
Guía de Comercios

5.17

01/06/2008

TPV Virtual
Para ventas por Internet.



ÍNDICE DE CONTENIDO

1. Introducción	1
2. Funcionamiento del Cyberpac y garantías de seguridad	1
3. Tipos de peticiones de autorización	4
4. Perfiles de funcionamiento del comercio	9
5. Instrucciones de conexión al Cyberpac	12
6. Plan de pruebas	13
7. Operación de compra: punto de vista del titular	14
8. Identificación de anomalías durante el proceso de compra	15
9. Módulo de administración del Cyberpac SIS	16
9.1 Confirmación de una venta	18
Consultas y administración de operaciones	18
9.2 Consulta de totales	21
9.3 Cambio de contraseña	22
10. Consultas operativas y de funcionamiento	23
11. Envío de transacciones al Cyberpac mediante XML	24
12. Anexos técnicos	25
1. Especificación del documento DATOSENTRADA	39
2. Especificación del documento RETORNOXML	42

1. Introducción

La guía de comercios SIS recoge los aspectos a tener en cuenta por los comercios que deseen utilizar el Cyberpac SIS en la instrumentación de sus compras por Internet.

Este paquete resume el conjunto de funcionalidades que el SIS ofrece a los comercios: perfiles operativos de funcionamiento, tipos de peticiones de autorización, nivel de seguridad de los pagos,...

Asimismo, expone las indicaciones técnicas necesarias para realizar la conexión del servidor del comercio con el Cyberpac, junto con otros servicios añadidos de consulta y envío de transacciones vía XML.

Por último, se detallan las opciones disponibles en la aplicación de administración del SIS, de gran utilidad cara a la gestión de los pedidos del comercio.

2. Funcionamiento del Cyberpac y garantías de seguridad

El Cyberpac es un dispositivo preparado para trabajar en modo totalmente seguro dentro de la operativa de ventas a través de Internet, es decir:

A.- Intentará contactar con el banco emisor de la tarjeta para solicitar la autenticación del titular (verificación de su identidad) antes de solicitar la correspondiente petición de autorización. De esta forma se garantiza que solo **el titular genuino**, dueño de la tarjeta, podrá operar con ella.

B.- Implementa SSL en todas las comunicaciones que impiden la interceptación de la información por terceros. Por tanto, la **confidencialidad está asegurada** en todas las comunicaciones que se establezcan durante la transacción.

C.- También habilita mecanismos para probar la **autenticidad del origen** de las transacciones y que **impiden, asimismo, la manipulación de datos por terceros**. De esta forma se asegura **la integridad** de los datos de la transacción.

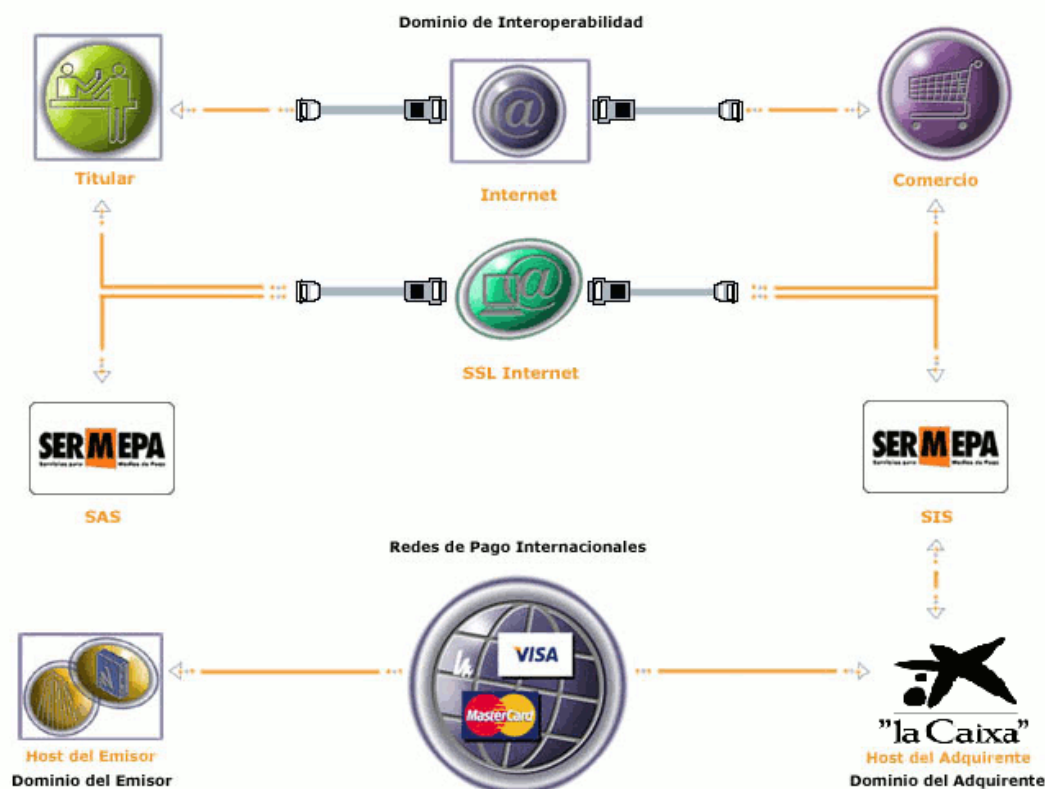
D.- Los datos de **las tarjetas no son normalmente conocidos por el comercio**, con lo que se evita que esta información pueda ser utilizada posteriormente por terceros de forma fraudulenta. (La mejor manera de salvaguardar en el comercio una información sensible de clientes es NO tenerla). Esta información es almacenada convenientemente por el Cyberpac que a su vez la proporcionará al sistema de pagos cuando sea necesario (por ejemplo en una devolución).

