLANTACION DE EQUIPAMIENTO Y SERVICIOS DE MANTENIMIENTO DE LA  
INFRAESTRUCTURA DE COMUNICACIONES Y CIBERSEGURIDAD**

## SUMARIO

|                                                                                         |           |
|-----------------------------------------------------------------------------------------|-----------|
| <b>1. INTRODUCCIÓN .....</b>                                                            | <b>4</b>  |
| <b>2. OBJETO DEL CONTRATO .....</b>                                                     | <b>4</b>  |
| <b>2.1. Suministro de la infraestructura necesaria.....</b>                             | <b>5</b>  |
| <b>2.2. Servicios profesionales.....</b>                                                | <b>5</b>  |
| <b>2.2.1. Servicios asociados a implantaciones.....</b>                                 | <b>5</b>  |
| <b>2.2.2. Servicios de Operación y Mantenimiento de Seguridad y Comunicaciones.....</b> | <b>6</b>  |
| <b>2.2.3. Servicios de Consultoría de Seguridad y Comunicaciones.....</b>               | <b>6</b>  |
| <b>2.2.4. Servicios de Fabricante .....</b>                                             | <b>6</b>  |
| <b>2.2.5. Gestión de dominios de internet y certificados de seguridad.....</b>          | <b>6</b>  |
| <b>3. ESPECIFICACIONES TÉCNICAS .....</b>                                               | <b>7</b>  |
| <b>3.1. CONSIDERACIONES .....</b>                                                       | <b>7</b>  |
| <b>3.2. REQUISITOS TÉCNICOS DE LA SOLUCIÓN.....</b>                                     | <b>7</b>  |
| <b>3.3. EQUIPAMIENTO A EVOLUCIONAR .....</b>                                            | <b>7</b>  |
| <b>3.4. SERVICIOS REQUERIDOS.....</b>                                                   | <b>8</b>  |
| <b>3.4.1. Servicio de implantación.....</b>                                             | <b>8</b>  |
| <b>3.4.2. Servicio de operación, mantenimiento y monitorización.....</b>                | <b>8</b>  |
| <b>3.4.2.1. Servicio de mantenimiento .....</b>                                         | <b>9</b>  |
| <b>3.4.2.2. Servicio de operaciones de comunicaciones y seguridad .....</b>             | <b>9</b>  |
| <b>3.4.2.3. Servicio de monitorización de comunicaciones y seguridad.....</b>           | <b>9</b>  |
| <b>3.4.3. Soporte Técnico Especialista.....</b>                                         | <b>10</b> |
| <b>3.4.4. Servicio de EDR.....</b>                                                      | <b>11</b> |
| <b>3.4.4.1. Suministro de licencias de EDR .....</b>                                    | <b>11</b> |
| <b>3.4.4.2. Servicio de monitorización, análisis y contención de incidentes .....</b>   | <b>11</b> |
| <b>3.4.4.3. Servicio de instalación y mantenimiento de agentes EDR .....</b>            | <b>12</b> |
| <b>3.4.5. Análisis técnicos de sistemas.....</b>                                        | <b>12</b> |
| <b>4. Condiciones del contrato.....</b>                                                 | <b>13</b> |
| <b>4.1. Horario de Servicio y Localización.....</b>                                     | <b>13</b> |
| <b>4.2. Nivel de Servicio .....</b>                                                     | <b>13</b> |
| <b>5. Equipo de Trabajo.....</b>                                                        | <b>14</b> |
| <b>6. Supervisión, Control del servicio y Seguimiento .....</b>                         | <b>16</b> |
| <b>6.1. Supervisión .....</b>                                                           | <b>16</b> |

---

|                                             |           |
|---------------------------------------------|-----------|
| <b>6.2. Control de servicio .....</b>       | <b>16</b> |
| <b>6.3. Mecanismos de Seguimientos.....</b> | <b>16</b> |

## 1. INTRODUCCIÓN

SPRI-Agencia Vasca de Desarrollo Empresarial (en adelante, “SPRI”), ente público de derecho privado dependiente del Departamento de Industria, Transición Energética y Sostenibilidad, centra su actividad en la gestión de diferentes tipos de instrumentos de apoyo a las empresas de la Comunidad Autónoma de Euskadi, con el objetivo de contribuir a la mejora de la competitividad de estas y al desarrollo económico de la región. Con carácter general, estos instrumentos suelen materializarse en forma de programas de ayudas o servicios dirigidos a diferentes ámbitos empresariales tales como el Emprendimiento, la Digitalización, el I+D, la Innovación, o el desarrollo industrial entre otros.

