

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN, MEDIANTE PROCEDIMIENTO ABIERTO SIMPLIFICADO DE TRAMITACIÓN ABREVIADA, DEL MANTENIMIENTO Y SOPORTE DEL SISTEMA DE CONTROL DE PRESENCIA CRONO, DE LA AGENCIA ANDALUZA DE COOPERACIÓN INTERNACIONAL PARA EL DESARROLLO.

Expte. CONTR 2024 944761

1. INTRODUCCIÓN

La Agencia Andaluza de Cooperación Internacional para el Desarrollo, en adelante AACID, ha iniciado a partir del año 2020 un proceso real de Transformación Digital y de modernización de los servicios ofrecidos a los ciudadanos y las entidades externas.

La AACID cuenta con un sistema de información desde mayo de 2009 para el control presencial de su personal denominado “Sistema de control de Presencia CRONO V.2”, muy utilizado por los organismos de la Junta de Andalucía, que actualmente se encuentra actualizado a la versión 2.83.

CRONO es gestionado por el Departamento de Recursos Humanos para las siguientes actividades:

- Control horario. Permite registrar las entradas y salidas de las personas empleadas.
- Gestión de permisos, licencias y vacaciones. A través del interfaz web permite la solicitud, validación y aprobación de los permisos susceptibles de ser disfrutados por las personas empleadas.
- Generación de informes.

Se trata por tanto de un sistema de información de vital importancia, utilizado a diario por todas las personas empleadas de la Agencia, que necesita disponer de un mantenimiento y soporte por parte de una empresa con personal técnico especializado en dicho sistema, con conocimientos tanto para resolver las incidencias que puedan surgir, como para la implementación de cambios de configuración/parametrización o bien de nuevas funcionalidades solicitadas por el Departamento de Recursos Humanos.

Como quiera que la AACID no dispone de recursos propios con los conocimientos especializados requeridos para abordar las actividades descritas, se considera necesaria la contratación de un servicio de mantenimiento y soporte de CRONO.

2. OBJETO

El objeto del presente contrato es que la Agencia disponga de un servicio de mantenimiento y soporte del sistema de información CRONO en todos sus subsistemas.



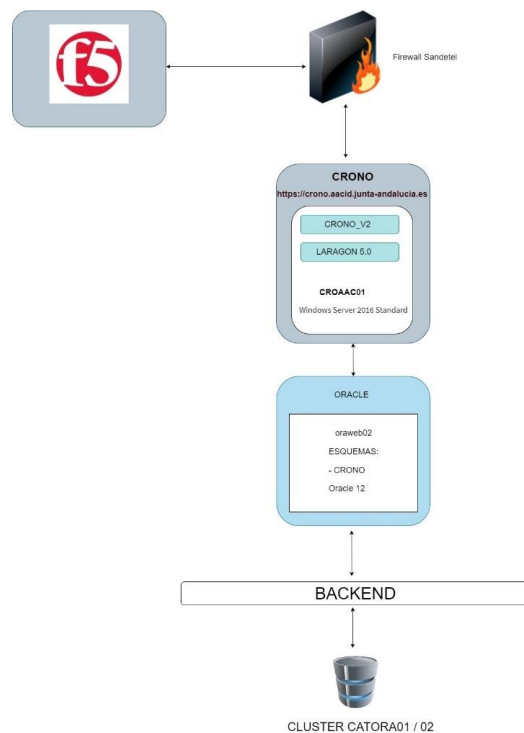
CELIA ROSELL MARTI		15/10/2024 09:29:10	PÁGINA: 1 / 20
VERIFICACIÓN	NJyGw1Q4vt3u2qg5KSOoC738d7A3v	https://ws050.juntadeandalucia.es/verificarFirma/	

El contrato deberá prestarse de conformidad con lo establecido en el presente Pliego, así como en el Pliego de Cláusulas Administrativas Particulares, debiendo seguir el adjudicatario, en todo caso, las indicaciones del responsable del contrato.

3. DESCRIPCIÓN DE LA SITUACIÓN ACTUAL

CRONO es un sistema de información basado en una arquitectura cliente-servidor, de forma que al igual que el resto de las aplicaciones de la AACID, se ha migrado al hosting gestionado por SANDETEL.

La arquitectura del entorno de producción de la aplicación se representa mediante la siguiente figura:



La aplicación cuenta también con un entorno de desarrollo (servidor DESAACCRO01), en el que se realizan las pruebas antes de la puesta en marcha.

En la parte cliente, la Agencia cuenta con un único terminal de fichaje en el acceso principal de la sede. Se trata de un ordenador de sobremesa con Microsoft Windows 10 Pro y Cronopicar 2.75, que se conecta de forma periódica con la base de datos de la aplicación para el volcado de los fichajes registrados a través de la aplicación Cronopicar.

Por último, los equipos de sobremesa de las personas del Departamento de RRHH disponen de un cliente de la aplicación CRONO, desde el que pueden realizar las tareas de administración.

CELIA ROSELL MARTI		15/10/2024 09:29:10	PÁGINA: 2 / 20
VERIFICACIÓN	NJyGwl1Q4vt3u2qg5KSOoC738d7A3v	https://ws050.juntadeandalucia.es/verificarFirma/	

El código fuente de la aplicación se encuentra publicado en el Repositorio de Software de la Junta de Andalucía.

4. DESCRIPCIÓN DEL SERVICIO

El servicio de Mantenimiento y Soporte del sistema de información CRONO, incluye las siguientes tareas:

- Resolución de incidencias que afecten a las funcionalidades de la aplicación.
- Mantenimiento correctivo, necesario en los casos en los que la resolución de una incidencia implique una modificación en el código (software) de la aplicación.
- Implementación de cambios en la configuración y parametrización de la aplicación.
- Mantenimiento proactivo de la aplicación, mediante revisiones periódicas, para asegurar el rendimiento adecuado presente y futuro.
- Mantenimiento evolutivo, necesario en los casos en los que la implementación de una nueva funcionalidad o mejora implique una modificación en el código (software) de la aplicación.

