PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES

Nº Expediente: 582023114100
Denominación: SERVICIO DE ADMINISTRACION AVANZADA GESTION DE IDENTIDADES Y DE CIBERSEGURIDAD
Departamento: 3800 DPTO.TECNOLOG.INFORMACIÓN Y COMUNICAC.
Técnico: JOSE GAREA LOUREIRO

CSV:202079MZDXuE4hYXwtH7eilbgyFKV8BOQ=

Contenido

Pliego Prescripciones Técnicas

1 INTRODUCCIÓN

El objeto del presente pliego es definir las condiciones técnicas necesarias para contratar los servicios de administración avanzada de Gestión de Identidades y de Ciberseguridad, que el Departamento presta a toda la organización del INTA en sus distintos campus.

Con este nuevo pliego el INTA debe seguir en su proceso de mejora continua en cuanto a Ciberseguridad, y adaptarse al Real Decreto 311/2022, de 3 de mayo, por el que se regula el nuevo Esquema Nacional de Seguridad.

CSV:202079MZDXuE4hYXwtH7eilbgyFKV8BOQ=

2 DESCRIPCIÓN DEL SERVICIO

Los servicios incluidos en este pliego proporcionan un escenario para la administración avanzada de Gestión de identidades y de la Ciberseguridad basado en la prevención, protección, detección y respuesta.

El detalle, con cada uno de los servicios incluidos en este **pliego**, se especificará en el apartado: ***Servicios de Administración Avanzada de Gestión de Identidades y de Ciberseguridad***

CSV:202079MZDXuE4hYXwtH7eilbgyFKV8BOQ=

3 REQUISITOS LEGALES TÉCNICOS

Con carácter general serán de aplicación genérica a lo largo del ciclo vital del proyecto las siguientes normas:

En materia de Administración Electrónica:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

En materia de Seguridad - Protección de Datos de Carácter Personal:

- 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 la libre circulación de estos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
- Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

En materia de Seguridad - Instrucciones técnicas de seguridad:

- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

En materia de Transparencia:

- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

CSV:202079MZDXuE4hYXwtH7eilbgyFKV8BOQ=

En materia de Seguridad – Ciberseguridad – Sector Público:

- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información
- Secretaría General de Administración Digital. Resolución de 7 de julio de 2021
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones
- Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

En materia de Interoperabilidad:

- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

En materia de Registros Electrónicos:

- La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia, por el que se modifica la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En materia de Accesibilidad:

- Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.
- Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público.

En materia de Reutilización de la Información del Sector Público

- Ley 37/2007, de 16 de noviembre, sobre Reutilización de la información del sector público
- Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal.

En materia de Factura Electrónica

- Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación
- Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público.

4 REQUISITOS DEL SERVICIO

4.1 Conocimientos demostrables

Los conocimientos demostrables se desarrollan a lo largo de este pliego y del PCAP.

La empresa adjudicataria debe contar con la habilitación HSEM (Habilitación de Seguridad de Empresa), o tenerlo solicitado con fecha previa a la publicación de esta licitación, dado que en el INTA existen sistemas TIC que manejan información clasificada.

Y por lo tanto los recursos del adjudicatario que tengan que interactuar o administrar sistemas que manejen información de difusión limitada deberán estar en posesión de la Habilitación Personal de Seguridad (HPS) Nivel C, EU-C, NC o superior.

La empresa Adjudicataria deberá cumplir las cláusulas de seguridad expresadas en el **Anexo_C** durante la ejecución del contrato.

4.2 Organización del servicio

Debido a la necesidad operativa de comunicación entre los diferentes contratos del Dpto. TIC se deberá garantizar los canales adecuados para realizarse de forma correcta y eficiente. Para ello las empresas adjudicatarias de cada pliego del Dpto. TIC, en caso de colaboración entre ellas, deberán cumplir con el Marco Colaborativo que el Departamento de Tecnologías de la Información y Comunicaciones tiene integrado en sus procesos. Este Marco Colaborativo se puede solicitar a la dirección (ciberseguridad_DTIC@inta.es).

Debe existir una organización específica prevista para el desarrollo de las actividades del pliego en la que cada función quede perfectamente identificada, y cada función tenga asignada una persona responsable de su cumplimiento.

Se establecen las siguientes figuras y órganos de gobierno del proyecto:

- Director Técnico del Proyecto.
- Jefe de Proyecto.

Las funciones y responsabilidades de cada uno de ellos serán:

Director Técnico del Proyecto

Será designado por el INTA y deberá seguir las directrices marcadas por los diversos comités que existen o que se creen a este efecto, siendo sus funciones y responsabilidades las siguientes:

- Dirigir, supervisar y coordinar la realización y desarrollo de los trabajos.
- Aprobar el Programa de realización de los trabajos.
- Velar por el nivel de calidad de los trabajos.
- Coordinar las reuniones entre usuarios y técnicos involucrados en el proyecto.
- Decidir sobre la aceptación de las modificaciones técnicas propuestas por el Equipo de proyecto a lo largo del desarrollo de los trabajos.
- Asegurar el seguimiento del Programa de realización de los trabajos.
- Hacer cumplir las normas de funcionamiento y las condiciones estipuladas en este Documento.
- Autorizar cualquier alteración de la metodología empleada, tanto en los productos finales, como en la realización de las fases, módulos, actividades y tareas.

- Revisar los resultados parciales y totales de la realización del proyecto; a estos efectos deberá recibir y analizar los resultados y documentación elaborados a la finalización de cada etapa, pudiendo introducir las modificaciones o correcciones oportunas antes del comienzo de las siguientes.

Jefe de Proyecto
Será aportado por el adjudicatario, siendo su responsabilidad la ejecución de los trabajos. Además, tendrá como objetivos específicos los siguientes:

- Organizar la ejecución del proyecto de acuerdo con el Programa de realización de los trabajos y poner en práctica las instrucciones del Director Técnico del Proyecto.
- Ostentar la representación del equipo técnico en sus relaciones con INTA en lo referente a la ejecución de los trabajos.
- Proponer al Director Técnico del Proyecto, las modificaciones que estime necesarias, surgidas durante el desarrollo de los trabajos.
- Asegurar el nivel de calidad de los trabajos.
- Presentar al Director Técnico del Proyecto, para su aprobación, los resultados parciales y totales de la realización de las actividades y trabajos.

Medición de los trabajos
Para realizar un seguimiento y gestión de las tareas en las cuales se divide el servicio, será del máximo interés disponer de una medición del mismo lo más afinada posible, que distinga las dedicaciones a los distintos tipos de trabajos que la componen. Se entregarán mensualmente reportes, con el detalle de las actividades y trabajos desarrollados, durante el mes.

4.2.1 Lugar de la prestación del servicio

Los servicios incluidos en **el pliego** que se van a prestar, y que fueron mencionados anteriormente, tendrán lugar en las siguientes localizaciones:

- **Campus 1: INTA – TORR (Sede Central).**

  Constituye la **Sede Central**, incluye el organismo externo GALILEO – GSC (Galileo Service Centre).
  Carretera de Ajalvir km. 4, s/n. 28850 Torrejón de Ardoz (Madrid).

- **Campus 2: INTA – PARD (Campus "El Pardo" - Madrid).**

  Carretera de la Sierra s/n. 28048 El Pardo (Madrid).

- **Campus 3: INTA – SANM (Campus “La Marañosa”).**

  Incluye el organismo externo GALILEO – GSMC (Galileo Security Monitoring Centre). Carretera M-301, km. 10,500. 28330 San Martín de la Vega (Madrid).

- **Centro de Ensayos 1: INTA – MADR (Centro “General Marvá”).**

  Calle Princesa, 38 - 2. 28008 Madrid.

- **Centro de Ensayos 2: INTA – GUAD (CEAR - Centro de Evaluación y Análisis Radioeléctrico).**

Carretera N-320, km. 274, 19145 Guadalajara.

- **Centro de Ensayos 3: INTA – CADI (CET - Centro de Ensayos de Torregorda).**

  Vía Augusta Julia, s/n. 11071 Torregorda (Cádiz).

- **Centro de Ensayos 4: INTA – LUGO (CIAR - Centro de Investigación Aeroportada de Rozas).**

  Aeródromo de Rozas. Mondriz, s/n. 27250 Castro de Rei (Lugo).

- **Centro de Ensayos 5: INTA – AREN (CEDEA - Centro de Experimentación de "El Arenosillo").**

  Carretera San Juan del Puerto, km. 33. 21130 Mazagón (Huelva).

- **INTA-MO. Centro para Ensayos, Entrenamiento y Montaje de Aeronaves no Tripuladas (CEUS).**

  Carretera de Moguer. 21800 - Huelva**.**

- **Estación Espacial 1. INTA-VILL (ESAC - Estación de Seguimiento de Satélites de Villafranca del Castillo (LAEFF).**

  Camino bajo del castillo, s/n. 28692 Villafranca del Castillo (Madrid).

- **Estación Espacial 2. INTA-RO (Estación de Seguimiento Espacial Robledo NASA).**

  C/ Villafranca del Castillo. 28691 Robledo de Chavela (Madrid).

- **Estación Espacial 3. INTA-CEBR (Estación Espacial de Cebreros).**

  Instalaciones de Cebreros, AV-562, Coordenadas (40°27'12.4"N, 4°22'08.1"W). 05260 Cebreros (Ávila).

- **Estación Espacial 4: INTA – MASP (CEC - Centro Espacial de Canarias).**

  Wagner 14 - Montaña Blanca - Maspalomas. 35005 Maspalomas (Las Palmas de Gran Canaria).

- **INTA – CUAD (Polvorín de Cuadros).**

  Antiguo Polvorín de Cuadros. Coordenadas (42°45'50"N 5°39'14"W). 24620 Cuadros (León).

- **INTA – GR (Ensayos de experimentación en vuelo para la certificación de aeronaves).**

  Aeropuerto de Granada. Autovía A-92 (dirección Sevilla). 18329 Chauchina (Granada).

- **INTA – SEVI (Maestranza aérea de Sevilla).**

  Urbanización Los Maldonados, nº 6. 41807 Sevilla.

- **INTA – VALE (INTA Valencia).**

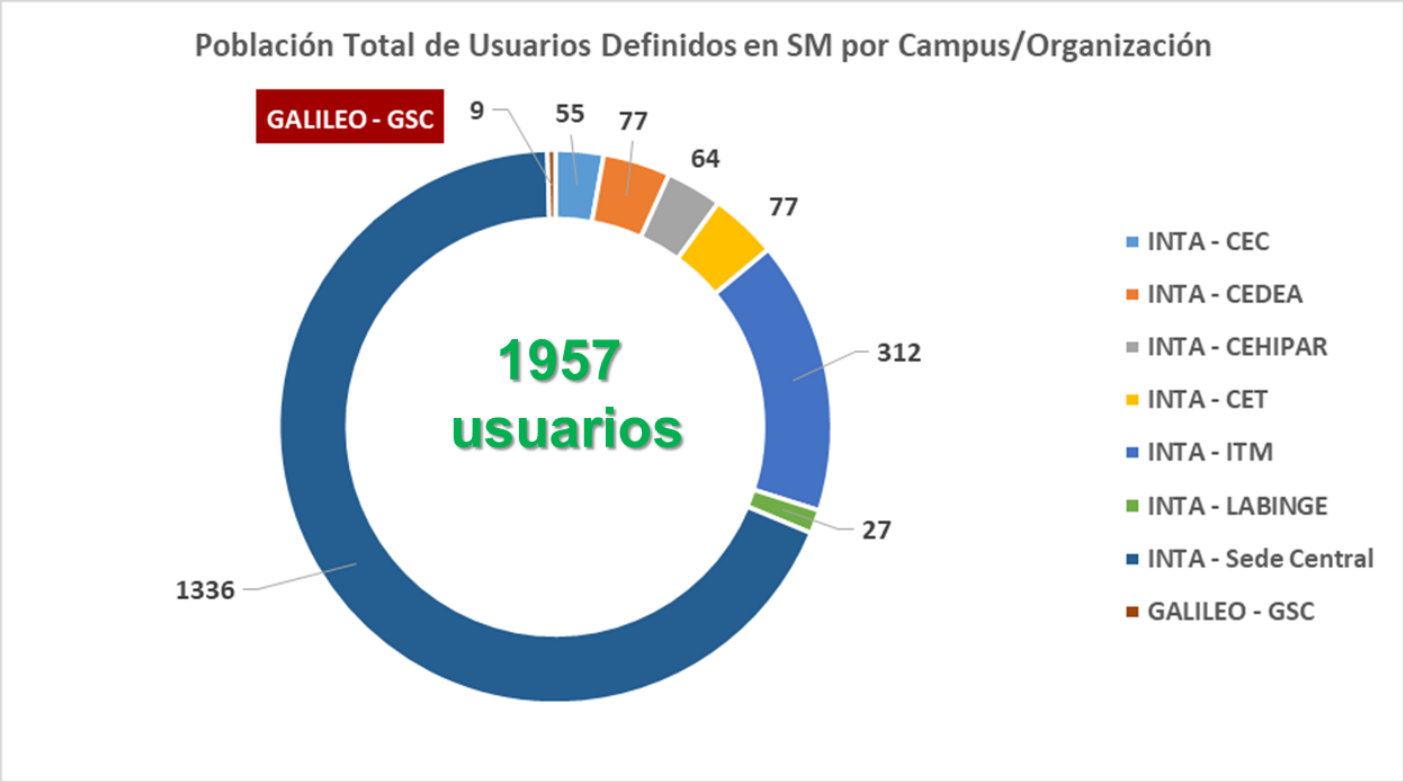
  Pianista Amparo Iturbi, nº 32. 46607 Valencia.

NOMENCLATURA PARA PRESTACIÓN DE SERVICIOS POR CAMPUS / Organismos Externos:

INTA – GLOBAL: Incluye todas las localidades de Campus INTA (Campus, Centros de Ensayo y Estaciones Espaciales) a excepción del organismo externo GALILEO – GSC (Galileo Service Center).

