Cliente/Servicio – *Client/Service*: ES0227/S001
Referencia - *Reference*: ES022700104606530
Fecha de validez – *Valid until*: 31/07/2027

Proveedor de servicio / *Service provider*

CTI Tecnología y Gestión SA

Identificación del servicio calificado/ *Rated Service identification*

Externalización de procesos (BPO)/
Business Process Outsourcing (BPO)

Descripción del servicio calificado / *Rated service description*

Identificacion servicio:Servicios de externalización de los procesos (BPO) para la gestión de información del Registro de Aceptaciones Impagadas (RAI)

Las entidades presentadoras enviarán su información a CTI mediante una sesión EDItran, o cualquier otro metodo de envio pactado con la entidad, y con los datos cifrados, un fichero en el que figurarán los datos de los deudores a los que habrá que enviar notificación de impago.
Recepción de los ficheros de contribución remitidos por los usuarios, la validación de la información, la carga de los datos, producción de ficheros, envío de ficheros de errores, realización de bajas comunicadas por las entidades y bajas por la actualización semanal y por prescripción de la información, y en general todos los relativos al mantenimiento del Fichero RAI.
Los relativos al servicio de Notificación de Impago a Deudores (SNID) del RAI.

Service Identification: Business Process Outsourcing (BPO) services for managing information in the Register of Unpaid Acceptances (RAI)

Submitting entities will send their information to CTI via an EDItran session, or any other transmission method agreed upon with the entity. The data will be encrypted and submitted as a file containing the information of debtors to whom non-payment notifications must be sent.
This includes receiving contribution files submitted by users, validating the information, uploading the data, generating files, sending error files, processing removals requested by the entities and removals due to weekly updates and the expiration of the information, and, in general, all tasks related to maintaining the RAI File.
This also includes tasks related to the Debtor Non-Payment Notification (SNID) service of the RAI.

Alcance / *Scope*

Recepción de Ficheros
CTi es responsable de la recepción de los ficheros de contribución remitidos por los usuarios; este intercambio se realiza acordando con cada entidad presentadora la configuración de envío a través de alguna de las opciones:

- Línea dedicada,
- Túneles Ipsec con un equipo FortiGate 101F,
- Proxy Editrán.

Una vez establecida la conexión segura, la entidad establece una sesión con Editran y envía así con doble cifrado los ficheros.
Semanalmente las entidades informantes enviarán a CTI dos ficheros, uno con los datos para notificar los impagos y otro con las modificaciones y bajas de la semana, produciendo el borrado del apunte en el fichero RAI, o en el fichero de notificaciones, caso de hallarse en esa situación, evitando su inclusión en el fichero RAI.

Recepción alternativa
Las entidades podrán enviar los datos al CPD de CTI, utilizando un soporte físico (CD / DVD (700MB / 4.7GB).
En el caso que el soporte fuera otro, la entidad deberá notificar a CTI para que se estimen los plazos para el procesamiento del nuevo soporte.
Antes de cada envío de soportes físicos a CTI, la entidad deberá notificarlo mediante una petición de proceso excepcional de ficheros, mediante un correo

electrónico a CTI indicando la descripción del tipo y contenido del soporte enviado a través de la dirección mail rai@ctisoluciones.com

El envío del soporte se deberá realizar, a la atención del contacto principal del Proyecto de CTI, a la siguiente dirección: Avda. deEuropa nº 19, Alcobendas - Madrid 28108
Cuando CTI reciba el soporte, enviará una nota de recepción a la entidad vía correo electrónico.

Procesamiento de información
Una vez recibida toda la información de las entidades, se iniciarán los procesos Batch de actualización, con los ficheros de datos enviados por las entidades presentadoras a lo largo de la semana. CTi procesa la información en su servidor interno con la aplicación de desarrollo RAI con las siguientes funciones:

- Validación de la información,
- carga de los datos,
- producción de ficheros,
- envío de ficheros de errores,
- realización de bajas comunicadas por las entidades
- bajas por la actualización semanal y por prescripción de la información,

Así como en general todos los relativos al mantenimiento del Fichero RAI conforme a las Normas de Funcionamiento del fichero, definidas por CCI.