Para la gestión de peticiones de la Agencia a la empresa proveedora se implementará un modelo de trabajo basado en solicitudes de trabajo, soportado por una herramienta de ticketing, Redmine. Las tareas solicitadas por la Agencia se valorarán por parte de la empresa proveedora en horas de esfuerzo de cada uno de los perfiles involucrados. Las solicitudes de trabajo únicamente serán ejecutadas tras la validación por parte de la AACID de la planificación y recursos propuestos.

El horario del servicio será de 8:00 a 15:00 de lunes a viernes. También se tendrá la posibilidad de realizar trabajos programados fuera del horario laboral habitual, en los casos que junto con la empresa proveedora se acuerde que es lo más conveniente.

5. ORGANIZACIÓN DEL SERVICIO

La empresa proveedora deberá especificar una interlocución técnica única a efectos del contrato (Coordinación Técnica), que coordinará la ejecución de los trabajos de acuerdo con este proyecto técnico, pondrá en práctica las directrices de la Jefatura TIC de la AACID e impartirá las pertinentes instrucciones a los equipos de trabajo involucrados.

El trabajo se organizará principalmente en forma de proyecto.

Las principales funciones de la Coordinación Técnica por parte de la empresa proveedora son las siguientes:

- Garantizar que existe la documentación y en general los entregables requeridos por la Agencia.
- Coordinación de las actividades y tareas, y supervisión de los equipos técnicos.

CELIA ROSELL MARTI		15/10/2024 09:29:10	PÁGINA: 3 / 20
VERIFICACIÓN	NJyGwI1Q4vt3u2qg5KSOoC738d7A3v	https://ws050.juntadeandalucia.es/verificarFirma/	

- Asegurar el nivel de calidad de los trabajos. Control del cumplimiento de los Acuerdos de Nivel de Servicio (ANS), así como las desviaciones respecto a los niveles objetivo.
- Elaboración de propuestas de mejora en el ámbito de los trabajos solicitados.

Los equipos técnicos involucrados estarán constituidos por el personal técnico necesario, en número, cualificación y nivel de dedicación, para atender a los objetivos y programación de actividades previstas en el desarrollo del servicio.

6. CONTROL Y SEGUIMIENTO

Durante el transcurso de los trabajos, la AACID podrá establecer los controles que considere necesarios sobre la actividad desarrollada y los productos obtenidos. El seguimiento y control del servicio se efectuará mediante la presentación por parte de la empresa proveedora de informes, reuniones y cuantas acciones se estimen oportunas.

7. ACUERDOS DE NIVEL DE SERVICIO

Como medio para garantizar la calidad de los servicios suministrados, se establecerán unos Acuerdos de Nivel de Servicio (ANS), y el compromiso por parte de la empresa proveedora de cumplirlos. Los recursos tanto humanos como de otra índole disponibles para el servicio, deberán ser dimensionados de forma cualitativa y cuantitativa como mínimo para garantizar los Acuerdos de Nivel de Servicio establecidos.

Los Acuerdos de Nivel de Servicio se basarán en la definición de unos indicadores de calidad que reflejen de forma objetiva la calidad del servicio real suministrado, con especial atención a los aspectos más críticos del mismo, y en el establecimiento de un umbral o valor mínimo de calidad para cada uno de ellos.

Los Acuerdos de Nivel de Servicio (ANS) son los siguientes:

Tipo	Indicador	Valor objetivo
Gestión de incidencias	Tiempo de Respuesta <= 7h laborables	>= 90%
	Tiempo de Intervención <= 14h laborables	>= 90%
Gestión de peticiones	Tiempo de Valoración <= 28h laborables	>= 90%

De acuerdo con las siguientes definiciones:

- Tiempo de Respuesta: tiempo transcurrido desde que el equipo técnico de la Agencia envía la incidencia por alguno de los canales establecidos, y la empresa proveedora emite una primera respuesta.
- Tiempo de Intervención: tiempo transcurrido desde que el equipo técnico de la Agencia envía la incidencia por alguno de los canales establecidos, y la empresa proveedora realiza una primera actuación sobre el sistema de información CRONO.

- Tiempo de Valoración: tiempo transcurrido desde que el equipo técnico de la Agencia envía la solicitud de trabajo por alguno de los canales establecidos, y la empresa proveedora emite la valoración en horas de esfuerzo de cada uno de los perfiles involucrados.

8. CONDICIONES GENERALES DE LA PRESTACIÓN DEL SERVICIO

8.1. LUGAR DE REALIZACIÓN

Por petición del responsable del Contrato y para la óptima realización del proyecto, existe la posibilidad de que algunos trabajos se deban desarrollar en instalaciones o edificios de la AACID.

8.2. PROPIEDAD INTELECTUAL DE LOS TRABAJOS

Todos los estudios y documentos, así como los productos y subproductos elaborados por el contratista como consecuencia de la ejecución del presente contrato serán propiedad de la AACID, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el adjudicatario autor material de los trabajos. El adjudicatario renunciará expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del presente contrato pudiera corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este documento de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa de la AACID, específicamente todos los derechos de explotación y titularidad de las aplicaciones informáticas y programas de ordenador desarrollados al amparo de este contrato, corresponden únicamente a la Agencia.

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

8.3. SEGURIDAD

Las proposiciones deberán garantizar el cumplimiento de los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información que constituyen el Esquema Nacional de Seguridad, regulado por el 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.