Servicios Compartidos: Incluye todas las localidades de Campus INTA (Campus, Centros de Ensayo y Estaciones Espaciales) **incluyendo organismo externo, por ejemplo, GALILEO – GSC (Galileo Service Center)**

La distribución (promedia) de **población de usuarios de servicios por** campus es la siguiente:



4.2.2 Horario de la prestación del servicio

En la tabla siguiente se describe el horario y el lugar de prestación, para cada uno de los servicios, **de este pliego.**

Servicio	Horario	Lugar de prestación

Servicios de prevención de incidentes de seguridad	Horario de oficina De 09:00 a 19:00 los días laborables excepto los viernes de 09:30 a 14:30	Oficinas del adjudicatario; excepto para las auditorías de seguridad de infraestructuras que deberán ser realizadas desde las instalaciones del INTA en Madrid.
Servicios de protección	Horario de oficina De 09:00 a 19:00 los días laborables excepto los viernes de 09:30 a 14:30	Oficinas del adjudicatario.
Servicios de detección de incidentes de seguridad	24x7x365	Oficinas del adjudicatario.
Servicios de respuesta a incidentes de seguridad	8x5	Oficinas del adjudicatario.
Gestión de Identidades	Horario de oficina De 09:00 a 19:00 los días laborables excepto los viernes de 09:30 a 14:30	Oficinas del adjudicatario.

4.2.3 Acuerdos de niveles de servicio, disponibilidad y operatividad

En este punto se establecen los acuerdos de niveles de servicio que como mínimo se exigen en este Pliego, y que regularan los términos de Prestación de Servicio, en lo que concierne a ANS, Disponibilidad, Soporte y Mantenimiento, Guardias y Desplazamientos.

4.2.4 Niveles de servicio en horario comprometido

Campus	Elemento	Prioridad	Tiempo Atención (Horas)
Servicios Compartidos	Atención	Todas	Mínimo 30 minutos
Servicios Compartidos	Resolución	Crítica	Máximo 4h + SLA HW
		Alta	Máximo 8h + SLA HW
		Media	Máximo 72h + SLA HW
CO *	Incidencia	Critica	Tiempo de atención: 1h Tiempo de escalamiento: 1h
		Severa	Tiempo de atención: 2h Tiempo de escalamiento: 2h
		Leve	Tiempo de atención: 4h Tiempo de escalamiento: 4h

Tipo Contingencia CO	Descripción
Tipo 1: Incidencia CRÍTICA	Incidencia que provoca problemas en la continuidad de los servicios de Producción.

Tipo 2: Incidencia SEVERA	Incidencia que provoca degradación de los servicios de Producción
Tipo 3: Incidencia LEVE	Incidencia que no tiene impacto, aunque si mensajes de error o informativos

*Si la contingencia no es resuelta en el tiempo máximo de escalamiento o si el operador de turno requiere soporte de más alto nivel, la contingencia se escala al Soporte de Segundo Nivel (Grupo Supervisión). El operador de turno informará telefónicamente esta acción al Jefe del CO.

Si la contingencia es resuelta en el plazo inferior al tiempo de escalamiento, el operador de turno registrará este evento y se informará al Grupo Gestión para su evaluación.

4.2.5 Disponibilidad en horario comprometido

Servicios	Nivel	Disponibilidad
Gestión de Identidades. Ciberseguridad. Correlación de Eventos al Centro de Operaciones.	ALTO	>=99%

4.3 Descripción de los trabajos a realizar

A continuación, detallamos la prestación de los Servicios para este pliego.

4.3.1 Servicios de Administración Avanzada de Gestión de Identidades y de Ciberseguridad

4.3.1.1 Introducción

El presente pliego de prescripciones técnicas tiene por objeto definir las condiciones para la definición de los Servicios de Administración Avanzada de Gestión de Identidades y de Ciberseguridad para ayudar al Instituto Nacional de Técnica Aeroespacial “Esteban Terradas” (INTA) en su proceso de transformación digital seguro.

En un mundo hiperconectado como el actual, implementar la seguridad en el ciberespacio se ha convertido en una prioridad estratégica. El nuevo escenario de guerra en el que se ha convertido el ciberespacio y lo sensible que es cualquier organización a cualquier disfunción TIC precisa garantizar un uso seguro y responsable de las redes y sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques potenciando y adoptando medidas específicas para contribuir a la promoción de un ciberespacio seguro y fiable.
Esto, acompañado del incremento de la adopción de los entornos de Nube o Híbridos aumenta en gran medida la superficie de ataque, y difumina el concepto de perímetro corporativo; lo que hace imprescindible mejorar la visibilidad y el control sobre los dispositivos, aplicaciones y servicios que existen en el organismo.

En INTA surge la necesidad de adaptar nuestras soluciones de seguridad TIC a este complejo escenario, con soluciones que combinan las tecnologías más avanzadas junto al conocimiento y

experiencia de profesionales altamente certificados. Además, el INTA debe seguir en su proceso de mejora continua, y adaptarse al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

El escenario necesario en Ciberseguridad está basado en la prevención, protección, detección y respuesta y en la Gestión de Identidades.

4.3.1.2 Descripción del servicio

El objeto del contrato a ejecutar en el marco del presente expediente es la prestación de los "Servicios de Administración Avanzada de Gestión de Identidades y de Ciberseguridad" que den respuesta a todas las necesidades identificadas en el presente pliego de prescripciones técnicas, proporcionando un entorno en el que la seguridad sea integral y funcional.

Adicionalmente, forman parte del objeto del contrato los trabajos de migración de configuraciones desde el sistema actual, así como la instalación, configuración, administración, mantenimiento, monitorización y escalado de todos los servicios propuestos por el adjudicatario en la fase de licitación y su adecuada integración con el actual sistema de información del INTA, incluida su reconfiguración para adaptarse a los posibles cambios de la institución a lo largo de la duración del periodo del contrato.

Igualmente, también forman parte del contrato todos los trabajos de devolución o transferencia del servicio, incluidos los datos, una vez terminada la vigencia del mismo.

Es parte integrante del contrato, proporcionar todas las licencias de base para la construcción del sistema, así como su mantenimiento y soporte durante la vigencia del contrato, independientemente de la modalidad de adquisición, suscripción o pago por uso que se establezca.

Igualmente, es parte del contrato cualquier coste por uso derivado de los distintos servicios ofertados.

Se establece también, como parte del objeto del contrato, definir y proporcionar la infraestructura necesaria en modo servicio para la puesta en producción del sistema de Ciberseguridad, así como el mantenimiento y gestión de la misma durante la vigencia del contrato de acuerdo al nivel de servicio definido.

Se trata, en definitiva, de un proyecto de servicios gestionados, al que se deberá dar respuesta. Todo ello de conformidad con lo establecido en el presente Pliego de Prescripciones Técnicas (PPT) y en el Pliego de Cláusulas Administrativas Particulares (PCAP).

4.3.1.3 Requisitos

Para ayudar a que el INTA tenga la conformidad según el ENS la empresa adjudicataria deberá realizar una auditoría de cumplimiento de ENS anual, que permita que la auditoría bi-anual de conformidad con el ENS que será realizada por una entidad de certificación acreditada por ENAC para expedir certificaciones de conformidad con el ENS, de acuerdo a la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, pueda ser superada por el INTA.
La empresa adjudicataria debe tener experiencia en auditorias tipo ENS en los últimos 5 años.
La empresa adjudicataria debe contar con Centros de Operaciones de Seguridad fuera de Europa, para que el INTA pueda adelantarse a posibles amenazas.

El Centro de Operaciones de Seguridad (SOC) debe poseer una experiencia mínima de cuatro años prestando el servicio de SOC

La empresa adjudicataria debe contar con la habilitación HSEM (Habilitación de Seguridad de Empresa), o tenerlo solicitado con fecha previa a la publicación de esta licitación, dado que en el INTA existen sistemas TIC que manejan información clasificada.

Los Servicios de Administración Avanzada de Gestión de Identidades y de Ciberseguridad ofrecerán las funcionalidades que se describen a continuación. Los productos actualmente en funcionamiento en el organismo dentro de su arquitectura de Seguridad que deberán de ser mantenidos (y pagados por la empresa adjudicataria) y administrados se encuentran en la columna Arquitectura TIC (dicha columna está *CLASIFICADA* y la empresa licitadora, deberá de consultarlo en la Tabla 1 *Servicios* completa, disponible en el ***Anexo A. Ciberseguridad***, que deberá de solicitar al INTA (a través de un email a <ciberseguridad_DTIC@inta.es>)

CATEGORÍA FUNCIONAL	SERVICIO	Arquitectura TIC
PREVENCIÓN	Jefe de Proyecto de Seguridad	*CLASIFICADA*
	Servicio de escaneo de vulnerabilidades y alertas	
	Servicio de Auditoría de Sistemas	
	Servicio de Bastionado de Sistemas	
PROTECCIÓN	Gestión de dispositivos	
	Limpieza de correo electrónico	
	Protección y trazabilidad del dato	
	Web Application Firewall (WAF)	
DETECCIÓN Y RESPUESTA	Servicio de protección del puesto de trabajo	
	Servicio de Análisis de Red	
	Servicio de respuesta ante incidentes y de análisis forense	
	Servicio SIEM en la nube	
	Servicio SIEM on premise	
GESTIÓN DE IDENTIDADES	Servicio de soporte a la Gestión de Identidades	

Tabla 1 Servicios

El personal responsable de la ejecución de cada uno de los servicios solicitados, tendrá que tener la **experiencia mínima** requerida en la Tabla 7, disponible en el citado ***Anexo A. Ciberseguridad***.

Las empresas licitadoras deberán incluir como parte de la documentación, los currículos del Equipo de Servicio ofertado, y cada uno de esos CV deberán estar firmados por el profesional correspondiente. Deberá aportarse un documento que certifique que los profesionales pertenecen efectivamente a la empresa licitadora o bien que, en el caso de que se subcontrate ese servicio, el currículum del profesional subcontratado.

Asimismo, deberán incluir el documento justificativo de Certificado de Informe de Vida Laboral del afiliado, profesional que pertenece a la empresa licitadora/subcontratada.

Las SLAs aplicables a los servicios son:

Req1	Los servicios deben proporcionar los siguientes SLAs: - SLA de atención mínimo: 30 minutos. - SLA de resolución mínimo: ▪ Crítico: 4 horas + SLA HW ▪ Alto: 8 horas + SLA HW ▪ Medio: 72 horas + SLA HW

4.3.1.3.1 Prevención

Los Servicios de Administración Avanzada de Gestión de Identidades y de Ciberseguridad se basan en la prevención mediante:

- Jefe de Proyecto de Seguridad.
- Servicio de escaneo de vulnerabilidades y alertas.
- Servicio de Auditoría de Sistemas.
- Servicio de Bastionado de Sistemas.
-

4.3.1.3.1.1 Jefe de Proyecto de Seguridad

La empresa adjudicataria deberá aportar un Jefe de Proyecto de Seguridad cuyo objetivo es ser el interlocutor principal en la fase de ejecución de los Servicios de Administración Avanzada de Gestión de Identidades y de Ciberseguridad aportando una visión global de todos los servicios de seguridad contratados por el INTA.

El Jefe de Proyecto de Seguridad será el responsable en fase de postventa de dichos servicios, controlando la calidad extremo a extremo de acuerdo con los compromisos adquiridos y en general, de impulsar la evolución de los servicios del INTA a lo largo de la vida del proyecto, siempre dentro del acuerdo establecido en el contrato.

El Jefe de Proyecto de Seguridad no será un recurso dedicado al INTA en exclusividad, estando su puesto de trabajo ubicado en las instalaciones de la empresa adjudicataria, y se desplazará a las instalaciones del INTA siempre que sea necesario.

Se detallan a continuación los requisitos exigibles al Jefe de Proyecto de Seguridad:

Req2	Responsabilidad ante el INTA de la provisión y explotación de los servicios que tenga contratados. Se ocupa de todos los proyectos nuevos que se contraten y es responsable de la planificación y seguimiento global de su implantación coordinando los equipos de trabajo involucrados.
Req3	Gestión externa e interna en la empresa adjudicataria de escalados de averías para todos los servicios de seguridad. Coordinación interna con los responsables de otros servicios de la empresa adjudicataria desde un punto de vista técnico.
Req4	Interlocución principal, tanto ante el INTA como internamente en la empresa adjudicataria, para la gestión de escalados y coordinaciones de incidencias de alto impacto relacionadas con las infraestructuras de seguridad.
Req5	Definición e implantación del modelo de gobierno y atención con el INTA, así como la aplicación de las metodologías actualizadas que conduzcan a la práctica de una cultura de Seguridad Informática.

Req6	Gestión de cambios y gestión de la configuración en el modelo/alcance de prestación del Servicio.
Req7	Visión extremo a extremo de la calidad del servicio prestada al INTA, seguimiento y control de los indicadores/SLAs, reporting al INTA y a la organización interna.
Req8	Definición y ejecución de procedimientos de actuación para garantizar la correcta provisión y explotación de los servicios, apoyándose en el resto de figuras/unidades dedicadas a la atención del INTA.
Req9	Definición y liderazgo de Planes de Mejora Continua de la prestación del servicio. Identificación de problemas tanto de seguridad como dentro del servicio, siendo responsable de la gestión de los mismos.
Req10	Asesoramiento sobre la constante evolución tecnológica y como ésta puede beneficiar o aumentar los niveles de seguridad existentes en el INTA.
Req11	Compartir los conocimientos sobre las mejores prácticas seguidas para garantizar la continuidad del negocio, la confidencialidad de la información y su integridad.

4.3.1.3.1.2 Servicio de escaneo de vulnerabilidades y alertas

El Servicio debe proporcionar una solución global integrando diferentes productos y herramientas de seguridad (que al menos debe contar con las definidas en la Tabla 1 disponible en el ***Anexo A. Ciberseguridad***) con la capacidad de ofrecer una gestión de vulnerabilidades end-to-end a través de un Portal del Servicio, y que permita realizar el seguimiento de una vulnerabilidad desde que se detecta hasta que se corrige.