Por tanto, todas las transacciones que se realicen a través del Cyberpac contarán con todas las garantías de seguridad, confidencialidad e integridad para los agentes participantes: titulares de tarjetas y sus entidades emisoras, y comercios y sus entidades adquirentes.

El Cyberpac se irá actualizando con las últimas versiones de pago seguro que vayan dictando los organismos internacionales, si bien se asegura que **el comercio NO tendrá que realizar adaptaciones**, ya que éstas se realizarán siempre de forma centralizada.

En todo momento, el comercio recibe puntual información del estado de cada transacción, permaneciendo a su disposición un histórico de 360 días para las consultas de detalle, totales, gestión de devoluciones, etc. que el comercio pudiera necesitar.

De modo gráfico, los pasos típicos que sigue una transacción segura son los siguientes:



1. El comercio contacta con el Cyberpac y le facilita los datos de la transacción: el importe, la moneda, el identificativo y nombre del comercio.
2. El Cyberpac solicita la tarjeta y fecha de caducidad al cliente.
3. El Cyberpac contacta con la entidad financiera que ha emitido dicha tarjeta.
4. La entidad emisora solicita autenticación al cliente. El cliente puede probar su identidad mediante una password, una llamada telefónica, etc. según haya acordado con su entidad emisora.
5. El Cyberpac solicita autorización a la entidad emisora por los circuitos tradicionales de medios de pago.

Puede ocurrir en algún caso que la entidad emisora y el titular de la tarjeta todavía no hayan pactado ningún método de autenticación, por lo que el paso 4 no siempre se realiza, si bien desde el punto de vista del comercio (al estar este conectado al Cyberpac - SIS) la transacción sigue efectuándose bajo la tecnología de compra segura, aunque el cliente no se haya autenticado.

3. Tipos de peticiones de autorización

En función de las necesidades de cada comercio el Cyberpac SIS ofrece una elevada variedad de peticiones de autorización, que el comercio puede combinar según sus necesidades.

Autorización:

Es el caso más general donde la transacción es iniciada por el titular que está presente durante el proceso de la misma. Una vez se ha recibido la petición de compra por parte del comercio, el Cyberpac solicita al cliente los datos para realizar la transacción de autorización.

Si la transacción es segura, se solicitará al titular por parte de su entidad emisora la correspondiente prueba de autenticación.

La solicitud de Autorización se lleva a cabo en tiempo real, produciendo un cargo inmediato en la cuenta del titular asociada a la tarjeta (crédito o débito).

La transacción es capturada automáticamente por el Cyberpac y enviada diariamente en lotes a "la Caixa" para que proceda a su abono al comercio.

El titular de la tarjeta recibe un justificante del pago realizado.

Autorización en diferido

Permiten a los comercios virtuales realizar una gestión del riesgo (en función de los parámetros definidos por el comercio virtual y/o su entidad) de sus operaciones antes de servir el pedido. El comercio tiene 72 horas, una vez realizada la autorización en diferido, para confirmarla (siempre por el mismo importe), o anularla en función del análisis de riesgo efectuado.

La transacción es transparente para el titular que en todo momento actúa exactamente igual que en el caso anterior, es decir, facilita sus datos y se autentica cuando corresponda, recibiendo por parte del Cyberpac el correspondiente justificante.