En concreto, se deberá asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que son objeto de la presente contratación. Para lograr esto, se aplicarán las medidas de seguridad indicadas en el anexo II del ENS, en función de los tipos de activos presentes y las dimensiones de información relevantes, considerando las categorías de seguridad en las que recaen los sistemas de información objeto de la contratación según los criterios establecidos en el anexo I del ENS: categoría de seguridad BÁSICA.

Deberá también tenerse en cuenta lo dispuesto en el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía (modificado por el Decreto 70/2017, de 6 de junio) y en su

CELIA ROSELL MARTI		15/10/2024 09:29:10	PÁGINA: 5 / 20
VERIFICACIÓN	NJyGwI1Q4vt3u2qg5KSOoC738d7A3v	https://ws050.juntadeandalucia.es/verificarFirma/	

desarrollo a partir de la Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía y normativa asociada.

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

Además, se deberá atender a las mejores prácticas sobre seguridad recogidas en las series de documentos CCN-STIC (Centro Criptológico Nacional - Seguridad de las Tecnologías de Información y Comunicaciones), disponibles en la web del CERT del Centro Criptológico Nacional (<http://www.ccn-cert.cni.es/>), así como a las guías y procedimientos aplicables elaborados por la Unidad de Seguridad TIC Corporativa de la Junta de Andalucía.

8.4. TRATAMIENTO DE LOS DATOS DE CARÁCTER PERSONAL

La empresa proveedora, en cumplimiento de lo previsto en el Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo, de 27 de abril de 2016, y la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, únicamente tratará los datos conforme a las instrucciones de la AACID, y no los aplicará o utilizará con fin distinto al del contrato; ni los comunicará, ni siquiera para su conservación, a otras personas. Además, deberá cumplir las medidas técnicas y organizativas estipuladas en las normas de desarrollo de la citada Ley Orgánica. Esta obligación se aplica tanto a los ficheros en soporte informatizado como a cualquier otro tipo de soporte.

En el presente documento se incluye un Anexo I con la descripción del tratamiento de los datos de carácter personal.

8.5. CONFIDENCIALIDAD

A los efectos del contenido del presente contrato, tendrá la consideración de información confidencial toda información susceptible de ser revelada de palabra, por escrito o por cualquier otro medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, intercambiada como consecuencia de la ejecución de los trabajos solicitados por la AACID a la empresa proveedora, salvo que una de las partes identifique expresamente y por escrito que la información no tiene carácter de confidencial.

La empresa proveedora se compromete a adoptar las medidas oportunas para asegurar el tratamiento confidencial de dicha información, medidas que no serán menores que las aplicadas por ella a su propia información confidencial.

La empresa proveedora deberá permitir el acceso a la información confidencial únicamente a aquellas de sus filiales, representantes y/o personas físicas o jurídicas de la empresa proveedora o, que necesiten la información para el desarrollo de tareas relacionadas con la realización del presente contrato y siempre que el uso de esta información sea estrictamente necesario.

La empresa proveedora mantendrá toda la Información obtenida de la AACID en el ámbito del proyecto objeto del presente contrato, cualquiera que sea la forma en que la misma haya sido obtenida, como información estrictamente confidencial, y no la divulgará ni cederá a terceras personas sin el previo consentimiento escrito de la AACID. Cuando finalice el contrato, la empresa proveedora devolverá en

CELIA ROSELL MARTI		15/10/2024 09:29:10	PÁGINA: 6 / 20
VERIFICACIÓN	NJyGwI1Q4vt3u2qg5KSOoC738d7A3v	https://ws050.juntadeandalucia.es/verificarFirma/	

formato electrónico la documentación generada para el proyecto en cuestión, así como cualquier otro tipo de información que pueda haber obtenido. La empresa proveedora tampoco mantendrá ni divulgará los medios para obtener información de los Sistemas de Información de la AACID. Finalizado el proyecto, la empresa proveedora no retendrá una copia para sus archivos ni del informe ni de cualquier información obtenida durante la ejecución de este.

Las obligaciones y términos contenidos en este apartado mantendrán su vigencia desde la fecha de la firma de la contratación y se deberá mantener el deber de confidencialidad durante cinco años.

Las partes reconocen que el incumplimiento o amenaza de incumplimiento del presente apartado de Confidencialidad puede suponer un daño irreparable para la AACID y en consecuencia esta podrá adoptar, juntamente con otras a las que tenga derecho, medidas cautelares con el fin de impedir cualquier incumplimiento continuado o amenaza de incumplimiento del presente apartado de confidencialidad.

8.6. INTEROPERABILIDAD

Las ofertas garantizarán un adecuado nivel de interoperabilidad técnica, semántica y organizativa, conforme a las estipulaciones del Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (ENI). En concreto, se cumplirán las Normas Técnicas de Interoperabilidad establecidas por dicho esquema. Se cuidarán especialmente los aspectos de interoperabilidad orientados a la ciudadanía, de tal forma que se evite la discriminación a los ciudadanos por razón de sus elecciones tecnológicas.

El sistema implantará los protocolos ENIDOCWS y ENIEXPWS para que los documentos y expedientes electrónicos que se gestionen en el mismo puedan, a partir de sus códigos seguros de verificación, ser puestos a disposición e interoperar de manera estandarizada con otros sistemas y repositorios electrónicos de la Junta de Andalucía, así como remitirse a otras Administraciones si procede.

También se atenderá a los modelos de datos sectoriales relativos a materias sujetas a intercambio de información con la ciudadanía, otras Administraciones Públicas y entidades, publicados en el Centro de Interoperabilidad Semántica de la Administración (CISE) que resulten de aplicación.

En relación con el desarrollo de soluciones para la tramitación electrónica de los procedimientos, en todo caso se garantizará la plena interoperabilidad de las soluciones implantadas, de acuerdo con el art. 37.4 del Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía.