Para el desarrollo de esta actividad, SPRI necesita mantener y evolucionar sus infraestructuras y servicios de comunicaciones y seguridad de la información, y realizar las adecuaciones necesarias para adaptarse al cumplimiento exigido por el Esquema Nacional de Seguridad.

La información es un activo estratégico para la SPRI, y debe ser adecuadamente protegida, sea cual sea la forma en la que esté representada, almacenada o sea procesada.

En este entorno cabe destacar el papel de las Tecnologías de la Información y de las Comunicaciones (TIC) por la creciente importancia en el tratamiento de esa información, siendo el rápido desarrollo de estas tecnologías uno de los factores principales que está permitiendo que las Administraciones Públicas mejoren su eficiencia, posibilitando acercarse al ciudadano mediante nuevos canales de comunicación. Pero la información y las tecnologías que la tratan están sometidas a riesgos, internos y externos, que es necesario gestionar adecuadamente para situarlos bajo umbrales aceptables.

En este campo, SPRI se propone utilizar sistemas y normas que permitan gestionar adecuadamente la seguridad de la información, como pueden ser la norma ISO/\*IEC 27001:2010, “Information technology - Security techniques - Information security management systems – Requirements”, o el Esquema Nacional de Seguridad, en el campo de la administración electrónica. Por este motivo las empresas licitantes deben estar certificadas en el Esquema Nacional de Seguridad, así como en las normas de referencia ISO 27000 e ISO 20000, valorándose positivamente que los fabricantes de la solución propuesta sean líderes en sus mercados correspondientes.

## 2. OBJETO DEL CONTRATO

El objeto del contrato consiste en el mantenimiento y evolución de la infraestructura de comunicaciones y seguridad actualmente existente, así como la prestación de los servicios profesionales asociados a las operaciones de mantenimiento, análisis,

consultoría e implantación para el correcto funcionamiento de la plataforma de comunicaciones y ciberseguridad de SPRI.

La solución propuesta debe consistir en una solución integral que incluya todos los elementos necesarios para el cumplimiento de los requisitos y especificaciones descritas a lo largo del presente pliego.

A continuación, se detalla el alcance del contrato cuyo contenido se complementa con los requerimientos técnicos del presente documento:

## **2.1. Suministro de la infraestructura necesaria**

El adjudicatario deberá realizar el mantenimiento y renovación del equipamiento actual en los casos que sean necesarios, incluyendo licencias para la implantación. Además de garantizar el correcto funcionamiento de la infraestructura de comunicaciones y ciberseguridad de SPRI.

El equipamiento suministrado cumplirá con los requisitos establecidos en el presente pliego de condiciones técnicas y deberá adaptarse a las exigencias de Esquema Nacional de Seguridad. El adjudicatario desplegará su solución en SPRI, ubicada en la Plaza Bizkaia, calle Alameda Urquijo, 36 de Bilbao.

## **2.2. Servicios profesionales**

El adjudicatario prestará los siguientes servicios, cuyos requerimientos se establecen en el presente pliego de prescripciones técnicas.

### **2.2.1. Servicios asociados a implantaciones**

Servicios asociados a la implantación de soluciones:

- Revisión de la solución final, del plan de trabajo y de la metodología establecida para validación por parte de SPRI.
- Instalación y configuración de acuerdo de la solución propuesta y validada.
- Elaboración y ejecución de un plan de pruebas que certifique la adecuada puesta en marcha de la solución.
- Formación a SPRI y/o a quien SPRI designe sobre las soluciones y tecnologías desplegadas.
- Documentación de la solución desplegada.

### **2.2.2. Servicios de Operación y Mantenimiento de Seguridad y Comunicaciones**

Servicios de operación y mantenimiento de seguridad y comunicaciones:

- Servicios de mantenimiento correctivo, preventivo y evolutivo de acuerdo con los niveles de servicio descritos en el pliego de prescripciones técnicas.
- Servicio de soporte técnico experto en las tecnologías en uso en SPRI.
- Servicios para el mantenimiento del equipamiento de SPRI.

