PLIEGO DE CONDICIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SERVICIO DE AUDITORÍA DE CERTIFICACIÓN EN ENS NIVEL MEDIO DE SERVICIOS DE LA DIPUTACIÓN DE CASTELLÓN.

1. OBJETO DEL CONTRATO

El servicio objeto del contrato es la realización de una Auditoría de Certificación de los sistemas de información de la Diputación de Castellón, conforme a lo dispuesto en el RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) y normativa de desarrollo, para dar cobertura a los requisitos normativos referentes a la auditoría de seguridad recogidos en el art. 31 y Anexo III del ENS.

2. SITUACIÓN ACTUAL

La Diputación de Castellón se encuentra en un proceso para el cumplimiento del ENS 311/2022 en los sistemas tecnológicos y de información.
Para cumplir con esto, es necesario llevar a cabo una auditoría de certificación de conformidad con el Esquema Nacional de Seguridad (ENS) de categoría MEDIA en la Diputación de Castellón. Esta solicitud se fundamenta en el compromiso de la entidad para adaptarse y cumplir con los estándares y normativas establecidos por el ENS.

A continuación indicamos unas razones clave para la Auditoría:

1. Proceso de Adaptación al ENS:
   La organización se encuentra actualmente inmersa en un proceso integral de adaptación al Esquema Nacional de Seguridad (ENS) de categoría MEDIA.
   Este proceso abarca la implementación de medidas y controles específicos para cumplir con los requisitos de seguridad establecidos por el ENS.

2. Necesidad de Evaluación Externa:
   La realización de una auditoría de certificación externa proporcionará una evaluación objetiva e imparcial del grado de conformidad de la organización con los requisitos del ENS de categoría MEDIA.
   La validación por parte de una entidad certificadora independiente refuerza la credibilidad de los esfuerzos de la organización en materia de seguridad de la información.

3. Cumplimiento Normativo:
   Cumplir con el Esquema Nacional de Seguridad (ENS) es esencial para garantizar la seguridad de la información y proteger los activos críticos de la organización.
   La obtención de la certificación de conformidad demuestra el compromiso de la organización con las mejores prácticas en seguridad de la información y refuerza la confianza de los grupos interesados.

4. Requisitos de Terceros:
   La certificación con el ENS puede ser un requisito contractual o de proveedores, lo que fortalece las relaciones comerciales y garantiza el cumplimiento de las expectativas de seguridad de los socios y clientes.

Impacto Positivo:

La auditoría de certificación proporcionará un marco estructurado para evaluar y mejorar continuamente los controles de seguridad de la Diputación de Castellón.
Facilitará la identificación de áreas de mejora y permitirá implementar medidas correctivas efectivas para fortalecer la postura de seguridad.

3. ALCANCE Y REQUISITOS

El alcance se extiende al sistema de información que soporta los servicios de Administración electrónica, Gobierno abierto e innovación, Secretaría General, RRHH, Prevención de riesgos laborales, Infraestructuras, Servicios jurídicos, Área técnica, Formación, Conserjes u ordenanzas, Carreteras, Gestión Tributaria y Recaudación, Tesorería, Grafico y Digital, Patrimonio y Expropiaciones, Contratación y Central de compras, Complejo Socio Educativo Penyeta Roja, Cultura, Deporte, Juventud y Restauración, Promoción económica y relaciones internacionales, Parque y taller, Archivo, gestión documental y publicaciones, Cooperación Municipal: Gestión de planificación y medio ambiente y medio rural, Intervención, Servicios sociales e Informática de las soluciones tecnológicas de la Diputación de Castellón.

Ubicaciones:
Oficinas Centrales: Diputación Provincial de Castellón-Nuevas Dependencias - Avda. Vall d'Uixó, 25 - 12004 Castellón

CPD Principal: Universidad Jaime I, Avenida de Vicente Sos Baynat, s/n, 12006 Castellón de la Plana, Castellón

CPD Respaldo: Diputación Provincial de Castellón-Nuevas Dependencias - Avda. Vall d'Uixó, 25 - 12004 Castellón

Descripción de los trabajos:

- Auditoría de Certificación del ENS (auditoría documental insitu o remota) y expedición, en su caso, de la correspondiente Certificación de Conformidad con el ENS), para el alcance señalado.
- La empresa licitadora deberá asegurarse que la renovación del certificado se publique en las webs del Centro Criptológico Nacional (CCN).
- Requisitos de cualificación y experiencia del Equipo Auditor adscrito al contrato: Será necesaria la presencia, al menos, de un Auditor Jefe, que deberá satisfacer los requisitos personales expresados en la Guía CCN-STIC CCN-CERT IC-01/19, complementados con los expresados en la Guía CCN-STIC 802).
- Metodología y entregables: la empresa licitadora deberá proponer de manera clara la metodología a seguir durante el desarrollo del proyecto, que deberá estar orientada a alcanzar los objetivos fijados en el Pliego. Asimismo, el licitador describirá en detalle el contenido y estructura de los entregables objeto del proceso de auditoría, entre ellos, el plan de auditoría, el informe de auditoría documental, el informe de auditoría presencial y, en el caso de hallarse desviaciones, el informe de evaluación del Plan de Acciones Correctivas (PAC), todo ello según se detalla en la ITS de Auditoría, en la Guía CCNCERT IC-01/19 y en la Guía CCN-STIC 802).
- Equipo Auditor Perfiles técnicos requeridos:
  - Se requerirá, al menos, un Auditor Jefe.
  - Dirección y seguimiento de los trabajos: determinación de la unidad encargada de la dirección y seguimiento del proyecto.

La empresa licitadora deberá proponer en su oferta las fechas previstas para la realización de la auditoría, que deberán estar incluidas en el segundo trimestre de 2024.

4. CUMPLIMIENTO DE ESTÁNDARES Y NORMATIVA

La solución técnica propuesta en su oferta por el licitador, así como el conjunto de los trabajos pertinentes para ofrecer los servicios demandados, deberán cumplir con la siguiente normativa:

 Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público.

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

 Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.

 Resolución de 19 de febrero de 2013, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Reutilización de recursos de la información (NTI-RISP).

 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.

 Ley 18/2015, de 9 de julio, por la que se modifica la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.

 Reglamento General de Protección de Datos (RGDP) relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

 Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

De producirse cualquier modificación de la legislación vigente señalada durante la ejecución del contrato, el adjudicatario deberá garantizar la adecuación del sistema, los procesos y los trabajos contenidos en este pliego a la normativa resultante.

5. INCUMPLIMIENTO DE ESTE PLIEGO DE CONDICIONES TÉCNICAS

Será causa de rechazo de la proposición presentada la no inclusión en la oferta de todos los elementos, licencias, productos y/o suministros solicitados, o de aquellos que fuesen necesarios para el correcto funcionamiento del conjunto de los elementos de la oferta presentada.

Los licitadores deben presentar un cuadro de cumplimiento de todas las características técnicas solicitadas.

6. CONFIDENCIALIDAD DE LA INFORMACIÓN

La información, datos o especificaciones facilitadas por la Diputación Provincial de Castellón al adjudicatario o al personal de su servicio, así como a los que hayan accedido en ejecución del contrato, deberán ser consideradas por éstos como confidenciales, no pudiendo ser objeto, total o parcial, de publicaciones, copia, utilización, cesión o préstamo a terceros.

El adjudicatario y el personal a su servicio adquieren la obligación fiel de custodiar cuidadosamente la información, documentación o datos de los que se le haga entrega para la realización de los trabajos objeto del servicio, y con ello el compromiso de que los mismos no lleguen bajo ningún concepto a poder de distintas personas.

El adjudicatario y el personal a su servicio no podrán acceder a aquellas informaciones, datos y documentos no directamente relacionados con el objeto del contrato.

En todo caso, el adjudicatario será responsable de los daños y perjuicios que el incumplimiento de las obligaciones enumeradas en esta cláusula pudieran derivarse para la Diputación o para terceras personas.

Castellón firmado digitalmente

Fdo: Antonio Sáez Sanz
JEFE DEL SERVICIO DE INFORMÁTICA

ANEXO DE LAS OBLIGACIONES RELATIVAS AL CUMPLIMIENTO DEL ESQUEMA NACIONAL DE SEGURIDAD, POR PARTE DE LOS TERCEROS ADJUDICATARIOS O CONTRATISTAS.

Para poder dar cumplimiento al ENS, se deberá de cumplir con una serie de requisitos básicos de seguridad que la organización ha establecido alineadas con el Real Decreto, en caso de ser aplicable a este contrato.
Estos requisitos mínimos serán imprescindibles para cualquier solución tecnológica que se preste. En caso de no disponer de ellos, deberá de justificarse adecuadamente el motivo, quedando la posibilidad de penalización al no disponer de ellos.

REQUISITOS TÉCNICOS MÍNIMOS

Ante todo, cualquier tecnología que vaya a ser introducida en el sistema tecnológico de la organización, deberá de contar con los siguientes requisitos técnicos mínimos:

1. Los productos que formen parte de productos de seguridad deberán de estar certificados o cualificados en ENS, encontrarse en el catálogo de productos del guía CCN-STIC 105 ó, en una metodología de seguridad conocida como es common criteria o Lincie.