Su finalidad es la de actualizar tanto los ficheros individuales de notificaciones de cada entidad, como el fichero común de RAI con los ficheros de aportaciones de datos de cada entidad.

Existen 3 tipos de procesos de actualización semanal:

A. Proceso de actualización de ficheros de notificaciones particulares de cada entidad.
B. Procesos de impresión de cartas de notificaciones y envío por Correos.
C. Procesos de actualización del fichero común del RAI.

Una vez finalizado el proceso de actualización semanal, CTI envía a CCI, o a quien esta designe, los ficheros de RAI y notificaciones a través de un servicio SFTP establecido por CCI o la entidad designada por CCI.
Una vez actualizados cada uno de los ficheros de notificaciones residentes, con cada uno de los registros de dichos ficheros, cuya fecha de inclusión en el fichero coincida con la del proceso, se confeccionará y enviará una carta de notificación al deudor.

Infraestructura
La aplicación es desarrollada en cobol y se ejecuta en un servidor RedHatEnterpriseServer 8.3, la base de datos de la aplicación se encuentra en Oracle 12 con un Sistema Operativo RedHatEnterpriseServer 7.9.
La infraestructura de CTi asociada al servicio RAI se encuentra alojada en el CPD Torrejon Calle Mar Adriatico 2, 28830 San Fernando De Henares, Madrid, España, las instalaciones son administradas por el proveedor de infraestructura Kyndryl, con quien CTi tiene contratados los servicios de alojamiendo, administración de infraestructura, backups, y servicios de seguridad. Kyndryl entrega anualmente los comprobantes de certificación ISO 27001 y resultados de auditoría ISAE 3402, CTi revisa las auditorías y da seguimiento a los resultados.

El equipo de mantenimiento, gestión y desarrollo realiza las labores desde las oficinas corporativas de CTi en Avenida de Europa 19, Alcobendas, Madrid, España y en caso de requerir realizarlas de manera remota se conecta desde

del ordenador corporativo cifrado a través de una conexión VPN de empleados con doble factor de autenticación.

En la actualidad, el fichero RAI no dispone de datos de personas físicas, ni datos protegidos por el reglamento de protección de datos

File Reception
CTi is responsible for receiving the contribution files submitted by users. This exchange is carried out by agreeing with each submitting entity on the delivery configuration through one of the following options:

- *Dedicated line*
- *IPsec Tunnels via a FortiGate 101F device*
- *Editran Proxy*

Once the secure connection is established, the entity initiates a session with Editran to transmit the files using double encryption.

On a weekly basis, reporting entities will send two files to CTi: one containing data to notify non-payments (defaults), and another containing the week's modifications and removals. This process triggers the deletion of the entry in the RAI file or in the notification file (if applicable), thereby preventing its inclusion in the main RAI file.

Alternative Reception
Entities may also send data to the CTi Data Center (CPD) using physical media (CD / DVD: 700MB / 4.7GB). If a different type of physical medium is used, the entity must notify CTi in advance so that processing timeframes for the new format can be estimated.

Before shipping any physical media to CTi, the entity must provide notice by requesting an exceptional file process. This must be done via an email to CTi describing the type and content of the media sent, addressed to: rai@ctisoluciones.com

The media must be shipped to the attention of the primary CTi Project contact at the following address:

Avda. de Europa nº 19, Alcobendas - Madrid 28108

Once CTi receives the media, an acknowledgment of receipt will be sent to the entity via email.