### **2.2.3. Servicios de Consultoría de Seguridad y Comunicaciones**

Servicio de consultoría especializada en ciberseguridad y comunicaciones:

- Servicios avanzados de seguridad como Hacking, Análisis Forense.
- Colaboración y asesoramiento a los Responsables de Seguridad de SPRI.

### **2.2.4. Servicios de Fabricante**

El adjudicatario debe ofrecer servicio de fabricante:

- Garantía y soporte de fabricante de acuerdo con los requisitos descritos en el pliego de prescripciones técnicas con la duración del contrato.
- El adjudicatario deberá disponer de un contrato de soporte con el fabricante correspondiente. Dicha contratación garantizara al menos la modalidad 8x5xNBD. Es decir, soporte técnico 8x5 y tiempo de reemplazo y sustitución hardware NBD (Next Business Day). Además del propio soporte del fabricante durante la duración del contrato, los licitadores incluirán en su propuesta un servicio de soporte y mantenimiento adicional para la mejora de la cobertura y niveles de servicio del fabricante.
- La propuesta incluirá todo el software y licencias necesarias para las diferentes funcionalidades y tecnologías propuestas para el periodo de duración del contrato del equipamiento dentro del alcance de esta licitación.

### **2.2.5. Gestión de dominios de internet y certificados de seguridad**

Adquisición, renovación y mantenimiento de certificados de seguridad y dominios de internet. Gestión de dominios en la plataforma del proveedor correspondiente o en la plataforma de BATERA.

### **3. ESPECIFICACIONES TÉCNICAS**

#### **3.1. CONSIDERACIONES**

En este apartado se describen las características técnicas que conforman el objeto del contrato y que el adjudicatario deberá prestar, no siendo el listado que aparece a continuación una relación exhaustiva de las características del servicio contratado. Los referidos requisitos deben entenderse como mínimos (a excepción de que se indique lo contrario) pudiendo los licitadores ampliarlos y mejorarlos en sus ofertas. El adjudicatario aportará y describirá los conocimientos, metodologías, herramientas y equipo humano en el que se apoyará para asegurar el resultado óptimo del proyecto.

#### **3.2. REQUISITOS TÉCNICOS DE LA SOLUCIÓN**

El adjudicatario deberá renovar el equipamiento de ciberseguridad actual (tanto hardware como software y suscripciones), y complementarlo con las nuevas adquisiciones detalladas en el siguiente punto. Todo ello para el correcto funcionamiento de la infraestructura de comunicaciones y ciberseguridad de SPRI.

Es importante puntualizar que, por razones de seguridad, las características del equipamiento actual únicamente se describen de forma somera en este pliego. En caso de que alguno de los licitadores necesitara conocer más detalles de las características del equipamiento actual, deberá ponerse en contacto con SPRI, y previa firma de acuerdo de confidencialidad, se podrá acceder a dicha información.

#### **3.3. EQUIPAMIENTO A EVOLUCIONAR**

A continuación se detallan las plataformas y equipamientos a evolucionar como parte de esta licitación:

- Actualización de la actual infraestructura de WIFI
- Actualización de los componentes del BIG-IP para adecuar el ciclo de vida del producto
- Actualización de la actual infraestructura de Firewall perimetral.

### **3.4. SERVICIOS REQUERIDOS**

#### **3.4.1. Servicio de implantación**

El licitador deberá proporcionar y describir los servicios de implantación asociados a las nuevas plataformas señaladas anteriormente, considerando los siguientes puntos dentro del alcance de cada uno de los proyectos de implantación asociados.

- Implantación de la solución y migración de los servicios actuales a las nuevas plataformas.
  - Suministro de software, así como licencias necesarias
  - Despliegue de los diversos servicios y software.
  - Definición de la configuración y/o migración de la configuración actual al equipamiento en los casos de evolución, siguiendo las mejores prácticas de diseño siempre que sea posible. En la solución de seguridad perimetral para aumentar el nivel de seguridad, se requiere una política de Nivel 7.
  - Plan de pruebas y puesta en producción. Deberá considerarse en la propuesta que, en caso de necesidad, y dependiendo del impacto de la puesta en producción ciertas acciones podrán llevarse a cabo fuera del horario habitual del servicio.
- Integración de la solución con las herramientas de monitorización existentes en SPRI.
- Formación de la solución instalada al personal de SPRI o a quien SPRI designe para ello.
- Documentación de la solución desplegada.