8.7. SOBRE LA GESTIÓN DE USUARIOS Y EL CONTROL DE ACCESOS

En todo lo relativo a la implementación de la funcionalidad de gestión de usuarios y control de accesos, se tendrán en cuenta las estipulaciones que sobre seguridad hace la legislación vigente en materia de tratamiento de datos personales, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) así como de la legislación nacional vigente en materia de

CELIA ROSELL MARTI		15/10/2024 09:29:10	PÁGINA: 7 / 20
VERIFICACIÓN	NJyGwl1Q4vt3u2qg5KSOoC738d7A3v	https://ws050.juntadeandalucia.es/verificarFirma/	

protección de datos, y el Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad, modificado por el Real Decreto 951/2015, de 23 de octubre. En particular, se perseguirá:

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

a) En relación con las directrices corporativas que se creen en materia de gestión de identidades.

En todo lo relativo a la implementación de la funcionalidad de gestión de usuarios y control de accesos (roles, gestión de login y password,) se deberán respetar las directrices que la Junta de Andalucía elabore en lo referente a la gestión de identidades y en su caso, adaptándose a la solución de single sign-on que la Junta haya provisto. Dichas directrices se proporcionarán con la suficiente antelación, aportando la documentación técnica existente para tal fin.

b) En el caso de que, en alguno de los sistemas, aplicaciones, herramientas, etc. objeto del contrato se gestionen trámites y actuaciones que se realizan con la Administración de la Junta de Andalucía por razón de la condición de empleado público.

El sistema deberá admitir, para los trámites y actuaciones que su personal realice con ella por razón de su condición de empleado público, el sistema de identificación de la plataforma de Gestión Unificada de Identidades de Andalucía (GUIA) de acuerdo con el artículo 25.1 del Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía.

8.8. USO DE INFRAESTRUCTURAS TIC Y HERRAMIENTAS CORPORATIVAS

En el marco de lo dispuesto sobre el impulso de los medios electrónicos en el art. 36.1 del Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía, se tendrán en cuenta todas las infraestructuras TIC (sistemas de información, tecnologías, frameworks, librerías software, etc.) que en la Junta de Andalucía tenga la consideración de corporativas u horizontales y sean susceptibles de su utilización. Se considerarán, entre otras, las siguientes:

- Para el modelado y tramitación de los flujos de trabajo ligados a procedimientos administrativos se deberá utilizar el tramitador TREW@ y herramientas asociadas (eximiéndose de esta obligación en El certifiel caso de flujos de trabajo que no estén ligados a procedimientos).
- @firma: la plataforma corporativa de autenticación y firma electrónica para los procedimientos administrativos, trámites y servicios de la Administración de la Junta de Andalucía.
- Autoridad de Sellado de Tiempo de la Junta de Andalucía.
- @ries: el registro unificado de entrada/salida.
- notific@: prestador de servicios de notificación.

CELIA ROSELL MARTI		15/10/2024 09:29:10	PÁGINA: 8 / 20
VERIFICACIÓN	NJyGwI1Q4vt3u2qg5KSOoC738d7A3v	https://ws050.juntadeandalucia.es/verificarFirma/	

- LDAP del correo corporativo para la identificación y autenticación de usuarios, hasta que se produzca la implantación definitiva del Directorio Corporativo de la Junta de Andalucía.
- port@firma: gestor de firma electrónica interna.
- etc.

8.9. METODOLOGÍA

Tanto para la organización del trabajo como para las fases de desarrollo y los productos a obtener se tendrá como referencia la metodología para la planificación y el desarrollo de sistemas de información METRICA v3 publicada por el Ministerio de Administraciones Públicas. Dadas las especiales características de este trabajo, los procesos y las actividades que indica la metodología se adaptarán al mismo con el objeto de conseguir la mayor eficacia en su desarrollo. La empresa oferente indicará a la Agencia la adecuación metodológica al proyecto que proponen.

La Jefatura TIC de la AACID aprobará al comienzo de este las directrices metodológicas e interpretará de igual modo las posibles dudas que sobre su aplicación puedan surgir a lo largo de la ejecución del servicio.

8.10. CONFORMIDAD CON LOS MARCOS METODOLÓGICOS DE DESARROLLO DE SOFTWARE DE LA JUNTA DE ANDALUCÍA

Durante la realización de los trabajos se tendrán en cuenta los recursos proporcionados por los marcos metodológicos vigentes de desarrollo de software en la Junta de Andalucía, así como las pautas y procedimientos definidos en éstos.

8.11. ACCESIBILIDAD

Todos los sitios webs y aplicaciones para dispositivos móviles desarrollados o que sean mejorados de manera significativa en el marco del presente contrato deberán ser accesibles para sus personas usuarias y, en particular, para las personas mayores y personas con discapacidad, de modo que sus contenidos sean perceptibles, operables, comprensibles y robustos. La accesibilidad se tendrá presente de forma integral en el proceso de diseño, gestión, mantenimiento y actualización de contenidos de los sitios web y las aplicaciones para dispositivos móviles.

En este ámbito se deberán cumplir lo establecido por el Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público. En particular, se deberán cumplir los requisitos pertinentes de la norma UNE-EN 301-549:2019, de Requisitos de accesibilidad de productos y servicios TIC, o de las actualizaciones de dicha norma, así como de las normas armonizadas y especificaciones técnicas en la materia que se publiquen en el Diario Oficial de la Unión Europea y/o hayan sido adoptadas mediante actos de ejecución de la Comisión Europea.