El Portal del Servicio, deberá de integrarse con la solución de BMC Remedy instalada en el organismo.

El Servicio debe atender al siguiente esquema de funcionamiento:

- INTA, Portal del Servicio y Empresa adjudicataria son las tres partes en que se estructura el esquema de funcionamiento del servicio.
- El INTA es considerado una entidad en el Portal del Servicio que permite a los usuarios realizar el seguimiento del ciclo de vida de las vulnerabilidades que afectan a sus activos.
- Por otro lado, se encuentra la plataforma del servicio, donde se realiza detección de vulnerabilidades.
- Los resultados de la ejecución de herramientas de seguridad sobre los activos del INTA son inmediatamente cargados en el Portal del Servicio para seguidamente ser validados por el equipo de expertos del Servicio.

Adicionalmente, el Servicio debe poner a disposición del INTA la figura del Analista Local como canal de comunicación de confianza que entienda el contexto de los activos y, con ello, permita una mejor adaptación de los resultados a las necesidades del INTA, así como la priorización de vulnerabilidades y activos a proteger.

El Portal del Servicio es el interfaz principal que provee el Servicio a los usuarios, y centraliza la solicitud y entrega de informes, el envío de notificaciones y alertas, y entrega de resultados de las ejecuciones de las pruebas.

El Servicio de escaneo de vulnerabilidades y alertas debe componerse de los siguientes módulos:

- Alertas de vulnerabilidades.
- Análisis de vulnerabilidades.
- Escaneo de Aplicaciones Web.

Los requisitos del módulo de Alertas de vulnerabilidades son:

Req12	Una parte de la funcionalidad de este módulo consiste en relacionar el inventario actualizado de activos en formato Common Platform Enumeration (CPE) del INTA con la base de datos de vulnerabilidades publicadas por el National Institute of Standards and Technology (NIST) contenida en el feed Common Vulnerabilities and Exposures (CVE) al menos, dando como resultado las vulnerabilidades que afectan específicamente a sus activos. Así mismo habrá agentes desplegados en EndPoints y Servidores que de forma dinámica envíen información adicional sobre vulnerabilidades y caminos funcionales validos en los EndPoints y Servidores. El software debe de incluir una plataforma de gestión de rutas de ataque, descubre continuamente rutas de ataque ocultas a los activos críticos de la organización, calculando la ruta de ataque, con un gran arsenal de técnicas de ataque que incluyen vulnerabilidades, configuraciones incorrectas, actividades de los usuarios, problemas de credenciales y acceso a la red y totalmente automatizado. La plataforma brindará una priorización integral y soluciones enfocadas en las vulnerabilidades y debilidades que son explotables y conducen a sus activos críticos. INTA obetendrá recomendaciones de remediación detalladas y precisas, priorizados en función del riesgo y los cuellos de botella (eslabones más débiles), sin falsos positivos, con un modelo de seguridad proactivo. Para esos EndPoints INTA tiene desplegada la solución descrita en el ***Anexo A. Ciberseguridad*** en la Tabla 1 Servicios, que es necesario seguir manteniendo y administrando por parte del adjudicatario.
Req13	Cada nuevo resultado provoca, de forma automática, el envío de alertas y la generación de vulnerabilidades de la misma forma que si se detectara de forma proactiva. Estas vulnerabilidades son clasificadas como potenciales en el Portal del Servicio, posibilitando de esta forma el seguimiento del estado de las vulnerabilidades o la asignación de diferentes niveles de criticidad.
Req14	De forma general, este módulo no realiza un escaneo sobre los activos ni accede a ellos y necesita solamente una lista actualizada de activos tecnológicos con CPE asociado y la configuración de reglas para recibir alertas (y opcionalmente crear vulnerabilidades).
Req15	En su fase inicial, el INTA proporciona un listado de activos tecnológicos (elementos hardware y las versiones de software instalados, incluyendo sistemas operativos y paquetes software) y el Servicio lo cargará en el Portal del Cliente siguiendo el estándar de clasificación de activos CPE para tecnología de información de sistemas, software y paquetes. El Servicio ofrecerá flexibilidad para adecuarse a los recursos y características específicas del INTA para el mantenimiento continuo del inventario de activos.
Req16	Una vez que los activos tecnológicos están en el Portal del Cliente en formato CPE, el INTA puede establecer los criterios de configuración de las alertas automáticas en base a varios parámetros como la severidad según Common Vulnerability Scoring System (CVSS), cuándo ser notificado (diariamente, semanal o individual para cada vulnerabilidad), o el producto de una familia concreta, entre otros. No existe limitación en el número de reglas y cada usuario del Portal crea y recibe sus propias alertas respectivamente, aunque la gestión de vulnerabilidades es unificada.
Req17	La siguiente fase relaciona los activos del INTA en formato CPE con nueva entrada o actualización del feed CVE. Cada entrada CVE contiene un listado de activos CPE afectados y es comparada siguiendo las reglas anteriormente establecidas. Si se

	requiere, una vulnerabilidad en estado Potencial es también creada en el Portal lo que permite al INTA realizar su gestión.

Los requisitos del módulo de Análisis de vulnerabilidades son:

Req18	La funcionalidad de este módulo consiste en el uso de tecnología líder en el mercado (descrita en ***Anexo A. Ciberseguridad*** en la Tabla Servicios) que analiza los activos del INTA automáticamente con el fin de identificar vulnerabilidades potenciales en sus sistemas de información y descubrir nuevos sistemas, identificar puertos abiertos. Este módulo permite el escaneo interno usando una sonda de escaneo desplegada en las instalaciones del INTA.
Req19	En una primera fase se definen el conjunto de sistemas, redes y plataformas críticas para el INTA que formarán parte del alcance del módulo. Unido a ello, se acuerdan y planifican con el INTA las ejecuciones de los análisis, las franjas horarias de las pruebas de seguridad, la periodicidad de las pruebas, las posibles restricciones y las políticas de escaneo (pruebas a realizar) que mejor se ajusten a sus necesidades. Para ello, se indicarán al INTA los distintos tipos de políticas (las propias de la herramienta y las definidas por el equipo de expertos) y una descripción asociada a cada una de ellas.
Req20	La empresa adjudicataria debe tener en cuenta las siguientes consideraciones: - No se realizarán ataques de Denegación de Servicio. - En determinados tipos de prueba, se requerirán al INTA las credenciales de acceso necesarias para continuar con el proceso de análisis de vulnerabilidades. - El tipo de pruebas a realizar podrá diferir teniendo en cuenta el tipo de análisis, tiempo disponible para su ejecución y las evidencias descubiertas.
Req21	En base a la información acordada con el INTA, los expertos en seguridad de la empresa adjudicataria se encargan de realizar la configuración de las herramientas e iniciar la ejecución del proceso de análisis de vulnerabilidades. Es recomendable que el equipo de trabajo realice un escaneo de descubrimiento inicial con el fin de optimizar la ubicación de los elementos que escanean. Este proceso no requiere de la instalación de hardware adicional en la organización y no precisa de tareas de configuración por parte del INTA. No obstante, pese a que en los escaneos externos no es necesario software adicional, no ocurre lo mismo en los escaneos de redes internas, en los que sí es necesaria la instalación de un software adicional (sonda) en la infraestructura del INTA que será el encargado de realizar los escaneos. Esta instalación será llevaba a cabo por el INTA con el soporte del equipo de seguridad y Analista Local de la empresa adjudicataria.
Req22	Cuando la ejecución de las pruebas ha finalizado, los resultados de los análisis se cargan automáticamente en el Portal del Servicio al estar integrado con la tecnología descrita en ***Anexo A.*** , en la Tabla 1 Servicios, usada para el escaneo de vulnerabilidades. El equipo de expertos de seguridad de la empresa adjudicataria revisa los resultados obtenidos de las herramientas y valida las vulnerabilidades creadas en el Portal del Servicio.
Req23	El INTA dispone de los resultados de los escaneos en el Portal del Servicio según son reportados por las herramientas, y puede generar por él mismo y sin límite informes técnicos, de seguimiento y diferenciales que le permitan ver la evolución del servicio.

Los requisitos del módulo de Escaneo de Aplicaciones Web son:

Req24	El módulo de Escaneo de Aplicaciones Web encuentra balance entre el uso de pruebas automáticas y la experiencia y conocimientos de un pentester, ya que una herramienta no alcanza a simular completamente el comportamiento de una atacante y necesita una revisión de los resultados y, por otro lado, una evaluación continuada enteramente

	llevada a cabo por un equipo de seguridad sin el apoyo de herramientas automatizadas puede acarrear grandes costes económicos y recursos, sobre todo a la hora de la obtención y organización de la información.
Req25	Este módulo plantea el siguiente escenario: una plataforma que puede implementar de forma automática y continua (24x7) las fases que un atacante usa para intentar comprometer la seguridad de los sistemas de información de una empresa, junto con un equipo de seguridad cualificado que valide los resultados obtenidos por la plataforma, las vulnerabilidades descubiertas y recomendaciones brindadas.
Req26	El módulo Escaneo de Aplicaciones Web dispone de varias modalidades de funcionamiento para adaptarse mejor a las características y necesidades concretas del INTA, que podrá elegir la modalidad más conveniente contando siempre con el soporte del servicio. Cada una de estas modalidades dispone de una capacidad de ejecución de procesos concurrentes para el lanzamiento de tests y el análisis de las respuestas de éstos. Esta capacidad depende del número de Fully Qualified Domain Names (FQDNs) a escanear.
Req27	El límite de FQDNs representa una recomendación para poder cumplir con las demandas de prioridades y frecuencias de escaneo sobre los recursos del INTA, que dependen en gran medida del tamaño de los activos (número de URLs) y la complejidad de las páginas webs, elementos que a priori no se conocen.
Req28	Una vez elegido el plan, el INTA debe suministrar el listado de dominios que desea analizar indicando la prioridad deseable de escaneo sobre cada uno de ellos. Esta información será utilizada por el Servicio para el reparto de las capacidades de escaneo de Faast más adecuado.

El Servicio de escaneo de vulnerabilidades y alertas debe constar de un ciclo de vida formado por cuatro fases principales, que se desarrollan y repiten de manera cíclica.

El equipo de seguridad citado en las siguientes tablas hace referencia al adjudicatario, que ha de estar coordinado con el equipo de seguridad del INTA.

Req29	Planificación: En una fase inicial se acuerdan y planifican con el INTA el alcance, las franjas horarias y las posibles restricciones. En base a esta información, se provisiona el Servicio para que esté listo para que el equipo técnico de operaciones de la empresa adjudicataria ejecute las pruebas de seguridad.
Req30	Ejecución de las pruebas: Las pruebas de seguridad son ejecutadas en base a la planificación acordada usando herramientas de scanning que automatizan las fases de descubrimiento y análisis. Cada vulnerabilidad detectada es validada por el equipo de seguridad para descartar falsos positivos y determinar su severidad real. Las vulnerabilidades relevantes con CVSS (v2 y v3) > 7.0 son revisadas con mayor detalle para evaluar el riesgo que suponen para el INTA. Para ello, el equipo de seguridad lleva a cabo pruebas manuales de explotación.
Req31	Comunicación de resultados: El INTA puede acceder a los resultados (activos, vulnerabilidades, recomendaciones) a través del Portal del Servicio (informes, dashboards, proyectos) o por email (notificaciones automáticas, alerta de vulnerabilidades).
Req32	Gestión ciclo de vida de las vulnerabilidades: El Servicio proporciona un Portal de Servicio como plataforma de gestión de vulnerabilidades que permite realizar al INTA un seguimiento eficiente y efectivo, y una remediación priorizada de vulnerabilidades. El equipo de seguridad proporciona soporte en la remediación y ante cualquier petición relacionada con el Servicio como la entrega, resultados o alcance.

El equipo de seguridad se encarga de realizar las siguientes actividades:

Req33	**Formación** inicial sobre el Servicio y sus principales funcionalidades incluyendo el Portal del Cliente.
Req34	**Planificación** de las pruebas y provisión de las herramientas del Servicio en base a los requerimientos del INTA. El equipo de expertos proporciona soporte y recomendaciones en base a su experiencia para un aprovechamiento óptimo de recursos.
Req35	**Seguimiento de la ejecución de las pruebas** con herramientas automáticas para asegurar su correcto funcionamiento.
Req36	**Revisión de los resultados** de las pruebas de seguridad, lo que incluye el descubrimiento de activos, la verificación de ocurrencias y descarte de falsos positivos.
Req37	**Envío de correo de alerta temprana** para vulnerabilidades críticas con información detallada. Se realiza una prueba de concepto manual para determinar el riesgo real y el impacto en términos de confidencialidad, disponibilidad e integridad para el INTA.
Req38	**Soporte** ante solicitudes de mejora, peticiones de cambios en la provisión, dudas o incidencias relativas al Servicio indicadas en la sección de Escalado y Soporte.
Req39	En el equipo de seguridad se integra la figura del **Analista Local** que es un rol orientado a la relación con el INTA para comprender y trasladar sus necesidades ayudando en la entrega del Servicio durante la duración de este. El Analista Local se encargará de realizar el soporte inicial y seguimiento posterior.

4.3.1.3.1.3 Servicio de Auditoría de Sistemas

Los requisitos del Servicio de Auditoría de Sistemas son:

Req40	Se realizará una Auditoría de Sistemas al año según lo requerido por la siguiente legislación del ENS y RGPD: - *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).* - *Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.* - *Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.* - *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.* - *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.*
Req41	La empresa adjudicataria realizará una auditoria cada dos años por una entidad de certificación acreditada por ENAC para expedir certificaciones de conformidad con el ENS, de acuerdo a la *Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad*.
Req42	Este servicio no será responsable de aplicar las medidas para solucionar o mitigar las vulnerabilidades encontradas durante la auditoría.