El licitador definirá claramente el plazo de implantación de la solución, lo más detallada posible. Tras la fase de implantación, cada una de las plataformas será objeto de operación y mantenimiento bajo los servicios que se detallan en los siguientes apartados.

#### **3.4.2. Servicio de operación, mantenimiento y monitorización**

Con el objetivo de dar cobertura transversal a todas las necesidades en materia de Seguridad y Comunicaciones que puedan ser necesarios por parte de SPRI, a continuación, se describen los servicios de Operación y Mantenimiento requeridos para el periodo de vigencia del contrato. Estos servicios se proporcionarán sobre el equipamiento que se propondrá en esta licitación, así como equipamiento de Seguridad existente actualmente en SPRI que se enumera a continuación:

- Infraestructura de Protección Cortafuegos
- Herramienta de monitorización de seguridad por comportamiento
- Infraestructura WAF con funciones de balanceo
- Infraestructura WIFI actual
- Infraestructura de conmutación
- Infraestructura de protección perimetral del correo electrónico

- Sistema EDRsaas para parque de equipos y servidores

#### **3.4.2.1. Servicio de mantenimiento**

El servicio incluirá mantenimiento reactivo-correctivo, preventivo y evolutivo sobre las infraestructuras de comunicaciones y seguridad de SPRI.

##### **Mantenimiento Reactivo-Correctivo**

La propuesta deberá incluir un servicio de mantenimiento correctivo cuyo objetivo será la solución de deficiencias en alguno de los equipos incluidos en el contrato, entendiendo deficiencia como algo que debería funcionar o estar correcto y que no lo está. El servicio de mantenimiento correctivo incluirá la realización de todas las tareas necesarias para la resolución de las incidencias, tratando siempre de restaurar el servicio en el menor tiempo posible, minimizando el impacto y adoptando las medidas necesarias para prevenir la repetición de las mismas.

##### **Mantenimiento Preventivo y Evolutivo**

El licitador incluirá en su propuesta la prestación de un servicio de mantenimiento preventivo cuyo objetivo será garantizar el buen funcionamiento y fiabilidad de los equipos incluidos en contrato y detectar posibles focos de problemas que puedan surgir en el futuro. De la misma forma, el licitador deberá incluir en su propuesta la prestación de un servicio de mantenimiento evolutivo para realizar las modificaciones necesarias en la infraestructura con el objeto de aumentar o mejorar las funcionalidades del sistema, ya sea por las necesidades de SPRI o por otras causas como pueden ser, por ejemplo, cambios normativos, fin de soporte de versiones, etc.

#### **3.4.2.2. Servicio de operaciones de comunicaciones y seguridad**

El servicio de operaciones sobre las infraestructuras de comunicaciones y seguridad de SPRI incluirá:

##### **Gestión de Configuración y Políticas**

El licitador incluirá en su propuesta la prestación de un servicio de gestión de configuraciones y políticas que permita a SPRI adecuar las configuraciones y las políticas de los elementos objeto del mantenimiento y evolución a sus necesidades funcionales y de seguridad a lo largo de la vigencia del contrato.

##### **Gestión Certificados de seguridad y dominios**

El licitador incluirá en su propuesta la prestación de un servicio de gestión de certificados y dominios que permita a SPRI la adquisición y gestión administrativa (además de técnica) de los nuevos dominios que sean necesarios a lo largo de la vigencia del contrato. Se valorará la capacidad de migración y gestión de dichos certificados/dominios dentro de un entorno de Gobierno Vasco.

#### **3.4.2.3. Servicio de monitorización de comunicaciones y seguridad**

El servicio de monitorización sobre las infraestructuras de comunicaciones y seguridad de SPRI incluirá:

### **Gestión de Incidentes de Seguridad**

El licitador incluirá en su propuesta la prestación de un servicio de gestión de incidentes de seguridad que articulará con los responsables de SPRI en materia de Seguridad de forma que redunde en una gestión ágil y efectiva de cuantos incidentes se detecten en SPRI desde el registro, pasando por la coordinación hasta la actuación y mitigación de los mismos.

### **Identificación proactiva, análisis y tratamiento de Eventos de Seguridad**

El licitador incluirá en su propuesta la prestación de un servicio monitorización continua de los diferentes elementos de seguridad que le permita identificar de forma proactiva vulnerabilidades, ataques o amenazas a la infraestructura de SPRI que deberá analizar y tratar para corregir o mitigar.