Information Processing
Once all information has been received from the entities, the batch update processes will begin, utilizing the data files sent by the submitting entities throughout the week. CTi processes this information on its internal server using the RAI development application, which handles the following functions:

- *Validation of information*
- *Data loading*
- *File production*
- *Dispatch of error files*
- *Execution of removals communicated by the entities*
- *Removals driven by weekly updates and data expiration*

Generally, all tasks relating to the maintenance of the RAI File in accordance with the Operating Rules defined by the CCI.

Cliente/Servicio – *Client/Service*: **ES0227/S001**
Referencia - *Reference*: **ES022700104606530**
Fecha de validez – *Valid until*: **31/07/2027**

Its ultimate purpose is to update both the individual notification files of each entity and the common RAI file with the data contribution files provided by each entity.

There are 3 types of weekly update processes:

A. *Update processes for the individual notification files of each entity.*
B. *Printing and shipping processes for notification letters via postal mail (Correos).*
C. *Update processes for the common RAI file.*

Upon completion of the weekly update process, CTi sends the RAI and notification files to CCI (or its designee) via an SFTP service established by CCI or its designated entity.

Once each of the resident notification files is updated with its respective records—where the file inclusion date matches the processing date—a notification letter will be prepared and sent to the debtor.

Infrastructure
The application is developed in COBOL and runs on a RedHatEnterpriseServer 8.3 server. The application database resides in Oracle 12 running on a RedHatEnterpriseServer 7.9 Operating System.

The CTi infrastructure associated with the RAI service is hosted at the Torrejón Data Center (CPD), located at:

Calle Mar Adriático 2, 28830 San Fernando De Henares, Madrid, Spain

The facilities are managed by the infrastructure provider Kyndryl, with whom CTi has contracted hosting, infrastructure management, backups, and security services. Kyndryl provides annual proof of ISO 27001 certification and ISAE 3402 audit results; CTi reviews these audits and follows up on the findings.

The maintenance, management, and development team operates from CTi's corporate offices at Avenida de Europa 19, Alcobendas, Madrid, Spain. If remote work is required, they connect using an encrypted corporate computer via an employee VPN featuring dual-factor authentication (2FA).

Currently, the RAI file does not contain personal data of natural persons, nor any data protected by data protection regulations (such as GDPR).

Proceso de calificación

El proceso de calificación consta de cuatro etapas:

- Elaboración de la memoria justificativa por parte del proveedor del servicio o realización de auditoría de tercero independiente conforme a la norma internacional ISAE 3402
- Pre-evaluación documental de la memoria justificativa (o del informe de auditoría) y solicitud, en caso de que sea necesario, de subsanación de errores y/o aclaraciones
- Evaluación *in situ* de una muestra de controles incluidos en la memoria justificativa (solo en caso de que no se haya realizado auditoría previa)
- Elaboración de informe final y emisión del sello con la calificación obtenida

Una vez obtenido el sello, se ponen en funcionamiento los mecanismos de supervisión del esquema:

- Canal de incidencias
- Monitorización en fuentes abiertas

- Auditorías aleatorias

Este nivel de calificación se obtiene sobre la base de las respuestas indicadas por el proveedor de servicios en cuanto a la aplicabilidad y, en su caso, existencia de los controles incluidos en la metodología de calificación en su versión más actual y las evidencias aportadas por el mismo u obtenidas por el equipo de la agencia durante la revisión *in situ* en las instalaciones del proveedor del servicio.

Rating process

Rating and certification process have four steps:

- *Preparation of a memory by the service provider or conducting an audit by an independent third party according to ISAE 3402.*
- *Documentary pre-assessment based on previous memory (or audit report) and require, if needed, correction or errors and/or clarifications.*
- *In situ assessment based on a sample of controls included in the memory.*
- *Preparation of final report and issue of the label and certification with the rating level obtained.*

Once the label has been issued, supervision mechanisms come into place:

- *Incident channel*
- *Cybersecurity online monitoring*
- *Random exhaustive audits*

This report corresponds to the third step of the rating process and it shapes the final assessment of service rating, based on the answers that the service provider has included in the memory about applicability and implementation of controls included in the most recent version of the rating methodology and evidences provided by the provider or obtained by the agency team during the onsite visit in service provider facilities.