4.3.1.3.1.4 Servicio de Bastionado de Sistemas

Los requisitos del Servicio de Bastionado de Sistemas son:

Req43	Se realizarán dos guías de bastionado de sistemas o procedimientos de seguridad, determinados por el INTA, al año.

Req44	Las guías de bastionado de sistemas deberán incluir las políticas de seguridad, privilegios y configuraciones a aplicar necesarios para securizar el sistema.
Req45	Este servicio no será responsable de aplicar dichas guías de bastionado sobre los sistemas, pero sí de verificar que están correctamente aplicadas.

4.3.1.3.2 Protección

Los Servicios de Administración Avanzada de Gestión de Identidades y de Ciberseguridad se basan en la protección mediante:

- Gestión de dispositivos.
- Limpieza de correo electrónico.
- Protección y trazabilidad del dato.
- Web Application Firewall (WAF).
-

4.3.1.3.2.1 Gestión de dispositivos

El servicio de Gestión de dispositivos incluye:

- Administración delegada.
- Mantenimiento.
- Soporte especializado.
- Supervisión de salud.
- Administración y despliegue de la solución de MDM en dispositivos móviles.

Los requisitos del servicio Gestión de dispositivos son:

Req46	**Control remoto de las operaciones de los dispositivos de seguridad** del INTA en un horario de 24x7.
Req47	El listado de elementos que se deben de administrar en el servicio de Gestión de dispositivos se encuentra disponible en el ***Anexo A. Ciberseguridad***.
Req48	**Resolución de Incidencias**. La empresa adjudicataria colaborará en la revisión de la configuración y eventos de los equipos que administra para ayudar al INTA a solventar caídas en servicios críticos de sus procesos de negocio, independientemente de donde sea su origen, y activará todos los mecanismos de resolución que permitan solventar el problema en el menor tiempo posible.
Req49	**Participación en incidentes de seguridad**. La empresa adjudicataria participará en el descubrimiento de los orígenes y mitigación dentro del alcance de la visión que le proporcionan los equipos administrados de los incidentes de seguridad, no siendo en ningún caso la responsable de coordinar la gestión ni la respuesta ante dichos incidentes salvo que se haya indicado explícitamente por parte de INTA.
Req50	**Resolución de solicitudes realizadas por INTA.** Contempla la realización de las tareas de operación solicitadas por el INTA y tipificadas dentro del servicio.
Req51	**Planificación y ejecución de cambios**. Contempla el estudio y realización de los cambios sobre los elementos administrados que solicite el INTA o que sean recomendados desde el grupo de administración o desde el grupo de soporte de dispositivos, en base a las mejores prácticas o normativas de administración estándares o como solución ante una incidencia o incidente de seguridad. Los cambios solicitados cuya prioridad sea baja o media, se ejecutarán en la siguiente ventana de mantenimiento acordada con el INTA. A la hora de medir el ANS de este tipo de cambios, se tendrá en cuenta el momento en el que se planificó el ticket en una de las ventanas de mantenimiento y no el de la propia ventana.

	Los cambios con prioridad alta o crítica se atenderán bajo demanda, respetando el ANS comprometido.
Req52	**Actualización del software del dispositivo**. Se encuentran incluidas dentro de las tareas propias del servicio la actualización del propio software siempre que se cumpla alguna de las siguientes condiciones: - La actualización esté recomendada para la corrección de una vulnerabilidad detectada en la versión actual. - Dicha actualización incluya una nueva funcionalidad disponible en la nueva versión que ha sido requerida por el INTA. - La versión actual haya sido identificada por el fabricante como EOL y, por tanto, sea necesaria la actualización a una versión que siga estando bajo soporte del fabricante. Las actualizaciones se realizarán dentro de las ventanas de mantenimiento acordadas entre el INTA y la empresa adjudicataria.
Req53	**Corrección de vulnerabilidades identificadas en el equipamiento**. El servicio se encargará de la realización de los cambios necesarios para subsanar vulnerabilidades encontradas en el equipamiento incluido en el alcance del presente PPT. La resolución de las vulnerabilidades se realizará en las ventanas de mantenimiento definidas y en función del nivel de severidad asociado a la vulnerabilidad.
Req54	**Registro y control de las peticiones del servicio**. Todas las peticiones del servicio se recogerán mediante la herramienta de ticketing del INTA.
Req55	**Notificación automática de las alertas de seguridad** generadas por el equipamiento incluido en el alcance del presente pliego, limitando el formato y configuración de dicha notificación a la funcionalidad ofrecida por cada fabricante.
Req56	**Tareas correspondientes a Mantenimiento, Soporte Especializado y Supervisión de salud** en aquellos dispositivos contemplados en el alcance del presente pliego.

4.3.1.3.2.2 Limpieza de correo electrónico

El servicio de Limpieza de correo electrónico consiste en la administración especializada de la protección del correo electrónico frente a cualquier tipo de ataque (por ejemplo: ransomware, Business Email Compromise, ataques de suplantación de identidad, etc).

Los requisitos del servicio de Limpieza de correo electrónico son:

Req57	La empresa adjudicataria deberá mantener y administrar al menos las herramientas indicadas en la *Tabla 1* disponible en el ***Anexo A. Ciberseguridad*** para el servicio de Limpieza de correo electrónico, sin que esto sea excluyente de la incorporación de otras herramientas. Por lo tanto, los licitadores podrán proponer herramientas adicionales a las actualmente instaladas en la arquitectura del INTA.
Req58	**Protección del correo electrónico**. El servicio permite proteger a su personal, sus datos y su marca de las amenazas actuales y de las molestias más comunes como: Impostor email, Phishing, Malware, Spam, Bulk mail.
Req59	**Continuidad del correo electrónico**. El servicio permite proteger la continuidad del correo electrónico, mitigando el riesgo de pérdida de productividad. Permite a los usuarios enviar y recibir correo electrónico en caso de una interrupción, sin ninguna otra acción.
Req60	**Protección contra Ataque Dirigido**. El servicio ayuda a detectar, mitigar y bloquear las amenazas avanzadas que se dirigen a las personas a través del correo electrónico. Esto incluye los ataques que utilizan archivos adjuntos y URLs maliciosas para instalar malware o engañar a los usuarios para que compartan contraseñas e información confidencial. La Protección contra Ataque Dirigido también detecta las amenazas y los

	riesgos en las aplicaciones en la nube y conecta los ataques por correo electrónico relacionados con el robo de credenciales u otros ataques. Este servicio bloquea y pone en cuarentena los mensajes con archivos adjuntos maliciosos o URLs maliciosas. Al no llegar nunca a la bandeja de entrada, los usuarios no pueden hacen clic en ellos y así no pueden verse comprometidos.
Req61	**Descarte automático de respuesta a amenazas**. El servicio permite a los administradores de mensajería y seguridad analizar los correos electrónicos y mover los correos maliciosos o no deseados a la cuarentena, después de su entrega. Sigue el correo reenviado y las listas de distribución y crea un rastro de actividad auditable. El servicio también enriquece las alertas de correo electrónico, creando asociaciones entre los destinatarios y las identidades de los usuarios, revelando las campañas asociadas, e incluso sacando a la luz las direcciones IP y los dominios del ataque que están en las listas de reputación e inteligencia. El servicio es incluso lo suficientemente inteligente como para tomar acciones automatizadas basadas en los usuarios objetivo que pertenecen a departamentos o grupos específicos con permisos especiales. Además, también sigue los correos electrónicos reenviados, por lo que, si un correo electrónico dirigido se reenvía a un usuario, a varios usuarios o a una lista de distribución, intentará seguir y poner en cuarentena esos correos también, informando del estado de cuarentena y de lectura de cada mensaje. El servicio automatiza el proceso de eliminación de los mensajes no deseados o inapropiados, o los que violan la política de cumplimiento. El servicio está diseñado para automatizar la cuarentena o la eliminación de los mensajes de correo electrónico maliciosos después de recibir una alerta de Protección contra Ataque Dirigido u otros sistemas de seguridad. En los casos en los que no hay amenazas, el servicio ingiere un archivo CSV con la información de los mensajes y, mediante programación, accede al buzón de cada destinatario, encuentra el mensaje, lo mueve a la cuarentena y, a continuación, busca las versiones reenviadas del mensaje. El servicio repite este proceso hasta que se retiran todos los mensajes. Todas las acciones de los mensajes se documentan junto con el estado de lectura de los mismos.
Req62	**Defensa del correo electrónico interno**. El servicio: - Ofrece la posibilidad de ayudar a detectar las cuentas comprometidas. - Permite aumentar la protección con un sólido antispam y un escaneo de malware multicapa. - Protege contra las URL y los archivos adjuntos malintencionados, incluido el aislamiento de archivos adjuntos. - Identifica rápidamente las cuentas comprometidas y toma las medidas necesarias. - Reduce el tiempo para contener y poner en cuarentena las amenazas del correo electrónico. - Reduce el tiempo de exposición a los correos electrónicos maliciosos. - Pone en cuarentena los mensajes reenviados a personas o listas de distribución. - Proporciona sólidos informes para obtener rápidamente los detalles de las cuentas comprometidas, junto con las alertas automáticas para los cambios de incidentes o la confirmación de la cuarentena.
Req63	**Archivado.** El servicio proporciona las herramientas necesarias para hacer frente a las necesidades de información empresarial y reglamentaria a largo plazo. El servicio: - Reduce los costes administrativos y de infraestructura con una solución de archivo moderna y nativa de la nube. - Supervisa las comunicaciones digitales. - Permite acceder a información relevante para investigaciones internas y auditorías. - Mantiene las comunicaciones en un archivo seguro, accesible y conforme a la normativa.

	- Permite que los usuarios busquen su propia información archivada.
Req64	**Defensa de cuentas de correo en la nube**. El servicio protege al INTA de las cuentas hakeadas de Microsoft Office 365 y Google G Suite. Permite detectar, investigar y defenderse de los ciberdelincuentes que acceden a sus datos confidenciales y cuentas de confianza. El servicio identifica la actividad sospechosa de la cuenta, bloquea las amenazas de fuerza bruta en la nube y crea políticas para priorizar y actuar ante las alertas. - Detecta amenazas de cuentas en la nube desde todos los ángulos. - Permite crear políticas adaptadas a la empresa, priorizar alertas y vigilar de cerca a sus usuarios en riesgo.
Req65	**Protección de Información.** El servicio incluye **cifrado de correo**, para que los usuarios no necesiten encriptar manualmente su correo electrónico para enviar y recibir mensajes de forma segura, simplemente sucede en segundo plano. El cifrado de correo electrónico simplifica las comunicaciones seguras y le deja el control. El servicio incluye **Prevención de Perdida de Datos de Correo**, para mitigar el riesgo de violación de datos a través del correo electrónico al detectar datos sensibles e información confidencial y evita que se filtren fuera del INTA por correo electrónico. Clasifica con precisión la información confidencial, detecta las transmisiones de exfiltración de datos a través del correo electrónico y detiene la pérdida de datos críticos. El servicio incluye la funcionalidad de **compartir información de modo seguro**, para optimizar la experiencia de los usuarios en el intercambio de archivos grandes o sensibles a través del correo electrónico, garantizando al mismo tiempo que se compartan de forma segura y cumpliendo las normas comunes de protección de datos. La funcionalidad de compartir información de modo seguro debe estár integrada con la prevención de perdida de datos de correo y el cifrado de correo, para aplicar reglas y ofrecer los mismos beneficios de codificación para comunicaciones seguras.
Req66	El servicio de Limpieza de correo electrónico: - Debe estar 100% administrado por personal de ciberseguridad de la empresa adjudicataria especializado en la protección de correo electrónico. La empresa adjudicataria debe disponer entre su personal, en el momento de la licitación, de especialistas en Ciberseguridad de alta cualificación y certificación, con una gran experiencia en la resolución temprana y eficaz de incidentes de seguridad recibidos a través del correo electrónico. - El horario de soporte a incidencias es 24x365. - El horario para peticiones y cambios es 8x5. - Debe customizarse progresivamente, vía solicitud de cambios. - Debe proporcionar informes semanales de salud de la plataforma y estadísticos de seguridad. - Debe proporcionar informes mensuales de los indicadores claves de actuación. - Debe cumplir los acuerdos de nivel de servicio. - Debe cumplir los objetivos de nivel de servicio. - Soporte a personal VIP del INTA. - Incluye Análisis forense, en tiempo real, hasta 30 días atrás.

4.3.1.3.2.3 Protección y trazabilidad del dato

Los requisitos del servicio de Protección y trazabilidad del dato son:

Req67	La empresa adjudicataria deberá mantener, evolucionar y administrar la instalación de la herramienta descrita en el ***Anexo A. Ciberseguridad***, en la Tabla 1 Servicios.
Req68	El servicio de Protección y trazabilidad del dato deberá constar de las siguientes fases:

1. **Fase de análisis de las necesidades de confidencialidad y Planificación**: En esta fase se analizarán las necesidades de confidencialidad de las distintas unidades de la organización incluidas en el proyecto, así como la necesaria clasificación de la información a aplicar en las políticas de acceso a la documentación. Será necesaria la celebración de reuniones con las unidades identificadas, usuarios del sistema, y consensuar las políticas a aplicar en el sistema que da soporte al proceso.
   La empresa adjudicataria deberá realizar una fase de análisis de qué políticas de protección conviene crear y a qué usuarios asignarlas para que la puesta en marcha sea lo más sencilla posible.
   También deberá analizar la infraestructura preexistente y planificar la integración con los diferentes sistemas de información que participan en el piloto. Será especialmente importante la integración con el sistema de autenticación y autorización de la organización (Directorio Activo) para gestionar la identidad de los usuarios.
   Adicionalmente, en esta fase se realizará una planificación marcando fechas concretas para el despliegue de la solución. Estas fechas deben ser acordadas con el INTA.
   El entregable de esta fase deberá ser un plan detallado del proyecto con el análisis de necesidades inicial de confidencialidad y de configuración de la solución, la estrategia de implantación que recoja la integración con los sistemas de la organización, las fases e hitos asociados y una planificación de fechas.