### **Respuesta ante incidencias (DFIR)**

Este servicio comprende la respuesta ante incidentes de seguridad considerados críticos conforme al Acuerdo de Nivel de Servicio, prestado 24\*7. No obstante, sólo se facturará en el caso de producirse un incidente de seguridad crítico que requiera de estos servicios, a solicitud de SPRI.

Dentro de este servicio, cuando se haya detectado una incidencia de nivel crítico independientemente del tiempo de respuesta máximo establecido, el adjudicatario deberá presentar, sobre la base del Plan de Respuesta ante Incidencias, un plan de actuación concreto para la incidencia detectada, que incluirá, si fuera necesario (por la caída de comunicaciones y/o imposibilidad de actuar de forma remota), la presencia física en nuestras oficinas de un equipo técnico multidisciplinar según propuesta del adjudicatario, que coordinará y se responsabilizará de la implementación del Plan de Actuación, coordinado en todo momento con los responsable de SPRI.

Este Plan de Actuación incluirá asimismo las tareas a realizar por el adjudicatario de cara a la comunicación de la incidencia ante los organismos competentes según la normativa existente en el momento de la incidencia.

Además, se asesorará en comunicación interna /externa del incidente de seguridad.

## **3.4.3. Soporte Técnico Especialista**

El licitador deberá incluir en su propuesta la prestación de un servicio de soporte técnico experto, abierto a las necesidades de SPRI en consultas de soporte y evolución, en el ámbito de las tecnologías relacionadas con las infraestructuras de comunicaciones y seguridad en horarios de prestación del servicio establecidos. Se debe tener en cuenta que este soporte podrá ser requerido en las instalaciones de SPRI para cualquiera de las acciones para las que sea necesario su experiencia y/o conocimiento experto.

Además del soporte anterior se solicitan servicios avanzados y de gobierno de seguridad TI, como, por ejemplo:

- **Servicios Avanzados de Seguridad IT**
  - Hacking/Pentesting
  - Análisis Forense
  - Servicios de Formación y Concienciación
- **Servicios asociados al Gobierno de la Seguridad IT**
  - Colaboración en cumplimiento normativo (GDPR, ENS, etc.)
  - Colaboración y apoyo al responsable de seguridad de SPRI

### 3.4.4. Servicio de EDR

El sistema EDR, Endpoint Detection and Response integra todos los equipos de SPRI:

- Ordenadores personales
- Host y servidores
- Otros equipos relacionados en el resumen de infraestructura

El objetivo de éste EDR es analizar los comportamientos de los equipos y poderlos aislar o tomar decisiones sobre ellos en determinadas circunstancias.

El EDR deberá generar avisos y/o actuaciones integradas en el servicio de monitorización en comportamientos anómalos detectados por el EDR en tiempo real. Con posibilidad de aislamiento completo del equipo de forma inmediata, a definir con SPRI los equipos y el procedimiento a implementar.

Adicionalmente, se dispone de un servicio EDRAaaS el cual dispone de un despliegue de una tecnología Endpoint Detection & Response (EDR), monitorización 7x24 y operación de la herramienta que detecta amenazas basada en comportamiento. Todos los equipos están registrados (a través de ese agente EDR), y monitorizados en consola del fabricante.

Por esto se proveerán los siguientes servicios:

#### 3.4.4.1. Suministro de licencias de EDR

Se suministrará licencias hasta 500 licencias del sistema actual de EDR, siendo los requisitos mínimos de versión soportada:

| Sistema Operativo | Versión                                              |
|-------------------|------------------------------------------------------|
| <b>Windows</b>    | Win 10 (32-bit and 64-bit)                           |
|                   | <u><b>Server 2003 R2 SP2 (32-bit and 64-bit)</b></u> |
|                   | Server 2008 (32-bit and 64-bit)                      |
|                   | Server 2008 R2, R2 SP1, R2 SP2 (64-bit)              |
|                   | Server 2012 (32-bit and 64-bit)                      |
|                   | Server 2012 R2 (32-bit and 64-bit)                   |
|                   | Server 2016 (32-bit and 64-bit)                      |
| <b>Linux</b>      | RHEL 6.8+, 7.2+, 8 (64-bit)                          |
|                   | CentOS 6.9+, 7.2+, 8 (64-bit)                        |
|                   | Ubuntu 14.04, 16.04, 18.04, 19.04                    |
|                   | Oracle Linux 6.10, 7.6                               |