Por último, como obliga la normativa se deberá realizar al menos una revisión anual de la accesibilidad de los sitios web y sistemas desarrollados o mejorados de manera significativa en el marco del contrato, así como actualizar y en su caso, elaborar, la correspondiente Declaración de accesibilidad de conformidad con el modelo europeo establecido Decisión de Ejecución (UE) 2018/1523 de la Comisión

CELIA ROSELL MARTI		15/10/2024 09:29:10	PÁGINA: 9 / 20
VERIFICACIÓN	NJyGw1Q4vt3u2qg5KSOoC738d7A3v	https://ws050.juntadeandalucia.es/verificarFirma/	

de 11 de octubre de 2018 por la que se establece un modelo de declaración de accesibilidad de conformidad con la Directiva (UE) 2016/2102 del Parlamento Europeo y del Consejo sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público.

8.12. NORMALIZACIÓN DE FUENTES Y REGISTROS ADMINISTRATIVOS

Con la finalidad de asegurar la compatibilidad e interoperabilidad con otras fuentes y registros administrativos, el tratamiento de variables demográficas (sexo, edad, país de nacimiento, nacionalidad, estado civil, composición del hogar), geográficas (país, región y provincia, municipio y entidad de población, dirección, coordenadas) o socioeconómicas (situación laboral, situación profesional, ocupación, sector de actividad en el empleo, nivel más alto de estudios terminado) que se haga en el sistema seguirá las reglas para la normalización en la codificación de variables publicadas por el Instituto de Estadística y Cartografía de Andalucía accesibles a través de la URL:

<http://www.juntadeandalucia.es/institutodeestadisticaycartografia/ieagen/sea/normalizacion/ManNormalizacion.pdf>

8.13. APERTURA DE DATOS

El diseño y desarrollo informático deberá facilitar el acceso y descarga de todos los datos existentes en la aplicación, así como posibilitar su publicación en el Portal de Datos Abiertos de la Junta de Andalucía. Los datos se proporcionarán en formatos estructurados, abiertos e interoperables, de acuerdo con la normativa vigente de publicidad y reutilización de información pública.

Los sistemas de información desarrollados deberán permitir la descarga de todos los datos en bruto y desagregados en varios formatos no propietarios como, por ejemplo, CSV, JSON, XML o también un estándar de facto como EXCEL (de las tablas que constituyan el núcleo de la aplicación, así como las tablas auxiliares para su interpretación) preferiblemente mediante API REST (interfaz de programación de aplicaciones), basado en estándares abiertos que permitirá el acceso automático a los datos y en tiempo real.

Si los anteriores conjuntos de datos contienen información de carácter personal, se realizarán la extracción de datos mediante un proceso de disociación o anonimización que garantice el cumplimiento de la Ley de Protección de Datos.

8.14. APERTURA DE SERVICIOS

Las ofertas presentadas deberán estar orientadas a la estrategia “API First”, teniéndose en cuenta la necesidad de definir y publicar servicios comunes que puedan ser consumidos desde varios canales, sistemas u organismos. Este enfoque está basado en definir en la fase inicial una API de servicios externos e internos de la organización o sistema, para que los distintos interlocutores y canales puedan utilizar los servicios de la API en cuanto se publique.

La especificación OpenAPI (OAS) define un estándar para la descripción de APIs REST, que permite tanto a humanos como a servicios de integración descubrir y entender las capacidades y características de un servicio sin necesidad de acceder a los detalles de implementación del código fuente, documentación técnica, o detalles del tráfico de mensajes. Los servicios definidos apropiadamente a partir del estándar

CELIA ROSELL MARTI		15/10/2024 09:29:10	PÁGINA: 10 / 20
VERIFICACIÓN	NJyGwI1Q4vt3u2qg5KSOoC738d7A3v	https://ws050.juntadeandalucia.es/verificarFirma/	

OpenAPI, permiten que un consumidor pueda entender e interactuar con un servicio remoto a partir de una implementación mínima.

En concreto, la definición de los servicios de la API se realizará cumpliendo las especificaciones OpenAPI establecidas por dicha organización (OAS). En relación con los estándares a emplear en el marco del presente contrato, las ofertas deben garantizar el cumplimiento y utilización del estándar y normas establecidas por OpenAPI, en los casos que fuese necesario.

8.15. COSTES DEL SERVICIO Y APLICACIÓN DE LA INSTRUCCIÓN 1/2024

En aplicación de la Instrucción 1/2024, de 2 de abril de 2024, de la Agencia Digital de Andalucía, sobre Perfiles, Precios de referencia y desglose de costes en contratos de Bienes y Servicios TIC:

1. Todas las contrataciones de bienes y servicios TIC de la Junta de Andalucía en cuya estimación del Presupuesto Base de Licitación se empleen perfiles profesionales deberán emplear los perfiles recogidos en el Anexo I de dicha Instrucción.

2. Se incluye en el Anexo II de dicha instrucción una memoria que sirve de referencia para los contratos de bienes y servicios TIC sobre la metodología de justificación de costes indirectos en la determinación del precio del contrato, de acuerdo con la legislación actual.

3. Para la determinación del precio en las contrataciones de bienes o servicios informáticos en las que intervengan costes laborales se tomaran como precios de referencia la lista de precios recogidos en el Anexo III.A de dicha Instrucción.

Estos precios ya incluyen los costes directos e indirectos aplicando la metodología descrita en el Anexo II de la citada Instrucción, de conformidad con la Ley de Contratos del Sector Público. Por el mismo motivo, en el listado del Anexo III.B se incluye también junto con cada perfil profesional la categoría profesional equivalente del área de actividad 2 (Gestión de medios y procesos) o del área de actividad 3 (Consultoría, desarrollo y sistemas) del XVIII Convenio colectivo estatal de empresas de consultoría y estudio de mercado y de la opinión pública (BOE nº. 177, 26 de julio de 2023), de obligada observancia para todas las empresas que presten servicios de informática, y el precio mínimo del citado perfil según convenio.

En el caso de que en una contratación se considere para la determinación del precio de licitación una tarifa que incremente el precio medio de referencia definido en el Anexo III.A, se deberá realizar una justificación en la documentación asociada a la solicitud de Informe Vinculante correspondiente a dicha contratación.