2. **Instalación del Sistema:** Al tratarse de un software en la modalidad SaaS (Software as a Service), no hay una instalación del producto propiamente dicha en los servidores del INTA, sino una configuración inicial del producto en la nube, que permita su uso por usuarios del INTA. Para ello, se requiere la instalación y configuración del software necesario para proporcionar la integración con el Directorio Activo de la organización a través de un conector AD/LDAP. Asimismo, se tiene que efectuar una instalación de un complemento software en los servidores de ficheros donde sea necesario por requerirse la protección de la información que contienen. El software se probará con una serie de usuarios y escenarios de prueba para asegurar que la instalación se ha realizado de forma completa y tiene la calidad adecuada para pasar a la fase siguiente.

   Las actividades a realizar en esta fase serán:
   - Comprobación requisitos previos.
   - Integración del conector AD/LDAP.
   - Instalación de CARLA para Servidores de Ficheros para proteger carpetas compartidas o librerías de SharePoint.
   - Ejecución de pruebas básicas sobre la instalación.

   La etapa finalizará con las siguientes entregas:
   - Guía de despliegue: descripción de los pasos realizados durante la instalación de los distintos componentes.
   - Plan de test de aceptación del sistema: plan de pruebas que se realizarán en la fase siguiente como base para dar por finalizado el despliegue.
   - Software empleado durante la instalación: los instaladores y ficheros de configuración a partir de los cuales se ha realizado la instalación.

	▪ Backups de forma que podría ser posible crear de cero un sistema de cero en el improbable caso de que se diera una pérdida completa del sistema. ▪ Software instalado y con pruebas básicas realizadas: resultado con éxito de las pruebas básicas con las que se termina esta fase. **3. Despliegue del Sistema:** En esta etapa la plataforma instalada será configurada para la distribución del software cliente para ser instalados en desktops. Las actividades a realizar en esta fase serán: ▪ Configuración de Directorios Activos que deben ser integrados en el sistema. ▪ Creación de organizaciones. ▪ Alta de usuarios protectores en cada una de las organizaciones. ▪ Configuración de alta automática de usuarios internos consumidores en la organización correspondiente. ▪ Configuración de alta de usuarios externos. ▪ Instalación del software para usuarios internos. ▪ Ejecución del plan de test de aceptación del sistema. Los entregables de esta fase serán los siguientes: ▪ Resultados de la ejecución de los test de aceptación del sistema. ▪ Guía de operaciones. ▪ Software configurado y disponible para los usuarios finales. ▪ Software certificado con las pruebas de aceptación del sistema. **4. Formación.** En esta fase, punto final del arranque del proyecto, se realizará una formación tanto a usuarios del Dpto. TIC del INTA, como a usuarios de las áreas de negocio incluidas en el piloto. La etapa finaliza con las siguientes entregas: ▪ Guía de usuario y administrador. ▪ Manual de buenas prácticas. ▪ Presentaciones de formación y materiales (prácticas). ▪ Realización de las sesiones de formación a usuarios. **5. Garantía.** Una vez arrancado y en funcionamiento el proyecto piloto, el adjudicatario garantizará el correcto funcionamiento de la solución al INTA y apoyo a los usuarios durante la duración del contrato.

4.3.1.3.2.4 Web Application Firewall (WAF)

El WAF es una solución avanzada de protección de sitios web y aplicaciones web del organismo en Internet.

Los requisitos del WAF son:

Req69	El WAF detecta el tráfico anómalo hacia los sitios web del INTA en Internet actuando como intermediador y protector de dicho tráfico. La función del WAF es filtrar el tráfico dirigido a los sitios web del organismo de manera que bloqueará el tráfico detectado como ataque de aplicación y dejará pasar aquel tráfico detectado como legítimo. El organismo tiene actualmente desplegada una solución on premise de WAF (consultar la Tabla 1 Servicios en el ***Anexo A. Ciberseguridad***).
Req70	Se debe dar un servicio de administración del dispositivo WAF del organismo.
Req71	Se debe dar un servicio de consultoría/parametrización del WAF sobre nuevos servicios a proteger detrás del WAF.
Req72	El servicio WAF incluye: - Protección de todo tipo de webs. - Inspección de tráfico http y https. - Aprendizaje automatizado y personalizado. - Protección integral (ataques de fuerza bruta, buffer overflows, manipulación de cookies y campos, SQL injection, etc.). - Visibilidad.
Req73	El servicio WAF debe ser capaz de limpiar el tráfico permitiendo el paso del legítimo mientras detiene los ataques al filtrar el tráfico malicioso.
Req74	Para asegurar la calidad del servicio WAF éste deber ser gestionado por un equipo de la empresa adjudicataria especializado en ciberseguridad en sitios web y tecnología WAF.

4.3.1.3.3 Detección y respuesta

Los Servicios de Administración Avanzada de Gestión de Identidades y de Ciberseguridad se basan en la detección y respuesta mediante:

- Servicio de protección del puesto de trabajo.
- Servicio de respuesta ante incidentes y de análisis forense.
- Servicio SIEM en la nube.
- Servicio SIEM on premise.

4.3.1.3.3.1 Servicio de protección del puesto de trabajo

El servicio de protección del puesto de trabajo debe:

Req75	Estar basado en la tecnología descrita en el ***Anexo A. Ciberseguridad***, en la Tabla 1 Servicios. Las soluciones descritas en la Tabla 6 Elementos de Ciberseguridad del ***Anexo A. Ciberseguridad***, deben de ser totalmente compatibles debiendo interactuar dentro del endpoint sin mantener ningún problema técnico conocido. El adjudicatario deberá mantener, evolucionar y administrar la solución, con las funcionalidades de: • Visibilidad completa en ataque. • Inteligencia de amenazas integrada. • Control y respuesta. La empresa adjudicataria deberá verificar y remediar las incidencias de seguridad detectadas en los EndPoints, incluyendo las derivadas del centro de operaciones de seguridad. Asimismo, deberá hacer el seguimiento (abriendo, actualizando y cerrando las incidencias/ordenes de trabajo tanto en

	las herramientas corporativas como en las herramientas del CCN, como LUCIA, etc.). Debido al complejo ecosistema de investigación del organismo, la herramienta XDR además de las funcionalidades habitualmente cubiertas por las soluciones de protección de puesto de trabajo, debe de cubrir los siguientes requisitos: **Requisitos Generales** 1. La solución deberá disponer de un sistema EDR con funciones en pre-ejecución **que no esté basado en Firmas clásicas** para detectar malware. **Requisitos, control y respuesta** 1. Capacidad de creación de flujos de trabajo mediante interfaz visual en la propia plataforma. 2. Los disparadores de acciones deben poder provenir tanto de detecciones como de auditoría de elementos cloud o de la ejecución de un flujo de trabajo previo. 3. Las condiciones han de poder incluirse tanto de forma secuencial como paralela y deben incluir tanto las acciones tomadas por la plataforma durante la detección como cualquier elemento que define las características de un endpoint concreto o su pertenencia a un grupo determinado. 4. Acciones de respuesta: entre las acciones de respuesta posibles deben incluirse al menos las siguientes: a. Contención de red de un endpoint. b. Actualización del contenido de la detección. c. Exposición de URL para orquestar con elementos terceros. d. Enriquecimiento mediante infomación de terceros (Ejemplo: Virus Total). e. Notificaciones automáticas vía Email, Teams o Slack. f. Obtención y borrado de ficheros del endpoint. g. Obtención de procesos y conexiones activas del endpoint. h. Creación de Tickets en Service Now y Remedy. 5. Debe poder disponerse de un versionado de los playbooks o flujos de trabajo creados. 6. Debe proporcionar un log de ejecución del flujo de trabajo creado. 7. Todos los eventos de telemetría del endpoint podrán usarse como elementos de una condición.

4.3.1.3.3.2 Servicio de Análisis de Red

Los requisitos del servicio de Análisis de Red son:

Req76	La empresa adjudicataria deberá mantener y administrar al menos las herramientas indicadas en la *Tabla 1* disponible en el ***Anexo A. Ciberseguridad*** para el servicio de Análisis de Red, sin que esto sea excluyente de la incorporación de otras herramientas. Por lo tanto, los licitadores podrán proponer herramientas adicionales a las actualmente instaladas en la arquitectura del INTA.

Req77	El servicio de Análisis de Red debe proporcionar una solución para la monitorización de ciberseguridad de las redes TIC en paralelo, no en línea, y sin agentes, mediante inteligencia artificial que autoaprende del entorno donde se instala, con detección de ciberamenazas, análisis automático de las mismas y creación de informes de incidentes automáticos tras la investigación autónoma del sistema.
Req78	La solución de inteligencia artificial debe cumplir con los siguientes requerimientos: • Despliegue en forma de hardware, que no necesite conectarse a Internet o al fabricante para almacenar, analizar y comunicar alertas e informes. • El HW deberá disponer de: - Puertos de análisis = 1 x 1Gbe + 2 x 1Gbe / 10Gbe + 2 x SFP - Poder ampliar estos puertos de análisis en el mismo applaince - Soportar tráfico de 5 Gbps - Poder monitorizar hasta un mínimo de 25.000 dispositivos en un solo appliance - Soportar hasta 100.000 conexiones por minuto analizadas • Debe poder actualizarse off-line • Debe ser una solución escalable fácilmente a diferentes ubicaciones, entornos digitales y volúmenes de dispositivos y usuarios • No se necesiten licencias adicionales ni componentes externos (Windows, SQL u otros) para ejecutar la solución. • Debe ofrecer la posibilidad de mejorar el licenciamiento, previo acuerdo y pago, para ofrecer Respuesta o Neutralización automática de las ciberamenazas detectadas sin necesidad de utilizar software o hardware de terceros, como FW o terceras herramientas para neutralizar las amenazas. • Posibilidad de ampliar la cobertura de monitorización y detección y respuesta de ciberseguridad más allá de la red, en entornos de aplicaciones SaaS, endpoints fuera de la red, Cloud o Email • La solución no debe requerir de sets de datos de aprendizaje preparados para su configuración y aprendizaje, sino que debe autoaprender allá donde se instale • La solución debe proporcionar una aplicación móvil para poder consultar las alertas y los informes de incidentes que crea automáticamente. • La solución debe incluir al menos: - Detección de comportamientos anormales de uso - Detección de comportamientos anormales del huésped - Detección de comunicaciones con servidores de mando y control - Detección de movimientos inusuales en la actividad de navegación - Detección de amenazas persistentes avanzadas (APT) - Detección de la actividad de los virus en la red - Detección de tráfico hacia sitios sospechosos - Detección de escaneos de direcciones y puertos - Detección de vulnerabilidades de día 0 - Detección de evasión de protocolos (por ejemplo, envío de datos maliciosos a través del protocolo DNS) - Detección de conexiones y máquinas TOR - Detección de algoritmos de generación de nombres de dominio

	- Detección de descargas de archivos sospechosos - Detección de movimientos laterales - Detección de la exfiltración de datos - Detección de escalada de privilegios - Detección de comandos de control - Detección de intentos de fuerza bruta - Detección del uso inapropiado de RDP, SSH, etc. - Detección del uso malicioso de los protocolos SMB y DNS - Detección de conexiones de red inusuales - Detección de actividades inusuales de los usuarios - Detección del uso indebido de herramientas de acceso remoto - La solución debe detectar las amenazas internas, como la filtración de información sensible por parte de empleados descontentos, el uso indebido de los accesos por parte de los administradores, la supervisión de la actividad de los empleados que se marchan • Clasificación de las amenazas por tipo o gravedad • Captura de muestras de tráfico en formato pcap • Envío de alertas por correo electrónico y Syslog • La solución debe supervisar, analizar y aprender automáticamente los comportamientos normales y anormales para construir un modelo de comportamiento de la organización y de cada dispositivo, y alertar a los administradores de los comportamientos anormales detectados. • La solución debe contar con múltiples algoritmos de aprendizaje automático que abarquen tanto el aprendizaje supervisado como el no supervisado. • La solución debe utilizar múltiples métodos de análisis estadístico • La solución debe ser capaz de identificar métodos de ataque desconocidos de amenazas externas e internas • La solución debe ser capaz de analizar y perfilar las entidades de la red para descubrir los primeros indicios de una brecha y el comportamiento malicioso subyacente para identificar a los actores de la amenaza que se esconden a la vista. • La solución debe ser capaz de alertar si se está haciendo un uso indebido o detectar si la entidad o uno de sus activos TIC se comporta con normalidad comparando los patrones de uso de los puertos históricos y actuales, si se están utilizando los protocolos correctos en los puertos a los que se accede y obteniendo visibilidad de las relaciones con otras entidades de la red. • La solución debe ser capaz de detectar las amenazas, aprender y adaptarse a los patrones de los usuarios, y hacer un seguimiento de todo, registrando cada ataque para una adecuada priorización que permita identificar qué entidad es la más peligrosa al entender que puede causar una crisis, o es algo de lo que hay que tener cuidado, o necesita ser vigilado de cerca, o necesita ser implementado inmediatamente. • La solución debe ser capaz de asignar a cada comportamiento o patrón anormal una puntuación de amenaza y una clasificación. Igualmente, debe poder mapear las amenazas en la *kill chain* y en la matriz del MITRE ATT@CK

	• La solución debe utilizar algoritmos avanzados de aprendizaje automático para procesar rápidamente grandes cantidades de datos y proporcionar un análisis comparativo contra una serie de amenazas internas y externas para ayudar a las organizaciones a defenderse de las amenazas modernas. • La solución debe permitir etiquetar redes, dispositivos, etc. Así como asignar prioridades o niveles de importancia a los dispositivos y alertas • La solución debe utilizar múltiples algoritmos de agrupación y clasificación para agrupar las anomalías de modo que el analista pueda determinar si varios sistemas forman parte de la misma anomalía. • La solución deberá analizar automáticamente las alertas de detección disparadas, y poder contextualizarlas y correlacionarlas entre sí, preparando informes sencillos y fácilmente comprensibles sobre los incidentes de ciberseguridad • La solución debe ser sin agente, basada en el dispositivo, que no requiera agentes en los puntos finales y sistemas. Por lo tanto, una huella cero en nuestros terminales y sistemas. Pero deberá permitir esta posibilidad en los casos de dispositivos portátiles de usuarios. • La solución debe proporcionar escalabilidad con una arquitectura única para escalar a través de grandes redes empresariales con una sobrecarga mínima • La solución debe admitir puertos de red de cobre o fibra • La solución debe soportar un entorno distribuido con una combinación de dispositivos físicos y virtuales • La solución debe ser instalada en local y no debe transferir datos a la nube para su análisis. • La solución debe tener capacidades de búsqueda avanzada de los datos de cabecera de las comunicaciones y logs. No debe requerir una sintaxis compleja ni un generador de búsqueda basado en un lenguaje de consulta. • La solución debe proporcionar muestras de capturas de paquetes para las anomalías detectadas • La solución debe registrar al menos los últimos 30 días de metadatos en el dispositivo, y debe ser capaz de consultar los metadatos históricos utilizando la funcionalidad de búsqueda • La solución debe admitir la toma de huellas dactilares de las comunicaciones encriptadas, como las SSL • La solución debe ofrecer una opción para que el usuario pueda guardar el filtro de búsqueda para su uso futuro. • La solución deberá proporcionar al administrador capacidades de generación y modificación de algoritmos. • La solución debe permitir archivar y restaurar las alertas y configuraciones • La solución debe proporcionar una visión del tráfico y los ataques dirigidos al entorno desde una perspectiva global. • La solución debe mapear visualmente los usuarios y las entidades en riesgo en una matriz de puntuación fácil de entender. • Debe permitir modificar los algoritmos de detección y acción existentes, así como poder crear nuevos.