#### 3.4.4.2. Servicio de monitorización, análisis y contención de incidentes

Se deberá proveer un servicio de monitorización, análisis y contención de incidentes para los agentes EDR instalados con los siguientes requerimientos mínimos:

- Gestión centralizada desde la consola del fabricante (no se admitirá el despliegue de la solución en nube de la empresa licitadora).
- Monitorización 24x7 de todos los activos (hasta 500 *endpoints*).
- Definición de un conjunto de equipos críticos para análisis en 24x7.
- Análisis 8x5 de todos los activos (un mínimo 20 análisis).
- Análisis 24x7 de activos críticos (al menos 2 análisis para un mínimo del 10% de activos).
- Contención de dispositivos afectados por una amenaza dentro del alcance del servicio, y contención automática de activos no críticos en menos de 5 minutos.
- Inyección de inteligencia específica:
  - Inyección de IOCs (indicadores de compromiso) en consola del fabricante.
  - Extracción de IOCs propios derivados de las investigaciones.
- Análisis proactivo de amenazas y *malware*.
- Gestión de incidencias, peticiones y seguimiento de tickets a través de una monitorización de operaciones de seguridad .

Se deberá desarrollar, al menos, las siguientes actividades de seguimiento:

- Elaboración de informes técnicos de los servicios mensualmente.
- Reuniones mensuales de seguimiento de servicio.
- Reuniones de trabajo técnicas trimestrales para tratar temas relacionados con el servicio determinados por SPRI.

#### **3.4.4.3. Servicio de instalación y mantenimiento de agentes EDR**

Será responsabilidad de la empresa adjudicataria el despliegue de los agentes EDR, así como las actualizaciones de estos, dotándose al servicio a tal efecto de una bolsa de horas.

Los equipos se encuentran registrados (a través de los agentes EDR) en una consola única del fabricante. El despliegue de nuevos agentes EDR, en su caso, debe realizarse en la consola actual del fabricante.

Se valorará la activación del módulo de antivirus disponible para el agente EDR en los equipos de tipo servidor, siendo responsabilidad de la empresa adjudicataria la desinstalación de la solución de antivirus instalada en la actualidad, y la activación del nuevo módulo de antivirus.

#### **3.4.5. Análisis técnicos de sistemas**

Esta fase tiene como objetivo el análisis de la información para la identificación de las tecnologías utilizadas en los procesos de IT de la organización, sus procedimientos relacionados y los sistemas de información que soportan. La identificación de estos procesos y tecnologías determinará el alcance para el desarrollo del “Análisis Técnico”.

Asimismo, se identificarán aquellas normativas o políticas definidas en la organización que condicionan o establecen los criterios a la hora de implementar las topologías y configuraciones de los diferentes elementos que serán analizados posteriormente.

Finalmente, se extraerán criterios y planes en marcha o identificados para la mejora en materia de ciberseguridad por parte de SPRI que serán tenidos en cuenta en la evaluación y posterior redacción del plan de acción

El análisis técnico se realizará con una periodicidad anual, proporcionando un informe que revisará el estado de la seguridad de las infraestructuras actuales de SPRI que recoja las actividades realizadas, grado de cumplimiento por punto analizado, oportunidades de mejora detectadas, y las tareas a realizar, incluyendo área/puesto responsable y una estimación subjetiva del esfuerzo, impacto y la prioridad de estas acciones.

El análisis técnico, que deberá reflejarse en el Informe de Análisis de la Situación Actual deberá recoger, además del análisis técnico de la infraestructura del EVE, los siguientes apartados, entre otros:

**Análisis de vulnerabilidades en los sistemas implantados**

El objetivo es conocer en tiempo real cualquier vulnerabilidad que afecte a la totalidad de los sistemas IT y poder acometer acciones, de parcheo y/o aislamiento sobre los sistemas que sean vulnerables.

**Inteligencia y Threat Hunting**

Este servicio contemplará la integración con otras fuentes de información de amenazas tanto propios como externos.

Incluirá actividades de Threat Hunting, que permitan buscar de forma proactiva amenazas ocultas, en nuestros sistemas o en fuentes externas.

Se propondrá la metodología de trabajo, el método de comunicación a SPRI de las amenazas, así como la periodicidad de las actividades a acometer.