2. Toda aplicación o desarrollo de una aplicación que vaya a implantar o que se subcontrate para utilizarla en la nube deberá estar certificada en ENS. En caso de no estarlo, deberá de entregar una declaración de aplicabilidad dónde se refleje qué medidas de seguridad cumple y cuales no, sin perjuicio de que deba de cumplir obligatoriamente los siguientes puntos:

    i. Una aplicación no podrá disponer de usuarios locales, salvo aquella cuenta que sea para la administración local de la misma.
    ii. El software nunca dispondrá de cuenta de administrador y contraseña por defecto. En su lugar, se deberá de crear una nueva cuenta de administración que no incluya ninguna referencia en el nombre al rol de administrador, siempre que se pueda, y deberá de cambiar la contraseña por defecto de este antes de poner el software en producción.

    iii. No se podrá dejar credenciales en texto plano, scripts, sistemas o hardcodeadas en cualquier parte del código, ficheros de configuración, etc.

    iv. Las aplicaciones correrán en modo servicio en los sistemas operativos de windows o linux, y estas deberán de permitir ejecutarse bajo una cuenta de usuario de servicio.

    v. Las aplicaciones que hayan sido desarrolladas deberán haber sido desarrolladas mediante un proceso de desarrollo seguro S-SDLC y deberán de presentar un informe de análisis de código estático, otro informe de análisis de código dinámico y un último informe de análisis de vulnerabilidades. Estos informes deberán de ser aptos antes de su puesta en producción o contratación de la misma.

3. Para cualquier producto o aplicación, se usará autenticación y autorización de usuarios vía LDAPs. Esto implica que las políticas de seguridad serán definidas por el Active Directory o Azure Active Directory, como por ejemplo la política de contraseñas o la disponer de roles para los usuarios, como, por ejemplo: administrador, autorizado, usuario normal, técnico de seguridad, deberán de poderse sincronizarse e implementarse en este producto o aplicación.

4. Las aplicaciones o productos deberán de pasar un análisis de vulnerabilidades y no presentar ninguna vulnerabilidad crítica, alta o media, antes de ser puestas en producción. De presentar alguna, se rechazará su entrada en producción.

5. Las aplicaciones o productos deberán de disponer de logs seguridad que permitan su análisis de seguridad. Estos logs, indicarán, como mínimo:
    i. Auditar accesos correctos, fallidos;
    ii. Auditar modificaciones en las distintas acciones que realicen los usuarios: cambio de configuraciones, privilegios, subida o descarga de información, etc.

6. Los desarrollos de software y hardware que se realicen deberán de indicar en la documentación que se entregue, el listado de librerías o componentes software de terceros que utilicen.

7. La capacidad y dimensionamiento de un sistema o producto, deberá de ser coherente y soportar el producto o aplicación que quiera implementar, además de diversos servicios de seguridad que la organización establezca como medidas de seguridad. Estos servicios son del tipo: antivirus, copias de seguridad, monitorización, etc. En caso de que el sistema o producto no supere las pruebas de rendimiento con estos servicios de seguridad activados, el sistema o producto no podrá ser puesto en producción.

8. Si el proyecto, aplicación o sistema debe de estar conectado a internet o alguna red interna, deberá estudiarse el lugar dónde se ubicará y conectará este, dentro de su arquitectura, siempre desde el inicio del proyecto con el responsable de IT, IoT y OT.

9. Para la aceptación y el cierre de las actividades y fases de un proyecto que se implante en la organización, debe de estar autorizado por los técnicos del sistema, que mantendrán el sistema, y el responsable del servicio que contrate el proyecto.

10. Las aplicaciones están vivas, por tanto, si al cumplir el ciclo de vida de la aplicación no tiene mantenimiento de seguridad, deberá de ser retirada si dispone de vulnerabilidades conocidas o extraídas a través de los análisis de vulnerabilidades, provocando que se quite el servicio que presta esta aplicación y dicho servicio se quede inoperativo hasta reemplazarla o disponer de mantenimiento.

11. Se podrá realizar una auditoría de acciones realizadas en un servicio o desarrollo o realizar una auditoría de seguridad del proveedor para conocer el nivel de seguridad que se está estableciendo en los productos/aplicaciones/servicios.

En el caso de que se detecte alguna desviación en la auditoría, se podría para el proceso que se encuentre a la espera de que se solucione esta desviación o se podría proponer de manera interna un estudio de penalización al prestador debido a esta desviación.