	• La solución debe proporcionar un inventario de activos a través de la detección automatizada. • La solución debe permitir integraciones con sistemas de Directorio Activo, VPN, EDRs o herramientas ZeroTrust, así como enviar datos a herramientas SIEM o de gestión de tiquetes • La solución debe integrarse en la arquitectura existente sin requerir ponerse en línea con el tráfico, sino analizar y responder en paralelo. • Posibilidad de ampliar con agentes ligeros en endpoints de Windows, Linux y MAC. • La solución debe poder desplegar sondas virtuales en hipervisores de VMware, KVH o HyperV, para poder monitorizar también tráfico desde switches virtuales. • La solución debe poder realizar correctamente la traza del dispositivo final y las credenciales, cuando se utilizan *terminal servers o virtual desktops*, mediante un agente ligero que permita rastrear correctamente cada sesión de TS o VDI • Los datos recogidos deben permanecer en el almacenamiento local de la solución y en ningún caso salir de la red para ser procesados en la nube del proveedor. • Disponibilidad de API basada en JSON • Debe permitir la creación de diferentes perfiles de usuario y permisos • Debe poseer de un log de registro de actividad de usuarios en la plataforma • Solución Debe monitorear su propia salud y debe proporcionar un resultado de diagnóstico resumido al administrador para varios factores, pero no limitado a la RAM, el uso de la CPU, la carga de la red, etc. • La solución deberá ser capaz de integrarse con el servidor de Active Directory para el inicio de sesión y deberá soportar controles de acceso basados en grupos. Igualmente deberá poder integrarse con el AD para poder traer datos de usuarios cuando surja una alerta relacionada con una credencial • La solución deberá ser capaz de realizar copias de seguridad automatizadas de la configuración en momentos programados.
Req79	El servicio de Análisis de Red debe proporcionar un único panel de control y la herramienta de análisis de red debe tener conectores listos para usar con las plataformas de registro más utilizadas para que tanto las consultas de búsqueda como la extracción, el análisis y la evaluación se puedan realizar desde dicho panel de control.
Req80	El servicio de Análisis de Red debe ser capaz de recuperar cada registro, analizarlo, alimentar al motor de ML en busca de anomalías y ejecutarse a través de firmas interactivas para adquirir inteligencia e información sobre amenazas.
Req81	El servicio de Análisis de Red también debe ofrecer la posibilidad de realizar búsquedas de lenguaje natural en tiempo real en cada registro.
Req82	El servicio de Análisis de red debe dar servicio a múltiples sedes con múltiples usuarios a los que se les podrá dar diferentes roles de visualización y derechos de uso.
Req83	El servicio debe realizar Análisis de Logs y Análisis de tráfico de red con Machine learning, para la detección de Anomalías.

4.3.1.3.3.3 Servicio de respuesta ante incidentes y de análisis forense

Los requisitos del servicio de respuesta ante incidentes y de análisis forense son:

Req84	Incluye **asistencia 24x7x365 a través de línea telefónica.** El INTA puede llamar a la línea directa de Respuesta ante incidentes 24x7x365 de la empresa adjudicataria en cualquier momento. Inmediatamente después, el equipo de la empresa adjudicataria realizará un primer triaje del incidente y pondrá en marcha el proceso interno para activar el servicio, escalando la solicitud a un Gestor de Incidentes.
Req85	Incluye un **Gestor de Incidentes dedicado**, para coordinar la gestión de la crisis y apoyar la respuesta de principio a fin. Esto incluye la asistencia para la contención rápida, la recuperación segura de los datos y la asistencia en la comunicación externa e interna del incidente, a los CERTs, las LEAs y las partes interesadas.
Req86	Incluye **acceso completo a un equipo de expertos de la empresa adjudicataria** en análisis forense y de malware, hunters y equipo CTI & Forensics (Cyber Threat Intel and Forensics).
Req87	Incluye **asistencia en remoto**.(mínimo 8x5)
Req88	Puede incluir bajo demanda, **post-monitorización de incidentes** (por ejemplo, la monitorización continua de los puntos finales del INTA después del incidente, y la monitorización de sitios y foros de Internet para identificar fugas/exfiltraciones/signos de compromiso, etc.), como una característica añadida a petición del INTA, una vez que se haya finalizado la respuesta al incidente.
Req89	La respuesta debe estar respaldada con soluciones EDR líderes, DFIR (Digital Forensics Incident Response), CTI propia (ciberinteligencia) y pila de servicios MDR (Managed Detection and Recovery).
Req90	La empresa adjudicataria debe ser miembro de la red global de CERTs.
Req91	Incluye 10 jornadas DFIR al año. Las jornadas DFIR no consumidas antes de finalizar el contrato se podrán utilizar para jornadas del servicio de Compromise Assessment o DFIR Threat Intelligence Analysis (a petición del INTA).
Req92	El servicio de Respuesta de emergencia ante incidentes debe tener el siguiente ciclo de vida: - Triaje y análisis. - Despliegue y configuración de la tecnología EDR. - Coordinación durante el incidente con el equipo de Ciberseguridad del INTA y otros terceros involucrados. - Guía de contención, para minimizar el impacto del incidente. - Apoyo legal. - Apoyo en la comunicación de la brecha. - Asistencia para la erradicación. - Asistencia para la recuperación. - Emisión del Informe del incidente. - Post-monitorización.
Req93	El servicio de Análisis forense digital debe tener el siguiente ciclo de vida: - Triaje inicial. - Extracción de evidencias. - Análisis de los artefactos. - Obtención de indicadores de compromiso. - Contextualización de las amenazas. - Evaluación del alcance del compromiso. - Emisión del informe forense.
Req94	El equipo del servicio de respuesta ante incidentes y de análisis forense debe estar compuesto por las siguientes funciones/roles: - Gestor de Incidentes. - Expertos forenses. - Expertos en Malware/Reversing.

	- Analistas de Inteligencia de Amenazas.
Req95	El servicio de respuesta ante incidentes y de análisis forense debe proporcionar una plataforma de análisis de software completamente automatizada que garantice tanto la privacidad organizacional de los resultados como la posibilidad de conectarse con cualquier plataforma de gestión de amenazas de terceros.
Req96	Los requisitos de la plataforma de análisis de software son: • Se incluyen 2 Sandboxes para el análisis Dinámico. • Análisis estático Avanzado con posibilidad de decompilación de binarios y sistema Mul-tiantivirus. • Análisis estático de correos, URL´s y Pcap´s de tráfico. • 6.000 análisis de muestras al mes. • Informes de los análisis tanto Ejecutivo como Técnico en Español. El usuario debe poder editar el informe dentro de la plataforma para completarlo con sus comentarios. • La plataforma debe ser Multitenat para poder dar servicio a múltiples sedes con múltiples usuarios a los que se les podrá dar diferentes roles de visualización y derechos uso de la plataforma. • La plataforma debe estar abierta a la integración mediante API a terceros fabricantes tanto de Sandbox, Antivirus, SIEM, Feed de Inteligencia. • La inteligencia generada del análisis de muestras debe poder ser exportada automáticamente a plataformas de inteligencia como MISP (Malware Information Sharing Platform), STIX (Structured Threat Information eXpression y MAEC (Malware Attribute Enumeration and Chracterization) • La plataforma debe soportar TLP (Traffic Light Protocol), para compartir información con otras instituciones Públicas o Privadas o en la propia organización. • La plataforma debe incluir y correlacionar las muestras con el marco MITRE ATT&CK® lo que supone un excelente recurso para comprender sobre las tácticas y técnicas actuales de los ciberataques.
Req97	El servicio de respuesta ante incidentes y de análisis forense debe proporcionar una plataforma que centralice todos los eventos, alertas, amenazas y anomalías una vez que salen de los motores de Machine Learning, para predecir con precisión los ataques cibernéticos y las operaciones en una interfaz de un solo panel de control, interactiva y personalizada.
Req98	Los requisitos de la plataforma que centralice todos los eventos, alertas, amenazas y anomalías son: • La plataforma debe ser Multitenat para que permita dar servicio a múltiples sedes con múltiples usuarios a los que se les debe poder dar diferentes roles de visualización y derechos uso de la plataforma. • El usuario debe poder editar el informe dentro de la plataforma para completarlo con sus comentarios. • La plataforma debe estar abierta a la integración mediante API a terceros fabricantes. • Debe dar alertas en tiempo real de cualquier elemento de la infraestructura • Debe permitir la visualización de predicciones en tiempo real gracias a la evaluación constante de la I.A. de filtrado y valoración • El sistema de detección de anomalías debe permitir de un solo vistazo encontrar los puntos de la infraestructura que están presentando comportamientos sospechosos, incluso si no hay elementos de ciberseguridad desplegados, gracias a la I.A. de evaluación y análisis continuo.

	• Debe automatizar el proceso de aviso, alerta e incluso activación del Plan de Seguridad, facilitando la rapidez de respuesta y asegurando una concienciación completa y continua de los usuarios.

4.3.1.3.3.4 Servicio SIEM en la nube

Los requisitos del servicio de SIEM en la nube son:

Req99	Plataforma basada en Cloud.
Req100	Capa de monitorización de seguridad 24x7.
Req101	Capa de recolección de datos. (Mínimo 7000 EPS)
Req102	Capa de retención de datos a largo plazo. La empresa adjudicataria deberá archivar los logs y Eventos del SIEM durante el tiempo determinado por INTA para el cumplimiento normativo: En caliente (Accesibles de forma inmediata) Al menos 6-12 meses de histórico Eventos, sobre el que poder consultar “on-line”. Al menos 7 días de Logs En Frio: Al menos 2 año de almacenamiento en frío para logs y eventos.
Req103	Capa de orquestación y automatización.
Req104	Capa de inteligencia de amenazas.
Req105	Modelo global de operación de monitorización de alertas e incidentes, basados en reconocidos estándares y procesos de seguridad.
Req106	Notificaciones inmediatas de incidencias, a través del Portal de Clientes, correo electrónico y/o la herramienta de ticketing de INTA.
Req107	Métricas y KPIs avanzados.
Req108	Plataforma SIEM certificada en el ENS Nivel Alto y aprobado como producto STIC por el CCN-CERT o con la solicitud de certificación realizada de forma previa a la publicación de esta licitación.
Req109	Peticiones del INTA para revisión de alertas.
Req110	Revisión, fine-tuning y mejora continua.
Req111	Conectividad de la empresa adjudicataria al INTA a través de VPN IPSec.
Req112	El servicio incluye toda la migración de reglas del SIEM on premise actual del INTA al SIEM de la nube (véase los Casos de Uso del SIEM actual en la Tabla 3 del ***Anexo A. Ciberseguridad***). Así como el mantenimiento, administración y conectividad al centro de alarmas del SIEM on-premise actual hasta la integración de la funcionalidad en la actual solución SaaS (véase Tabla 1 de Servicios en el ***Anexo A.***).
Req113	El servicio de SIEM en la nube debe incluir como mínimo las fuentes integradas en el SIEM on premise actual del INTA (véase el Listado de las fuentes integradas en el SIEM actual en la Tabla 2 del ***Anexo A.***). La puesta en marcha del servicio de SIEM en la nube será 6 meses desde la fecha de la firma del contrato.
Req114	El servicio de SIEM en la nube incluye su evolución, administración y mantenimiento.

4.3.1.3.3.5 Servicio SIEM on premise

Los requisitos del servicio de SIEM on premise son:

Req115	Plataforma instalada on premise.No es objeto de mantenimiento de este expediente pero si su administración hasta su sustitución por el SIEM SaaS
Req116	Capa de monitorización de seguridad 24x7.
Req117	Capa de recolección de datos.