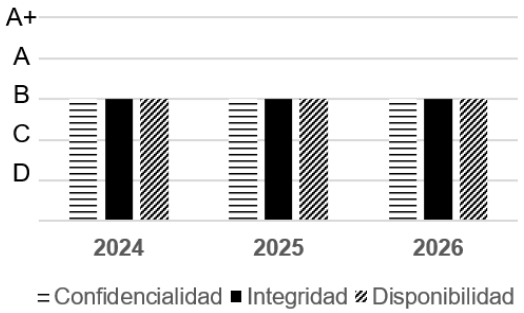
Calificación

El nivel de calificación obtenido por el servicio una vez realizado el proceso de calificación mencionado y su evolución respecto a años anteriores se muestran en los gráficos siguientes:

Rating

The rating level obtained by the service and the comparison with previous years according to the qualification level after the aforementioned rating process has been carried out are the following:

A+ A --**B**-- C D	A+ A --**B**-- C D	A+ A --**B**-- C D
Confidencialidad ***Confidentiality***	**Integridad** ***Integrity***	**Disponibilidad** ***Availability***



Los criterios para asignar la calificación global, según se establece en la versión 3 de la metodología son, implantar:

- El 100% de las medidas generales y para la dimensión correspondiente de prioridad ‘1’.
- Al menos, el 85% de las medidas generales y para la dimensión correspondiente de prioridad ‘2’.
- Al menos, el 50% de las medidas generales y para la dimensión correspondiente de prioridad ‘3’.

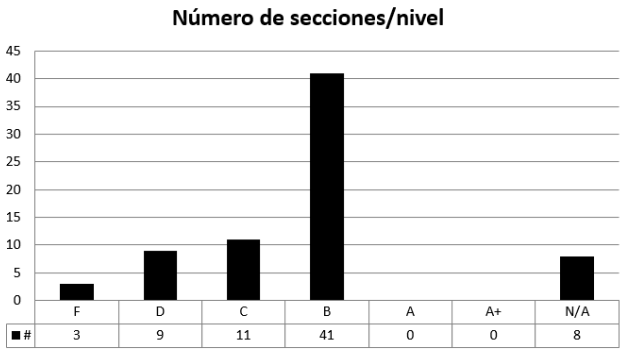
La evaluación de las secciones individuales que se resumen en el gráfico adjunto considera el 100% de los controles (con independencia de su prioridad). La calificación cuantitativa es una suma ponderada (base mil) de los niveles en los que han sido evaluadas las secciones (con más peso de aquellas que más contribuyen a una seguridad más ágil).

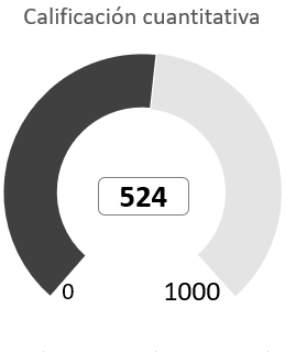
Cliente/Servicio – *Client/Service*: **ES0227/S001**
Referencia - *Reference*: **ES022700104606530**
Fecha de validez – *Valid until*: **31/07/2027**

The criteria for assigning the global rating, as established in version 3 of the methodology are:

- *100% of the general measures and for the corresponding dimension of priority '1'.*
- *At least 85% of the general measures and for the corresponding dimension of priority '2'.*
- *At least 50% of the general measures and for the corresponding dimension of priority '3'.*

The evaluation of individual sections considers 100% of the controls (regardless of their priority) and it is showed in the following diagram. Quantitative rating is a weighted sum (base thousand) of levels achieved by sections (with a higher weight of those with a closer relation to agile security).