En el caso de que en una contratación se considere para la determinación del precio de licitación una tarifa que decremente el precio medio de referencia, esta tarifa no podrá ser inferior al mínimo que se indican en la tabla del Anexo III.A, que se corresponden con un decremento del 20% sobre el valor medio.

Siguiendo la categorización y homogeneización de los perfiles profesionales anteriormente descritos, se incluye a continuación una tabla que representa el dimensionamiento inicialmente estimado:

Perfil DGTD	Tarifa hora (IVA inc)	Nº horas estimadas anuales	Importe total (IVA inc)
ESPECIALISTA TÉCNICO (TECHNICAL SPECIALIST)	40,00 €	60	2.400,00 €
DESARROLLADOR (DEVELOPER)	37,00 €	40	1.480,00 €
Importe total servicio Mantenimiento y Soporte CRONO (IVA inc)			3.880,00 €

CELIA ROSELL MARTI		15/10/2024 09:29:10	PÁGINA: 11 / 20
VERIFICACIÓN	NJyGw1Q4vt3u2qg5KSOoC738d7A3v	https://ws050.juntadeandalucia.es/verificarFirma/	

El precio de licitación para el servicio descrito en el presente documento es de TRES MIL DOSCIENTOS SEIS EUROS Y SESENTA Y UN CÉNTIMOS (3.206,61 €, IVA excluido).

8.16. PLAZO DE EJECUCIÓN

El plazo de ejecución será de 12 meses, a contar desde la fecha de formalización del contrato.

La Directora de la Agencia Andaluza de
Cooperación Internacional para el Desarrollo
Fdo.: Celia Rosell Martí

CELIA ROSELL MARTI		15/10/2024 09:29:10	PÁGINA: 12 / 20
VERIFICACIÓN	NJyGwl1Q4vt3u2qg5KSOoC738d7A3v	https://ws050.juntadeandalucia.es/verificarFirma/	

ANEXO I
TRATAMIENTO DE DATOS PERSONALES

El presente contrato conlleva el tratamiento de datos de carácter personal por lo que, en el desarrollo de los trabajos que el mismo contempla, se deberán respetar en su integridad el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (en adelante, RGPD), la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, Ley 3/2018) y demás normativa de aplicación en vigor en materia de protección de datos.

El sometimiento de la empresa adjudicataria a la normativa sobre protección de datos constituye una obligación esencial del contrato que se le formula, teniendo la consideración de persona encargada del tratamiento que se describe en el presente Anexo.

A) Descripción general del tratamiento de Datos Personales a efectuar

El tratamiento consistirá en:

- Línea de actuación: Acceso a datos personales de empleados públicos contenidos en la aplicación CRONO.

El personal adscrito por la persona adjudicataria, para proporcionar las prestaciones establecidas en el presente proyecto técnico puede tratar Datos Personales. Los Datos Personales se tratarán únicamente por el personal adscrito y al único fin de efectuar el alcance del contrato.

B) Colectivos y datos tratados

Los colectivos de interesados y Datos Personales tratados a los que puede tener acceso la empresa adjudicataria son:

Tratamientos y principales colectivos de interesados	Principales colectivos de interesados	Datos Personales del tratamiento a los que se puede acceder
Línea de actuación: Acceso a datos personales de empleados públicos contenidos en la aplicación CRONO.	<i>Empleados públicos</i>	Nombre y apellidos, dni, correo electrónico, teléfono, dirección, fecha de nacimiento, sexo, tipo de representación, periodos de incapacidad laboral y permisos retribuidos.

C) Elementos del tratamiento

El tratamiento de los Datos Personales comprenderá:

☒ Recogida (captura de datos)	☐ Registro (grabación)	☐ Estructuración
☐ Modificación	☒ Conservación (almacenamiento)	☐ Extracción (retrieval)
☒ Consulta	☐ Cesión	☐ Difusión
☐ Interconexión (cruce)	☐ Cotejo	☐ Limitación
☐ Supresión	☐ Destrucción (de copias temporales)	☒ Conservación (en sus sistema inf.)
☐ Duplicado	☐ Copia (copias temporales)	☐ Copia de seguridad
☐ Recuperación	Otros (especificar):	

D) Disposición de los datos al terminar la prestación

Una vez finalice el contrato, la empresa adjudicataria debe:

- Devolver al Responsable del Tratamiento los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación. La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado. No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación. No obstante, el Responsable del Tratamiento podrá requerir al encargado para que en vez de esta opción, cumpla con alguna de las dos siguientes.
- Entregar al encargado que designe por escrito el Responsable del Tratamiento, los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida prestación. La entrega debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado. No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.
- Destruir los datos, una vez cumplida la prestación. Una vez destruidos, el encargado debe certificar su destrucción por escrito y debe entregar el certificado al Responsable del Tratamiento. No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

E) Actualización del Anexo de Protección de Datos

En caso de que, como consecuencia de la ejecución de los trabajos por parte de la empresa adjudicataria, resultara necesaria la modificación de lo estipulado en el presente Anexo, así lo requerirá razonadamente a la AACID y señalará los cambios que solicita. En caso de que la AACID estuviese de acuerdo con lo solicitado emitiría un anexo actualizado, de modo que el mismo siempre recoja fielmente el detalle del tratamiento.

CELIA ROSELL MARTI		15/10/2024 09:29:10	PÁGINA: 14 / 20
VERIFICACIÓN	NJyGwl1Q4vt3u2qg5KSOoC738d7A3v	https://ws050.juntadeandalucia.es/verificarFirma/	

F) Medidas de seguridad

Los datos deben protegerse empleando las medidas que un organismo ordenado debe tomar para evitar que dichos datos pierdan su razonable confidencialidad, integridad y disponibilidad. De acuerdo con la evaluación de riesgos realizada, se deben implantar, al menos, las medidas de seguridad siguientes.