**Seguridad en comunicaciones internas/externas y seguridad perimetral**

Se analizarán los sistemas de comunicación actuales y se propondrá un plan de acción encaminado a la mejora en la seguridad en comunicación y políticas de seguridad (Firewalls, configuración de Switches, etc..).

Revisión de los Firewalls, a nivel de parcheo y revisión de las actuales políticas de seguridad.

## **4. Condiciones del contrato**

### **4.1. Horario de Servicio y Localización**

Los servicios de asistencia técnica objeto de la presente contratación serán requeridos en régimen de 24x7x365. El licitador garantizara el servicio todos los días del año a cualquier hora con una cobertura en atención de incidencias inmediata, cuando así sea requerido. Se entiende por inmediata la asistencia en la Sede de SPRI en un período inferior a 2 horas a contar desde reporte de la avería por parte de SPRI a la empresa adjudicataria. El horario de prestación del servicio presencial se adecuará al horario que rige en cada momento en SPRI. Si bien, el servicio podrá ofrecerse de forma remota, para realizar el servicio de soporte y mantenimiento, es un requisito que bajo necesidad de SPRI en la prestación del servicio se podrá acudir a las instalaciones de SPRI los días indicados por SPRI; con el objetivo de trabajar conjuntamente con el personal de SPRI en cualquiera de las labores que se estén tratando en cada momento o nuevas necesidades que puedan surgir.

Seguimiento de servicio remoto o in-situ a petición de SPRI de 2 horas por semana.

### **4.2. Nivel de Servicio**

El licitador propondrá un modelo de acuerdo de nivel de servicio que garantice la prestación de los servicios contratados dentro de unos límites aceptables, comprometiéndose al menos a

garantizar que los servicios serán prestados de acuerdo con un modelo 8x5 con los niveles mínimos que se detallan a continuación:

| Prioridad | Riesgo/Impacto                               | Descripción                                                                                                    | Tiempo máximo de respuesta | Tiempo máximo de resolución/contención |
|-----------|----------------------------------------------|----------------------------------------------------------------------------------------------------------------|----------------------------|----------------------------------------|
| Crítica   | Caída de Servicio<br>Intrusión<br>confirmada | Se ha caído algunos/todos los servicios debido a acciones no programadas.<br>Se detectan intrusiones o ataques | < 30 minutos               | < 2 horas (24X7)                       |
| Alta      | Servicios degradados<br>Ataque o intrusión   | Servicios degradados o no responden adecuadamente.<br>Se sospecha de ataque o intrusión                        | < 1 hora                   | < 4 horas (24X7)                       |
| Media     | Comportamientos anómalos                     | Comportamientos anómalos.<br>Degradación del servicio que impide trabajar adecuadamente                        | < 2 horas                  | < 8 horas laborables                   |
| Baja      | Resto de incidencias                         | Se detectan bajo rendimiento u otro tipo de incidencias                                                        | < 3 horas                  | < 24 horas laborables                  |

El cumplimiento de los niveles de servicio se revisará regularmente, para ello el adjudicatario realizará con periodicidad **trimestral** a SPRI un informe que detalle las estadísticas de la actividad del servicio durante el periodo, con el detalle suficiente que permita evaluar dicho cumplimiento.

## 5. Equipo de Trabajo

El licitador debe contar con personal técnico especializado y con experiencia contrastada en las tecnologías existentes y propuestas para SPRI. Además de poseer de un nivel adecuado de certificación en la solución de fabricante propuesta en cada caso.

La empresa licitadora deberá describir en su Propuesta Técnica la organización (perfiles) del equipo asignado a la realización de las actividades resultantes del presente pliego, además, de las funcionalidades de estos.

El equipo de trabajo estará formado por un mínimo de los siguientes perfiles para llevar a cabo el servicio de mantenimiento descrito en la presente licitación, pudiendo valorarse positivamente un número superior de perfiles y deberá contener necesariamente, al menos, una persona que cubra cada una de las funciones y/o perfil profesional que se detalla a continuación.