Madrid, 02 de junio de 2026/ *2nd of june of 2026*

LEET SECURITY
CyberSecurity
Rating Agency

Firmado digitalmente por LOPEZ CASADO, PATRICIA (FIRMA)

D.Patricia Lopez
Rating Evaluation Team – Operations Direction

Cliente/Servicio – *Client/Service*: **ES0227/S001**
Referencia - *Reference*: **ES022700104606530**
Fecha de validez – *Valid until*: **31/07/2027**

ANEXO I / *ANNEX I*

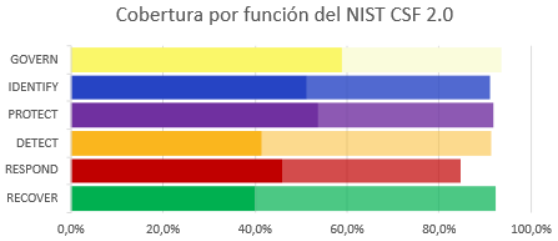
COBERTURA RESPECTO A ESTÁNDARES INTERNACIONALES
INTERNATIONAL STANDARDS COVERAGE

Cobertura respecto a NIST

Este gráfico muestra el porcentaje de implementación de las prácticas aplicables en el servicio, para el nivel objetivo evaluado (barra decolorada) y con respecto al nivel máximo (barra de color intenso), por cada una de las cinco etapas del marco de ciberseguridad del National Institute of Standards and Technology (NIST)[1].

NIST coverage

This chart shows the implementation porcentaje of practices aplicable in the service, for the goal level reviewed (discolored bar) and for the máximum level (intense bar) in each of the five steps of NIST Cybersecuerity Framework.



Cobertura respecto a CIS

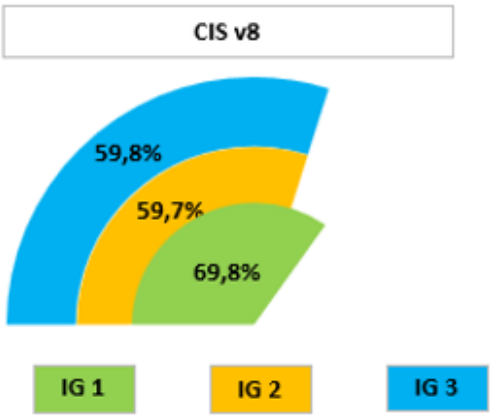
El Center for Internet Security (CIS) recoge y publica las prácticas de defensa frente a los ataques más comunes, conocidas como CIS Controls.

Los 20 controles de su versión 8[2] están divididos en tres grupos: *Basic, Foundational y Organizational*, que a su vez de se clasifican en tres grupos de implementación: IG 1, IG 2 e IG 3, según el nivel de exigencia en seguridad que se marque la propia organización. El siguiente diagrama muestra su grado de implementación en el servicio evaluado.

CIS coverage

Center for Internet Security (CIS) collects and publishes the defense practices for most common attacks, known as CIS Controls.

The 20 controls of versión 8 are divided in three groups: Basic, Foundational and Organizational, that are also classified in three implementaton groups: IG1, IG2 and IG3 in growing order of demand. Following chart shows the implementation grade in the service in scope.



[1] https://www.nist.gov/cyberframework

[2] https://www.cisecurity.org/controls/v8

Cliente/Servicio – *Client/Service*: **ES0227/S001**
Referencia - *Reference*: **ES022700104606530**
Fecha de validez – *Valid until*: **31/07/2027**

INFORMACIÓN ANALÍTICA DE SU EVALUACIÓN
ANALYTIC INFORMATION OF YOUR RATING

Resultado por áreas

Los controles han sido clasificados según los principios de *security economics* lo que permite obtener los gráficos siguientes con el porcentaje de implementados por cada tipo respecto al nivel evaluado como objetivo.

Results by areas

Controls have been classified according to security economics principles which allows getting the attached diagram showing the percentage of practices implemented in relation to those required by your goal level.

Security Economics respecto a Nivel objetivo B