La persona adjudicataria no podrá no implementar o suprimir dichas medidas mediante el empleo de un análisis de riesgo o evaluación de impacto salvo aprobación expresa del órgano de contratación.

A estos efectos, el personal del adjudicatario debe seguir las medidas de seguridad establecidas por el órgano de contratación, no pudiendo efectuar tratamientos distintos de los definidos.

1) Funciones y obligaciones del personal

- Las funciones y las obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal responsabilidad del Responsable del Tratamiento y a los sistemas de información estarán claramente definidas y documentadas por el Encargado de Tratamiento.
- El Encargado de Tratamiento deberá adoptar las medidas necesarias para que el personal con acceso a datos personales responsabilidad del Responsable del Tratamiento conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

2) Registro de incidencias

- El Encargado de Tratamiento deberá disponer de un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal responsabilidad del Responsable del Tratamiento que contendrá un registro en el que se haga constar:
 - el tipo de incidencia
 - el momento en que se ha producido, o en su caso, detectado
 - la persona que realiza la notificación
 - a quién se le comunica
 - los efectos que se hubieran derivado de la misma
 - las medidas correctoras aplicadas
- El Encargado del Tratamiento deberá resolver las vulnerabilidades críticas (según las escalas y métricas determinadas por CVSS) en el plazo de 1 mes desde que hayan sido detectadas y en caso de no ser críticas en el plazo máximo acordado entre ambas partes para su resolución.

3) Control de acceso

- Los usuarios deberán tener acceso únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

CELIA ROSELL MARTI		15/10/2024 09:29:10	PÁGINA: 15 / 20
VERIFICACIÓN	NJyGwl1Q4vt3u2qg5KSOoC738d7A3v	https://ws050.juntadeandalucia.es/verificarFirma/	

- El Encargado del Tratamiento deberá elaborar una relación actualizada de los usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos, así como establecer los mecanismos necesarios para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
- Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios que debe establecer el Encargado del Tratamiento.
- Proceso formal para el control y gestión de las autorizaciones respecto a los sistemas de información y siguientes dispositivos:
 - Se mantendrá un control en la entrada y utilización de instalaciones, tanto habituales como alternativas.
 - Se mantendrá un control en la entrada de equipos en producción, en particular, equipos que involucren criptografía.
 - Se mantendrá un control en la entrada de aplicaciones en producción.
 - Se mantendrá un control en el establecimiento de enlaces de comunicaciones con otros sistemas.
 - Se mantendrá un control en la utilización de medios de comunicación (tanto habituales como alternativos).
 - Se mantendrá un control en la utilización de soportes de información.
 - Se mantendrá un control en la utilización de equipos móviles.
- Para el acceso a los datos se deberá establecer un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

4) Gestión de soportes y documentos

- Los soportes y documentos que contengan datos de carácter personal del Responsable del Tratamiento deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado. En cuanto a los criterios de archivo, se debe garantizar la correcta conservación, localización y consulta de los documentos y posibilitar el ejercicio de derechos.
- La salida de soportes y documentos que contengan datos de carácter personal responsabilidad del Responsable del Tratamiento, incluidos los comprendidos y/o anexos a un correo electrónico, fuera de los locales en donde estén ubicados los ficheros, deberá ser autorizada por la persona que designe el Encargado de Tratamiento o encontrarse debidamente autorizada en el documento de seguridad. Dichos soportes deberán estar cifrados.
- En el traslado de la documentación que contenga datos de carácter personal responsabilidad del Responsable del Tratamiento, el Encargado del Tratamiento deberá adoptar las medidas

CELIA ROSELL MARTI		15/10/2024 09:29:10	PÁGINA: 16 / 20
VERIFICACIÓN	NJyGw11Q4vt3u2qg5KSOoC738d7A3v	https://ws050.juntadeandalucia.es/verificarFirma/	

necesarias para evitar la sustracción, pérdida o acceso indebido a la información durante su transporte. Se deberá mantener un registro de entrada y salidas de soportes o documentos que identifique quién accede y la fecha de estos.

- Siempre que se vaya a desechar cualquier documento o soporte que contenga datos de carácter personal responsabilidad del Responsable del Tratamiento, el Encargado del Tratamiento deberá proceder a su destrucción o borrado, mediante la adopción de las medidas necesarias para evitar el acceso a la información contenida en el mismo o su recuperación posterior.
- Los soportes que contengan datos de carácter personal especialmente sensibles se deberán identificar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de las personas.
- Los dispositivos de almacenamiento que contengan datos de carácter personal especialmente sensibles se deberán disponer de mecanismos que obstaculicen su apertura, o en su defecto, medidas que impidan el acceso de personas no autorizadas.
- Se debe custodiar la documentación cuando no se encuentre archivada en los dispositivos de almacenamiento.
- Se exigirá que los puestos de trabajo permanezcan despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.