Req118	Capa de retención de datos a largo plazo. La empresa adjudicataria deberá archivar los logs del SIEM durante el tiempo determinado por INTA para el cumplimiento normativo: • Al menos 6 meses de histórico “en caliente”, sobre el que poder consultar en “on-line”. • Al menos 2 años de almacenamiento en frío.
Req119	Capa de orquestación y automatización.
Req120	Capa de inteligencia de amenazas.
Req121	Modelo global de operación de monitorización de alertas e incidentes, basados en reconocidos estándares y procesos de seguridad.
Req122	Notificaciones inmediatas de incidencias, a través del Portal de Clientes, correo electrónico y/o la herramienta de ticketing de INTA.
Req123	Métricas y KPIs avanzados.
Req124	Peticiones del INTA para revisión de alertas.
Req125	Revisión, fine-tuning y mejora continua.
Req126	Conectividad de la empresa adjudicataria al INTA a través de VPN IPSec.
Req127	El servicio incluye el mantenimiento, administración, evolución y conectividad al centro de alarmas del SIEM on-premise actual hasta la integración de la funcionalidad en la solución SaaS (véase Tabla 1 de Servicios en el ***Anexo A.***).
Req128	El servicio de SIEM on premise debe incluir: - Mantenimiento de las fuentes integradas en el SIEM on premise actual del INTA (véase el Listado de las fuentes integradas en el SIEM actual en la Tabla 2 del ***Anexo A.***). - Integración de nuevas fuentes. - Creación de nuevas reglas de correlación. - Mantenimiento y evolución de informes. - Mantenimiento y evolución de los cuadros de mando. - Analizar los incidentes de seguridad y emitir los informes y recomendaciones de actuación. - Elaborar los procedimientos de trabajo y las propuestas para la mejora del servicio. - Identificar propuestas de mejora de los indicadores de seguridad, alertas de monitorización y reportes para el análisis del estado de seguridad. - Identificación proactiva de las mejoras a realizar en los sistemas para evitar la replicación en el futuro de incidentes similares.

4.3.1.3.4 Soporte a la Gestión de Identidades

Los requisitos del servicio de Soporte a Gestión de Identidades son:

Req129	El servicio de administración de la solución de Gestión de Identidades SailPoint (IdentityIQ/SecurityIQ) y del resto de la plataforma de CiberSeguridad (Listado de dispositivos de Ciberserguridad en todas las Tablas del ***Anexo A. Ciberseguridad***) requerirá mínimo 360 horas anuales para labores relacionadas con la gestión de la herramienta y elementos de ciberseguridad como: • Mantenimiento de la integración en la solución de las fuentes de identidades. • Integración de las diferentes soluciones adquiridas y proporcionadas por la herramienta. • Creación de nuevas reglas, workflows, parametrizaciones, instalaciones, optimizaciones de los elementos. • Mantenimiento y evolución de informes y cuadros de mando asociados a la herramienta y su relación para el cumplimiento con la RGPD.

	• Cualesquiera otras tareas relacionadas con los productos y su integración en el organismo.
Req130	De las 360 horas anuales, el INTA podrá decidir consumir las que estime oportuno en jornadas de formación sobre las soluciones de Gestión de Identidades, o si el INTA lo necesitara, sobre cualquier otra tecnología de Ciberseguridad administrada por la empresa adjudicataria.
Req131	Se deberá hacer cargo del coste de mantenimiento asociado a las licencias de la solución SailPoint adquiridas por el organismo que se describen en la Tabla 1 de Servicios del ***Anexo A.*** .
Req132	La empresa adjudicataria deberá hacer uso de la herramienta de Gestión del Soporte TI - INTA (BMC Remedy), para realizar el registro, la gestión y el reporting de todas las incidencias de seguridad. El adjudicatario no podrá hacer uso de otras soluciones de ticketing para la cuenta INTA.
Req133	El licitador opcionalmente podrá reflejar expresamente en su propuesta que otras herramientas, adicionales a las indicadas por el INTA, requerirá utilizar para prestar el servicio.

CSV:202079MZDXuE4hYXwtH7eilbgyFKV8BOQ=

5 RECURSOS MATERIALES

Los recursos materiales, entre otros portátiles, teléfonos móviles, vehículos, material de oficina y demás herramientas, que utilizará el equipo de trabajo para dar el servicio requerido deberán ser proporcionados por la Empresa Adjudicataria.

Cualquier otro equipo que suministre el adjudicatario al personal desplegado in-situ, y que tendrá conectividad con le red interna INTA, debe estar certificado con las políticas y estándares de seguridad del INTA.

Asimismo, para la correcta ejecución del servicio, los adjudicatarios tendrán acceso a las aplicaciones informáticas del INTA necesarias para el desarrollo de su trabajo, así como a las instalaciones especializadas del centro de trabajo.

El puesto de trabajo informático (Equipo y Software) del personal del adjudicatario que preste sus servicios en el Instituto deberá ser proporcionado por su empresa, pero bajo supervisión del Departamento de Tecnologías de la Información y las Comunicaciones.

Una vez realizado por parte del Dpto. TIC el análisis de necesidades de uso de sistemas de información del organismo para el trabajo a desarrollar, el Dpto. TIC tomará la decisión por la opción necesaria entre las siguientes:

• Opción 1:

Alta dependencia de SI del organismo. La empresa externa deberá de proporcionar equipo (CPU, teclado, lector de tarjetas inteligentes, ratón y monitor) y las licencias de SSOO (Última versión del Sistema Operativo Windows 10 en su versión PRO) y software de ofimática (última versión del paquete ofimático Microsoft Office / 365, siempre y cuando sean necesarios para el ejercicio de su actividad las funciones de este producto, si no son necesarias la alternativa LibreOffice, y si es necesario, cualquier otro software ofimático como Visio, Project, MindJet, etc. también deberá de ser proporcionado) y el equipo será instalado y plataformado por el INTA. El INTA proporcionará las licencias de software específico o de cálculo científico o de gestión SAP si procede. Es necesario que el sistema Operativo y el paquete ofimático sean Microsoft debido a que forman parte de la arquitectura de referencia TIC del organismo apoyada en la arquitectura de referencia TIC del Ministerio de Defensa, y por lo tanto son los seleccionados para los equipos ofimáticos de uso general.

• Opción 2:

Baja dependencia de SI del organismo. El equipo podrá ser plataformado y administrado de forma externa al organismo. Se proporcionará conectividad vía VPN para estos equipos y un acceso limitado a los servicios necesarios para desarrollar el trabajo en el INTA. Se exigirán unos requisitos mínimos de software actualizado para poder autorizar esa conexión. (Mínimo Windows 10 actualizado, Antivirus actualizado, y otros requisitos que Seguridad de la Información considere necesarios). No se permitirá equipos con otros sistemas operativos no Windows a esta VPN. Es necesario que el sistema Operativo y el paquete ofimático sean Microsoft debido a que forman parte de la arquitectura de referencia TIC del organismo apoyado en la arquitectura de referencia TIC del Ministerio de Defensa, y por lo tanto son los seleccionados para los equipos ofimáticos de uso general.

6 REQUISITOS DE SEGURIDAD INDUSTRIAL

La empresa adjudicataria deberá cumplir en todo momento las políticas de seguridad industrial y de informática del Instituto.

7 REQUISITOS DE PREVENCIÓN DE RIESGOS LABORALES

El adjudicatario contactará con el Servicio de Prevención de Riesgos Laborales, (e-mail: cae-torrejon@inta.es) previo al inicio de las actividades, con el fin de establecer la coordinación de actividades empresariales entre ambas partes para dar cumplimiento al REAL DECRETO 171/2004, de 30 de enero, por el que se desarrolla el artículo 24 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

CSV:202079MZDXuE4hYXwtH7eilbgyFKV8BOQ=

8 PLANIFICACIÓN

Los planes deberán estar avalados y fundamentados en metodologías probadas (ITIL V4, DevOps, COBIT, PMI, CMMi, entre otras), estas metodologías deberán complementarse con las mejores prácticas del sector y en la prestación de servicios similares a los descritos en el presente pliego.

La oferta deberá desarrollar entre otros, los siguientes planes dentro de su oferta:

Servicios de Administración Avanzada de Sistemas:

- **Plan del Modelo de Servicio**. La Empresa Licitadora definirá un Modelo de Servicio que garantice la prestación óptima de los servicios solicitados en el presente pliego, para lo que se designará un recurso con experiencia en Gestión de Proyectos para garantizar la coordinación en la prestación del Servicio.
- **Plan de Transición/Reversión del Servicio**. La Empresa Licitadora definirá un Plan de Transición del Servicio objeto de este contrato que garantice la realización efectiva de la gestión del cambio, con una duración mínima de 30 días para ello y mitigando cualquier riesgo o impacto sobre la calidad de las actividades y recursos. Este plan debe contener todas aquellas actividades y recursos necesarios para garantizar las labores del plan incluyendo el traspaso de funciones, servicios, activos, etc. de la empresa adjudicataria de este contrato a la finalización del mismo (Transición/Reversión)

- **Plan de Prestación y Gestión del Servicio**. La Empresa Licitadora definirá un Plan de Prestación y Gestión del Servicio que contenga todas aquellas actividades y recursos necesarias para garantizar la realización de la prestación de los servicios solicitados en el presente pliego, minimizando el tiempo y cualquier riesgo o impacto sobre la calidad de los mismos. Haciendo especial hincapié en la documentación y la gestión de la Base de Conocimientos.

Tal y como se muestra en el siguiente diagrama.

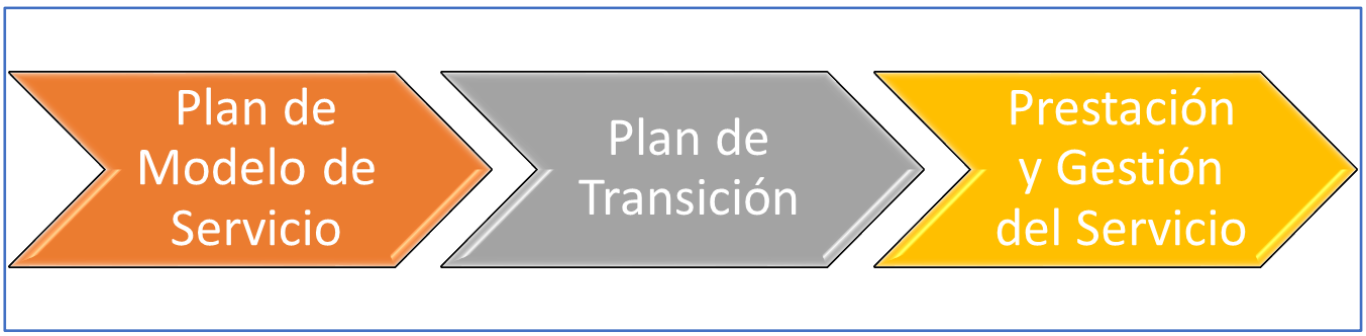


Diagrama 5. Diagrama del Plan de Proyecto

9 SEGUIMIENTO Y VERIFICACIÓN POR PARTE DEL PROVEEDOR

La Empresa Adjudicataria deberá elaborar un plan de seguimiento con las actividades de verificación que irá realizando durante la vigencia del contrato, con independencia de las actividades de seguimiento que el INTA considere oportunas realizar, para las cuales el proveedor deberá facilitar la información y datos que INTA le requiera.

Dicho plan deberá contener al menos:

- Calendario de actividades de seguimiento.
- Verificaciones a realizar.
- Muestras a tomar.
- Responsables de las verificaciones.

En todo momento la Empresa Adjudicataria actuará de buena fe, con diligente iniciativa y tratará de conseguir en la mayor brevedad la resolución de la pérdida de servicio detectada.

La Empresa Adjudicataria realizará sus servicios de una forma profesional y oportuna, encargando siempre su ejecución al personal cualificado más apropiado para cada servicio.

La Empresa Adjudicataria se adaptará en todo momento a las normas del INTA, muy especialmente a las normas de seguridad.

10 ACEPTACIÓN DEL SERVICIO POR EL INTA

El servicio deberá cumplir los requisitos contenidos en el presente pliego.

Para comprobar la idoneidad y aceptación final de los trabajos realizados, el INTA se reserva el derecho de realizar las comprobaciones pertinentes para la aceptación del servicio.

CSV:202079MZDXuE4hYXwtH7eilbgyFKV8BOQ=

11 DOCUMENTACIÓN A ENTREGAR

11.1 Documentación a entregar con la oferta

Para cada oferta se seguirá el siguiente índice, incluyendo en cada apartado los contenidos señalados. Se podrán subdividir en los sub-apartados que la Empresa Licitadora estime conveniente, para aclarar cada uno de los puntos.

1. **Índice.**

2. **Relación de Hojas Entregadas**.

3. **Características Generales.**

3.1. Introducción.

- Se describirá brevemente la estructura del documento.

3.2. Abreviaturas y Definiciones.

- Se indicará el significado de las abreviaturas que se utilicen a lo largo del documento y las definiciones de los términos especificados.

3.3. Descripción de la Empresa.

3.3.1. Datos generales de la empresa.

3.3.2. Identificación, referencias y justificación de los Centros de Asistencia que cumplan los requisitos expuestos en el apartado ***4.2.1 Lugar de la prestación del servicio.***
Se deberá incluir la localización del COS principal que prestará el servicio del pliego. (Las localizaciones de COS adicionales al ser un criterio valorable por formulas NO se describirá aquí ya que deberá de ir en el sobre correspondiente).

3.4. Condiciones Ofertadas.

- La oferta debe reflejar como se resolverán los **requisitos** solicitados para cada uno de los ***Servicios de Administración Avanzada de Gestión de Identidades y de Ciberseguridad***, y sus correspondientes sub-elementos, especificando:
  - Para cada uno de ellos los elementos que describen los mecanismos utilizados para brindar la solución en forma de servicios.
  - **Planificación.** Se deberá describir la planificación según lo expuesto en el apartado ***PLANIFICACIÓN.*** En cada uno de estos planes debe indicarse la metodología seleccionada y los elementos principales de la misma, haciendo énfasis en los entregables y mecanismos de control que se establecerán.
  - Deberán de rellenarse los proyectos de relevantes al Pliego en los que la empresa haya participado que tengan relevancia con el objeto de la licitación.