Acuerdo de nivel de servicio (SLA) y penalizaciones

El prestador del servicio garantizará la prestación de los servicios objeto del contrato con los niveles mínimos en caso de ser detallados en este pliego de condiciones tecnicas.
La revisión del grado de cumplimiento de dichos niveles de servicio se realizará trimestralmente por parte del prestador del servicio y deberán de ser entregados a Diputación de Castellón para ser evaluados.
En caso de existir un incumplimiento de dichos niveles, Diputación de Castellón se reserva el derecho de aplicar las penalizaciones que se indican en el Pliego Administrativo.
La imposición de penalizaciones no impide a Diputación de Castellón el exigir al prestador del servicio el cumplimiento de sus obligaciones contractuales ni la indemnización de daños y perjuicios a que Diputación de Castellón pudieran tener derecho.

Acuerdo de nivel de servicio

El prestador del servicio deberá proponer a Diputación de Castellón un modelo de acuerdo de nivel de servicio que garantice la prestación de los servicios contratados dentro de unos límites aceptables.
Independientemente del contenido de dicho acuerdo de niveles de servicio, el ofertante se comprometerá, al menos, a garantizar a Diputación de Castellón que los servicios serán prestados con los niveles mínimos que se detallan a continuación:

1.Niveles mínimos de servicio o SLAs

Los prestadores del servicio, podrán añadir SLAs a los que se indiquen a continuación.
Los niveles de servicio mínimos que deberá cumplir el ofertante durante la operación del servicio son los siguientes:

Entrega de estado proyecto:

Nombre	**Entrega de Estado Proyecto Indicador 1, EEP**
Descripción	Entrega de Informes trimestrales del estado del proyecto y se calcula a través de: Tiempo de entrega de Informes
Nivel de servicio	La medición para este nivel de servicio se describe a continuación: La entrega de los Informes se hará como máximo el décimo día hábil del mes siguiente.
Entregable	Informe estado del proyecto.
Cobertura (tiempo)	Mensual

Entrega de Informes:

Nombre	**Entrega de Informes Indicador 2, EI**
Descripción	Entrega de Informes de las diferentes tareas del proyecto, y se calcula

	a través de: Tiempo de entrega de Informes
Nivel de servicio	La medición para este nivel de servicio se describe a continuación: La entrega de los Informes se hará como máximo el décimo día hábil del mes siguiente.
Entregable	Informe finalización de tarea.
Cobertura (tiempo)	Finalización de tarea.

Entrega de Documentos:

Nombre	**Entrega de Documentos Indicador 3, ED**
Descripción	Entrega de documentos asociados a las distintas tareas descritas en el proyecto sujetos a algún nivel de servicio, y se calcula a través de: Tiempo de entrega de documentos
Nivel de servicio	La medición para este nivel de servicio se describe a continuación: La entrega de los documentos se hará como máximo el décimo día hábil del mes siguiente a la finalización del contrato.
Entregable	Informe finalización de tarea.
Cobertura (tiempo)	Finalización de contrato.

Gestión de incidentes y brechas de seguridad:

Nombre	**Gestión de incidentes y brechas de seguridad Indicador 4, GIS**
Descripción	Tal y como se regula mediante la LOPD y el ENS, se debe de establecer un canal para la gestión de los incidentes de seguridad. Este nivel de servicio cubre la comunicación de incidentes y brechas de seguridad hayan presentado sobre la infraestructura de seguridad del prestador de servicios y repercutan un problema de seguridad en la información de Diputación de Castellón o la prestación de las tareas del presente pliego. Este nivel de servicio se calcula a través de: Tiempo promedio de respuesta de incidentes de seguridad La acción a medir: (respuesta) será la que se haya predefinido en los procedimientos de actuación. Acción de respuesta se considera aquella acción en la que se recibe el incidente o brecha y se comienza a trabajar en él.
Nivel de servicio	La medición para este nivel de servicio se describe a continuación: En los casos en los que un problema de seguridad se convierta en un incidente o brecha de seguridad en el prestador del servicio, se realizará la notificación en un máximo de 72 horas posterior a su detección. Una vez confirmado el incidente de seguridad, se tomarán las acciones de contención o notificación que se hayan definido junto con Diputación de Castellón en los procedimientos de operación.
Entregable	Dentro del Informe de eventos de incidentes o brechas de seguridad

	durante el periodo, se entregará al producirse este, indicando en el informe el motivo de la brecha o incidente de seguridad.
Cobertura (tiempo)	365 días
Criterio para aplicar penalización	Que la notificación a partir de la declaración del incidente/brecha de seguridad se realice en un plazo mayor a 72 horas desde su detección.