5) Identificación y autenticación

- El Encargado del Tratamiento debe establecer una segregación interna de funciones adecuada, con la finalidad de gestionar el riesgo de acceso por parte de usuarios no autorizados. El Encargado del Tratamiento establecerá las medidas suficientes y necesarias para asegurar que los derechos de acceso (roles y perfiles) asignados internamente por el Encargado del Tratamiento para prestar el servicio, lo son de acuerdo a las necesidades funcionales del proyecto y a la seguridad para el Responsable del Tratamiento.
- El Encargado del Tratamiento deberá garantizar la trazabilidad de las acciones realizadas en los sistemas que almacenan información del Responsable del Tratamiento pudiendo identificarse en todo momento la persona concreta que las realizó. No se permitirá la existencia de usuarios genéricos salvo aquellos requeridos por las tecnologías empleadas y en este caso, su uso debe estar inventariado y controlado. Debe ser aprobado y validado por el Responsable del Tratamiento.
- Si el mecanismo de autenticación se basa en la existencia de contraseñas deberá existir un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. Las contraseñas se cambiarán con la periodicidad que indique el Responsable del

CELIA ROSELL MARTI		15/10/2024 09:29:10	PÁGINA: 17 / 20
VERIFICACIÓN	NJyGwI1Q4vt3u2qg5KSOoC738d7A3v	https://ws050.juntadeandalucia.es/verificarFirma/	

Tratamiento, que en ningún caso será superior a un año, y mientras estén vigentes se almacenarán de forma ininteligible.

6) Copias de respaldo y recuperación

- El Encargado de Tratamiento deberá encargarse de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos responsabilidad del Responsable del Tratamiento y deberá realizar copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.
- Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberán garantizar en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. En el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, se deberá grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.
- El Encargado del Tratamiento deberá verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos de carácter personal responsabilidad del Responsable del Tratamiento.
- Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal del Responsable del Tratamiento no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad. Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

7) Verificación

- El Encargado de Tratamiento deberá someterse a un proceso de verificación, evaluación y valoración de la eficacia de las medidas técnicas periódicamente o tras cada cambio importante en la organización.

8) Seguridad en los accesos a datos a través de redes de comunicaciones

- Las medidas de seguridad exigibles a los accesos a través de redes de comunicaciones deben garantizar un nivel de seguridad equivalente a los accesos en modo local anteriormente mencionados.
- El Encargado de Tratamiento deberá garantizar que las comunicaciones se realizan mediante protocolos de comunicación seguros (SSH, S-FTP, Editran, SSL, IPsec VPN, etc.). La transmisión de datos a través de redes públicas o de redes inalámbricas debe ser cifrada por algoritmos acreditados por el CCN.

CELIA ROSELL MARTI		15/10/2024 09:29:10	PÁGINA: 18 / 20
VERIFICACIÓN	NJyGw1Q4vt3u2qg5KSOoC738d7A3v	https://ws050.juntadeandalucia.es/verificarFirma/	

- El Encargado de Tratamiento deberá establecer mecanismos de defensa perimetral a la red (Cortafuegos, Proxy, DMZ, IPS/IDS, etc.).
- El Encargado del Tratamiento deberá garantizar el adecuado aislamiento entre los diferentes organismos a los que presta servicio.
- Ambas partes se comprometen a reducir al mínimo necesario las conexiones entre ambos organismos.
- El Encargado del Tratamiento deberá tomar las medidas preventivas necesarias para evitar que un incidente potencial en cualquier elemento de su red sea propagado al Responsable del Tratamiento.
- El Responsable del Tratamiento podrá realizar auditorías técnicas para validar la adecuada segmentación de dichas redes así como el nivel de seguridad de los elementos conectados.

9) Registros de accesos

- Para todo tratamiento de dato sensible, el prestador de servicios todas las actividades de los usuarios en el sistema de información, deberá indicar quién realiza la actividad, cuándo la realiza y sobre qué información, sea cual sea el usuario.
- El registro de acceso se mantendrá un mínimo de los dos últimos años de forma ininterrumpida.
- El Encargado de Tratamiento revisará mensualmente los registros de accesos y emitirá un informe con las incidencias surgidas durante la revisión, que podrá ser solicitado por el Responsable del Tratamiento.

10) Planes de contingencia y continuidad

- Planes de contingencia para los servicios que van a prestarse al Responsable del Tratamiento. El plan de contingencia deberá haber sido probado o disponer de un plan de pruebas y como tal el Encargado de Tratamiento deberá facilitar evidencias, resultado y/o la realización de las pruebas si así lo requiere el Responsable del Tratamiento.
- Plan de continuidad del Encargado de Tratamiento. El plan de continuidad deberá haber sido probado y como tal el Encargado de Tratamiento deberá facilitar evidencias y resultado de su última prueba si así lo requiere el Responsable del Tratamiento.

11) Cifrado

- Se protegerá la Información que contenga datos sensibles (datos especialmente protegidos: datos de ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual, datos genéticos, biométricos, las infracciones y condenas penales, aunque no las administrativas) almacenados en el disco mediante cifrado, de manera que un tercero no autorizado no pueda leerla.

CELIA ROSELL MARTI		15/10/2024 09:29:10	PÁGINA: 19 / 20
VERIFICACIÓN	NJyGwl1Q4vt3u2qg5KSOoC738d7A3v	https://ws050.juntadeandalucia.es/verificarFirma/	

12) Para encargados de tratamiento que desarrollen software

- El desarrollo de software se realizará sobre la base de las mejores prácticas de la industria, debiendo velar en todo el ciclo de desarrollo del software (diseño, desarrollo y prueba) por la seguridad de la información.
- El desarrollo de las aplicaciones web (tanto internas como externas siempre que incluyan acceso administrativo web a la aplicación) se basarán en directrices de codificación segura tales como la Guía OWASP (Open Web Application Security Project / Proyecto abierto de seguridad de aplicaciones web), por lo que el Encargado de Tratamiento deberá enfocar la seguridad de aplicaciones informáticas desarrolladas considerando todas sus dimensiones: personas, procesos y tecnologías.

La Jefatura TIC de la Agencia Andaluza de
Cooperación Internacional para el Desarrollo
Fdo.: Miguel Ballesteros Cáliz

CELIA ROSELL MARTI		15/10/2024 09:29:10	PÁGINA: 20 / 20
VERIFICACIÓN	NJyGwl1Q4vt3u2qg5KSOoC738d7A3v	https://ws050.juntadeandalucia.es/verificarFirma/	