- **Responsable del Servicio**

- Será el responsable de interlocución con SPRI
- Responsable del seguimiento y coordinación del Servicio

- Experiencia mínima de 5 años
- **Soporte Técnico experto**
  - Equipo multidisciplinar especialista en cada una de las tecnologías objeto del mantenimiento
  - Experiencia mínima de 3 años de la persona que lidere el equipo de soporte
- **Soporte Técnico sistemas**
  - Equipo especialista en sistemas de seguridad
  - Experiencia mínima de 3 años de la persona que lidere el equipo
- **Soporte Primer Nivel**
  - Monitorización, operación y administración del equipamiento de Comunicaciones y Seguridad
- **Soporte EDR**
  - Instalación y mantenimiento de agentes EDR
- **Soporte para la gestión de certificados y dominios**
  - Gestión de certificados y dominios

Con el objetivo de facilitar y homogeneizar las propuestas se presenta, en la siguiente tabla, la dedicación estimada para cada uno de los perfiles requeridos a modo orientativo.

| Perfil                                    | Dedicación anual                |
|-------------------------------------------|---------------------------------|
| <b>Responsable del Servicio</b>           | 50-100h                         |
| <b>Soporte de Técnico Experto</b>         | 250-300h                        |
| <b>Soporte Técnico de Sistemas</b>        | 100-150h                        |
| <b>Soporte Primer Nivel</b>               | 500-700h                        |
| <b>Soporte EDR</b>                        | 100-120h                        |
| <b>Gestión de certificados y dominios</b> | 10 certificados<br>100 dominios |

Se valorarán certificaciones sobre el servicio prestado en las infraestructuras de comunicaciones y seguridad recogidas en la presente licitación:

- A nivel de empresa proveedora del servicio se valoraran certificaciones de fabricante sobre productos como:
  - CheckPoint
  - F5
  - Aruba
  - Darktrace
  - Trellix
- A nivel de profesionales en la prestación del servicio certificaciones como:
  - Check Point Certified Security
  - Aruba Certified Professional Certification in Networking
  - F5 certified administrator

## **6. Supervisión, Control del servicio y Seguimiento**

### **6.1. Supervisión**

La dedicación de las personas asignadas al proyecto para cada contrato se ajustará mensualmente a la demanda del proyecto, bajo la supervisión de SPRI, sin superar en ningún caso el valor estimado del contrato

### **6.2. Control de servicio**

Los trabajos desarrollados por el equipo del proyecto serán supervisados directamente por el Departamento de Tecnologías de la Información y Comunicación de SPRI, que podrá pedir las explicaciones e informaciones que considere oportuno al objeto de verificar el correcto desarrollo de los trabajos contratados.

### **6.3. Mecanismos de Seguimientos**

El equipo de trabajo estará dirigido por un/una responsable del proyecto con dedicación estable y suficiente, quien coordinará las tareas implicadas y será el/la interlocutor/a principal con la persona asignada por el Departamento de TIC de SPRI.

Deberán establecerse todos los mecanismos de control que permitan verificar de forma continuada el cumplimiento de los objetivos especificados, tanto en plazos como en términos de calidad final. Para ello se contempla:

- Reuniones de seguimiento: se celebrarán reuniones periódicas destinadas a revisar el grado de cumplimiento y avance de las tareas planificadas, las reasignaciones de personal si fueran precisas, la validación de las programaciones de actividades a realizar, etc.
- Reuniones de seguimiento de ejecución de costes.
- Informes de situación y progreso: con los que la empresa adjudicataria comunicará a SPRI, el estado puntual de los trabajos, de los objetivos alcanzados, de las incidencias ocurridas, etc. Estos informes de forma periódica en los que reflejará, al menos los siguientes elementos:
  - La evolución y actividades del servicio de mantenimiento
  - El estado actual del equipamiento objeto del contrato
  - Propuestas orientadas a mejorar el servicio o el rendimiento y/o disponibilidad de los componentes de seguridad de SPRI.
- Informes de análisis que incluirán los siguientes aspectos como mínimo:
  - Incidencias relevantes
  - Revisión hardware, versiones software, fechas de fin de vida (tanto software como hardware), existencia de bugs y/o vulnerabilidades
  - Configuraciones realizadas más relevantes
  - Estado y consumo de licencias
  - Estado general de Seguridad en SPRI
  - Resultados de Auditorias y/o Análisis Forenses realizados en el periodo
  - Acciones recomendadas

SPRI analizará los resultados indicados y estudiará la conveniencia de llevar a cabo las acciones propuestas, si la decisión es favorable a la ejecución de alguna de las propuestas dicha ejecución será realizada por el adjudicatario, sin que ello conlleve

coste alguno. Tras la valoración por parte de SPRI se acometerán las acciones que se consideren adecuadas para la evolución y mejora del sistema de seguridad de SPRI.