Personal Asignado al Servicio:

Nombre	**Personal Asignado al Servicio Indicador 5, PAS**
Descripción	Los recursos presenciales que el prestador del servicio adjudicatario hubiere determinado en su oferta estarán sujetos a la aplicación de los siguientes indicadores para determinar el nivel de cumplimiento: Personas asignadas al servicio o producto
Nivel de servicio	Días transcurridos con menos recursos presenciales que los propuestos por oferta, durante el periodo de facturación. Menos de 1 día baja, 5 días media, +5 días alta Diferencia de días en la comunicación de la salida de un recurso, incumpliendo el periodo de preaviso fijado, durante el periodo de facturación. Menos de 1 día baja, 5 días media, +5 días alta. Número de días de incumplimiento en el periodo de solapamiento entre un recurso saliente y el entrante, durante el periodo de facturación. Menos de 1 día baja, 5 días media, +5 días alta. Número de cambios no solicitados de los recursos propuestos, a lo largo de un año. No computan las coberturas siempre y cuando se hagan con los mismos suplentes. 1 Cambio año baja, + de 2 media, + de 3 alta
Entregable	Informe del servicio comprometido a efectos de personal.
Cobertura (tiempo)	Mensual

Indicadores

A continuación, se definen los indicadores objetivos por los que trimestralmente se va a evaluar la prestación del servicio, de acuerdo con las definiciones y niveles de servicio indicados. Niveles mínimos de servicio. El incumplimiento en los valores comprometidos supondrá la aplicación de las correspondientes penalizaciones.

Resumen de Indicadores:

- **Indicador 1, EEP**: Tiempo promedio de envío de informes mensuales de servicio.
- **Indicador 2, EI**: Tiempo promedio de envío de informes finales de servicio.
- **Indicador 3, ED**: Tiempo promedio de envío de informes finalización de tarea del servicio.
- **Indicador 4, GIS**: Tiempo promedio de contestación y respuesta de incidentes/brechas de seguridad.
- **Indicador 5, PAS**: Tiempo y numero de la disponibilidad de los recursos de personal.

Los diez indicadores anteriores se evaluarán según lo establecido en cada uno de ellos y para ello el prestador del servicio, proporcionará herramientas de medidas de tiempo para la correcta evolución de los indicadores.

Penalizaciones

Los indicadores asociados a los SLA de las cláusula anteriores fijan los niveles de servicio objetivos y mínimos, que se consideran adecuados para desempeñar la prestación de los servicios objeto de este pliego.
Los niveles de servicio por debajo de los umbrales marcados por los indicadores estarán sujetos a penalizaciones.
Según se explica en este PPT, el objetivo principal que se persigue con la contratación de estos servicios es implementar de ciberseguridad todo el sistema tecnológico de Diputación de Castellón.
Las penalizaciones se indicaran en el pliego admiistrativo

Procedimiento de comunicación

Para comunicar cualquier tipo de incidente o brecha de seguridad, tal y como regula el ENS con la figura del POC, deberá de hacerse como se indican más adelante en el presente documento.
La comunicación, que deberá de gestionar el prestador del servicio para los proyectos, deberá de llevarse a cabo con los responsables de proyecto de Diputación de Castellón y, para la comunicación sobre incidentes o brechas de seguridad deberá de hacerse la comunicación directamente al Responsable de Seguridad de la organización, a través de los medios convenidos con estas figuras, tal y como se regula , siendo alguno de estos que se mencionan a continuación:

- Comunicación por correo electrónico
- Comunicación por correo electrónico cifrado y firmado
- Comunicación telefónica y posterior envío de

RESPONSABILIDADES DEL POC

Tal y como se establece en el artículo 13.5 del RD 311/2022, en adelante el ENS, se ha de formalizar la designación de una figura POC(Punto o Persona de Contacto), entre la administración pública y la organización que va a ser contratada.
Para llevar a cabo esta tarea, es necesario recoger estos datos mediante la siguiente tabla que ha de ser rellenada:

Nombre y Apellidos del Responsable de Seguridad de la organización	
Email del Responsable de Seguridad de la organización	
Teléfono o móvil del Responsable de Seguridad de la organización	
Email o teléfono alternativo para el POC*	

Firma electrónica del Responsable de Seguridad de la Organización	

*No es necesario que el Punto de contacto sea una persona, en ocasiones puede ser una lista de distribución. En caso de que exista esa opción en la organización que va a ser contratada, es necesario indicar este campo.