- Se deberá de rellenar de manera adicional, además de los importes, los datos solicitados en la Plantilla A del PPT para cada referencia

11.2 Documentación a entregar durante la prestación del servicio

Durante la prestación de ***Servicios de Administración Avanzada de Gestión de Identidades y de Ciberseguridad***se deberá entregar al menos la siguiente documentación con la frecuencia indicada:

- Seguimiento de Planes de Prestación (Aspectos Destacables) **Frecuencia: Mensual**
- Métricas Volumetría del Servicio **Frecuencia: Mensual/Anual**
- Acciones y Gestión de Riesgo **Frecuencia: Semanal**

EL TÉCNICO DEL EXPEDIENTE

JOSE GAREA LOUREIRO

ANEXOS DEL PLIEGO

Anexo A. Ciberseguridad

El presente pliego dispone de un anexo técnico (Anexo A. Ciberseguridad) con el detalle de la infraestructura técnica de ciberseguridad implantada en el INTA, y que podrá ser consultado bajo demanda durante el proceso de licitación, suscribiendo previamente el correspondiente clausulado de confidencialidad.

Para ello los interesados deberán cursar vía correo electrónico a través de la dirección ciberseguridad_DTIC@inta.es la correspondiente solicitud al INTA de acceso al presente anexo. Dicha solicitud, debidamente cumplimentada con los datos personales y de contacto del interesado, deberá estar suscrita por la entidad o persona que le represente, en su caso, debiendo de aportar la documentación acreditativa de la personalidad y representación, así como la correspondiente autorización en caso de actuar por medio de autorización expresa para tal acto.

En respuesta a esta solicitud, desde el INTA se pondrán en contacto con el interesado a la mayor brevedad posible para proceder a la firma del clausulado de confidencialidad y la entrega del anexo indicado.

CSV:202079MZDXuE4hYXwtH7eilbgyFKV8BOQ=

Anexo B. Listado de Acrónimos

AGE:	Administración General del Estado
ANS:	Acuerdo de Nivel de Servicio
AREN:	El Arenosillo
AV:	Tecnología de Seguridad
BAPI:	Business Application Programming Interface
BBDD:	Bases de Datos
BLE:	Bluetooth Low Energy
BO:	Best Effort. Lo antes posible.
CADI:	Cádiz
CEAR:	Centro de Evaluación y Análisis Radioeléctrico
CEBR	Cebreros
CEC:	Centro Espacial de Canarias
CEDEA:	Centro de Experimentación de “El Arenosillo”
CEHIPAR:	Canal de Experiencias Hidrodinámicas de El Pardo
CET:	Centro de Ensayos de Torregorda
CI:	Elementos de Configuración
CIAR	Centro de Investigación Aeroportada de Rozas
CMDB:	Base de Datos de Configuración
CMMI:	Capability Maturity Model Integration
CO:	Centro de Operaciones
COS:	Centro de Operaciones de Seguridad
CPD:	Centro de Proceso de Datos
CPU:	Central Processing Unit
CUAD:	Cuadros
DES:	Data Encryption Standard
DevOps:	Combinación de prácticas y herramientas para apoyar y acelerar la prestación de servicios en Desarrollo y Operaciones TIC.
DLNA:	Digital Living Network Alliance
DLP:	Data Loss Prevention
DNS:	Domain Name System
DPI:	Dots Per Inch
DTIC:	Departamento de Tecnologías de la Información y las Comunicaciones
EHP7	Enhancement Package
ERP:	Enterprise Resource Planning
ETL:	Extract-, Transform and Load
FTE:	Full Time Employee
GR:	Granada
GSC:	Galileo Service Center
GUAD:	Guadalajara
HANA	Hasso´s New Architecture
HAT:	Horario Atención Total
HIB:	Horario In-situ Básico

HIE:	Horario In-situ Extendido
HP	Hewlett Packard
HPE:	Hewlett Packard Enterprise
HPS	Habilitación Personal de Seguridad
HR:	Human Resources
HSEM:	Habilitación de Seguridad de Empresa
HTLM:	HyperText Markup Language
HW:	Hardware
IEC:	International Electrotechnical Commission
INTA:	Instituto Nacional de Técnica Aeroespacial
IPS/IDS:	Intrusion Prevention System/Intrusion Detection System
ISO:	International Organization for Standardization
ITIL:	Information Technology Infraestructure Library
ITSM:	Information Technology Service Management
KPI:	Key Performance Indicators
LABINGE:	Laboratorio de Ingenieros del Ejército
LAN:	Local Area Network
LC:	Conector pequeño de Fibra óptica
LUGO:	Lugo
MADR:	Madrid
MASP:	Maspalomas
MM:	Materials Management
MO:	Moguer
MS:	Microsoft
NGFW:	**Next-Generation Firewall**
NGL:	New General Ledger
OOB:	Tecnologia de Remedy
PARD	El Pardo
PBT:	Tereftalato de Polibutileno
PC	Personal Computer
PC's:	Personal Computer.
PCAP:	Pliego de Claúsulas Administrativas Particulares
PKI:	Public Key Infraestructure
PoC:	Piloto/Prueba de Concepto
PRE:	PREPRODUCCION
PRO:	PRODUCCION
PS:	Project System
RGPD	Reglamento General de Protección de Datos
RMS:	Record Management System
RO	Robledo de Chavela
SANM	San Martín de la Vega
SAP:	Sistemas, Aplicaciones y Productos en procesamiento de datos
SAT:	Servicio de Administración Tributaria

SC2:	Centro de Competencia de Seguridad
SD:	Sales and Distribution
SDN:	Software Defined Networking
SEVI:	Sevilla
SIC3:	Sistema de Información Contable
SIEM:	Gestión de eventos e Información de Seguridad
SII:	Sistema de Informacion Inmediato del IVA
SLA:	Service Level Agreement o Acuerdos de Nivel de Servicio
SP:	Service Pack
SPP:	Service Pack para ProLiant
SSID:	Service Set Identifier
SSOO:	Sistemas Operativos
SW:	Software
TI:	Tecnologías de la Información
TIC:	Tecnologías de la Información y Comunicaciones
TORR:	Torrejón de Ardoz
UCMDB:	Universal Configuration Management DataBase
UE:	Unión Europea
UNE-EN:	Una Norma Española-Normas Europeas
USB:	Universal Serial Bus
UX:	Experiencia del Usuario
VALE:	Valencia
VILL:	Villafranca del Castillo
VLAN:	Virtual Local Area Network
VoIP:	Voz IP
WAF:	Web Application Firewall
WiFi:	Wireless Fidelity
ZTP:	Zero Touch Provisioning

CSV:202079MZDXuE4hYXwtH7eilbgyFKV8BOQ=

Anexo C. Cláusulas de seguridad

Los requisitos de seguridad incluidos en el presente Anexo solo serán aplicables a aquellos programas/proyectos/actividades incluidos en el presente contrato en los que los consultores asignados a los mismos deban tener acceso real o potencial a información clasificada. La guía de clasificación que se adjuntará a la Comunicación de Contrato Clasificados incluirá la relación de los programas/proyectos/actividades que estén clasificados indicando su ámbito y nivel de clasificación.

A este fin, el Adjudicatario deberá atenerse al marco normativo establecido en las Normas de la Autoridad Nacional para la Protección de la Información Clasificada (ANS) o a la Política de Seguridad de la Información del Ministerio de Defensa. Dichas normas están publicadas en la página web del Centro Nacional de Inteligencia (CNI), Oficina Nacional de Seguridad (ONS), en el primer caso, mientras que la normativa referente al Ministerio de Defensa han sido publicadas en el B.O.D.

De acuerdo con el presente contrato, el contratista declara conocer y aceptar los siguientes compromisos en materia de Seguridad de la Información Clasificada, en el marco de las Normas de la Autoridad Nacional (ANS o ANS-D) y del Ministerio de Defensa para la Protección de la Información Clasificada:

1. **Habilitación de Seguridad de Empresa (HSEM):**

   El Contratista debe estar en posesión de la Habilitación de Seguridad de Empresa (HSEM) de grado RESERVADO o equivalente, o superior, en vigor, concedida por la Autoridad Nacional de Seguridad para, al menos, los ámbitos de aplicación para el presente contrato.

   Para la acreditación de este apartado, el contratista presentará al Servicio General de Protección de Materias Clasificadas / Subregistro Principal del INTA certificación oficial emitida por la ANS-D u Órgano de Control del que dependa de que dispone de dichas acreditaciones y éstas están en vigor.

2. **Sistemas de Información y Comunicaciones (CIS):**

   En el supuesto de que el contratista necesitase manejar en sus instalaciones Información Clasificada en sistemas de información y comunicaciones (CIS), éstos deberán estar acreditados por la ANS-D, como mínimo, con el grado de clasificación de la información clasificada manejada en ellos. Del mismo modo, deberá disponer de acreditación HSES con

el nivel RESERVADO o equivalente para, al menos, los ámbitos de aplicación para el presente contrato.

3. Habilitación Personal de Seguridad (HPS):

Toda persona de la empresa contratista que participe en la ejecución de este contrato y que tenga acceso a Información Clasificada debe estar en posesión de Habilitación Personal de Seguridad (HPS) en vigor, de igual o superior grado y tipo que el asignado a la Información Clasificada a la que pudiera acceder.

La empresa Contratista facilitará al Jefe de Seguridad del Servicio de Protección de Materias Clasificadas / Subregistro Principal del INTA, certificación emitida por la ANS-D o por el Órgano de Control del que dependa, de que todas las personas que vayan a participar en el contrato y que tengan acceso a Información Clasificada dispongan de Habilitación Personal de Seguridad vigente y con el grado adecuado, (hasta RESERVADO o equivalente, O SUPERIOR), y de los ámbitos correspondientes, (Nacional, OTAN, UE y/o ESA).

4. Vigencia de las Habilitaciones de Seguridad:

La empresa Contratista se compromete al mantenimiento de la vigencia de la Habilitación de Seguridad de Empresa/ Habilitación de Seguridad de Establecimiento (en caso necesario), así como de las Habilitaciones Personales de Seguridad del personal que participen en el mismo durante la ejecución del presente Contrato.

Si la Habilitación de Seguridad de Empresa fuera cancelada o suspendida por la Autoridad Nacional de Seguridad por alguno de los motivos expresados en el ap. 6.8.1 o 6.8.2 de la Norma NS/06 de la ANS-D, dicho acto conllevará la resolución del Contrato.

5. Posibilidad de elevación de grado:

Si durante la ejecución del Contrato surgiera la necesidad de proporcionar al personal de la empresa Contratista Información Clasificada de grado superior al de las Habilitaciones de Seguridad concedidas, de la empresa Contratista se compromete a solicitar la elevación de grado, de acuerdo con el procedimiento establecido en los apartados 6.4.1 y 6.4.2 de la Norma NS/06 de la ANS-D o normativa equivalente y aplicable del Ministerio de Defensa y a aportar los medios necesarios para la concesión de dicha elevación.

6. Acceso y tratamiento de la Información Clasificada:

La empresa Contratista se compromete a solicitar al INTA, como Órgano de Contratación, la autorización de acceso a Información Clasificada de acuerdo con lo establecido en el apartado 6.3.2. de la Norma NS-06 de la ANS-D o normativa equivalente y aplicable del Ministerio de Defensa. La solicitud del contratista para el acceso a información clasificada de su personal se realizará cumplimentado el formulario “Autorización de acceso” que deberá ser entregado al SGPMC del INTA tanto al inicio como cada vez que se produzca una modificación de los datos requeridos en dicho formulario. Este formulario está disponible en la página Web de la ONS y en la normativa equivalente y aplicable del Ministerio de Defensa
El tratamiento de la Información Clasificada que pudiera serle facilitada a la empresa Contratista en el marco de este Contrato se regirá por las normas establecidas por la ANS-D o por normativa equivalente y aplicable del Ministerio de Defensa. La Información Clasificada deberá transmitirse de acuerdo con lo recogido en los apartados “6. Transmisión de la información Clasificada” y “7. Recibos” recogidos en la Norma de Seguridad de la Información (NS/04) de la ANS-D. Los formatos (recibos) utilizados para la transmisión de las materias clasificadas serán los indicados en dichos apartados y, en todo caso, están disponibles en la página Web de la ONS.

7. Sobre la firma del presente Contrato:

En el acto de firma del presente Contrato, el Jefe de Seguridad del Servicio de Protección de Materias Clasificadas de la empresa Contratista deberá suscribir el formulario “Comunicación de Contrato Clasificado”, según modelo de la ONS disponible en su página web, por el que el INTA, como Órgano de Contratación, le comunica el grado de clasificación global del Contrato, a fin de que pueda aplicar las medidas de protección correspondientes.

8. Devolución de Información Clasificada

Una vez finalice el Contrato, la empresa Contratita deberá devolver al INTA toda la Información Clasificada que le haya sido suministrada o en su caso elaborada por ellos, de acuerdo con las Normas de la ANS-D o normativa equivalente y aplicable del Ministerio de Defensa

La Información Clasificada que se maneje o genere en el cumplimiento de este Contrato será empleada única y exclusivamente para el propósito para el que fue generada o proporcionada y no será cedida a terceros sin el consentimiento previo y por escrito del propietario de la misma.

Las obligaciones de la empresa contratista relativas a la protección de la Información Clasificada continuarán estando vigentes incluso después de la finalización del Contrato.

9. Subcontratación

En el caso que en el marco del presente contrato la empresa contratista realizara alguna subcontratación, la empresa contratista deberá solicitar autorización expresa al INTA y trasladar al Subcontratista las cláusulas de seguridad de la información clasificada contenidas en este anexo. El Subcontratista deberá disponer, a su vez, de HSEM en grado Reservado o equivalente.

10. Comunicación de Incidencias

La empresa Contratista se obliga a poner en conocimiento del INTA a la mayor brevedad posible, en el marco de la ejecución del presente contrato, los posibles comprometimientos de la Información Clasificada, sin perjuicio del cumplimento de lo establecido a este respecto en el apartado 11 de la Norma NS-04 de la ANS-D utilizando para ello el Anexo V “Informe de comprometimiento” incluido en dicha norma o normativa equivalente y aplicable del Ministerio de Defensa.

PLANTILLAS

Plantilla A: Referencia de Proyectos.

Se adjunta en documento a aparte.