La transacción no produce efectos contables en la cuenta del titular ni por tanto abono al comercio (algunas entidades emisoras si efectúan apuntes contables al titular sin esperar a la confirmación).

Toda autorización en diferido debe tener una "confirmación" o "anulación" en un período máximo de 72 horas. En caso contrario perderá su validez y el sistema generará una anulación automática de la transacción.

Confirmación de autorización en diferido

Complementa de forma inseparable la operación anterior.

El titular no está presente y por tanto es siempre iniciada por el comercio.

Debe realizarse en las 72 horas siguientes a la autorización en diferido original y su importe debe ser IGUAL que la de la original.

Esta transacción se trata contablemente, regularizando automáticamente el apunte en la cuenta del titular y enviándose a "la Caixa" para su abono al comercio.

El Cyberpac validará la existencia de la operación original y el importe que se desea confirmar, rechazando la operación en caso de existir algún error.

Anulación de autorización en diferido:

El titular no está presente y por tanto es siempre iniciada por el comercio. Debe realizarse en las 72 horas siguientes a la autorización en diferido original.

El Cyberpac validará la existencia de la operación original, rechazando la operación en caso de existir algún error.

Preautorización:

NOTA: esta operativa está restringida a determinados supuestos. Por favor, consulte con "la Caixa" para saber si su comercio la tiene permitida antes de realizar ninguna operación de este tipo.

Puede utilizarse cuando en el momento de la compra no se puede determinar el importe exacto de la misma o por alguna razón el comercio no desea que el importe sea cargado en la cuenta del cliente de forma inmediata.

La transacción es transparente para el titular que en todo momento actúa exactamente igual que en el caso anterior, es decir, facilita sus datos y se autentica cuando corresponda, recibiendo por parte del Cyberpac el correspondiente justificante.

La solicitud de preautorización se lleva a cabo en tiempo real, produciendo una retención por el importe de la venta en la cuenta del titular.

La transacción no se captura y por tanto no produce efectos contables en la cuenta del titular ni por tanto abono al comercio (algunas entidades emisoras SI efectúan apuntes contables al titular que anulan automáticamente pasados unos días).

Toda preautorización debe tener una Confirmación de Preautorización en un período máximo de 7 días. En caso contrario perderá su validez.

Confirmación de Preautorización:

Complementa de forma inseparable la operación anterior.

El titular no está presente y por tanto es siempre iniciada por el comercio.

Debe realizarse en los 7 días siguientes a la preautorización original y su importe debe ser MENOR o IGUAL que la de la original.

Esta transacción se trata contablemente, regularizando automáticamente el apunte en la cuenta del titular y enviándose a "la Caixa" para su abono al comercio.

El Cyberpac validará la existencia de la operación original y el importe que se desea confirmar, rechazando la operación en caso de existir algún error.

Anulación de Preautorización:

El titular no está presente y por tanto es siempre iniciada por el comercio. Debe realizarse en los 7 días siguientes a la preautorización original.

El Cyberpac validará la existencia de la operación original, rechazando la operación en caso de existir algún error.

Devolución Automática:

Son transacciones contables iniciadas por el comercio, que también podrá utilizar el módulo de administración del Cyberpac para realizarlas manualmente.

El Cyberpac comprueba la existencia de la autorización original que se desea devolver, así como que la suma de los importes devueltos no supere en ningún caso el importe autorizado original.

Producen efecto contable en la cuenta del titular (**algunas entidades emisoras pueden demorar unos días el abono al titular**) y, por tanto, son capturadas automáticamente y enviadas a "la Caixa" que procederá a realizar el cargo correspondiente en la cuenta del comercio.

Transacción recurrente:

Permite la suscripción del titular a un servicio ofrecido por el comercio.

El importe total de este servicio será abonado por medio del pago de un determinado número de cuotas.

Mediante esta operación, el comercio informará la cantidad total a pagar, el número mínimo de días a partir del cual se puede hacer el pago de la siguiente cuota y la fecha límite del pago de la última cuota.

El flujo de la operación es similar a la petición de autorización normal, si bien se informa al cliente que está presente, del importe total a pagar y cuotas que lo componen, realizándose la autenticación con estos datos. Por el contrario, la solicitud de autorización, que tendrá carácter contable, se realizará únicamente por el importe de la primera cuota como una solicitud de autorización normal.

Posteriormente, el comercio enviará transacciones sucesivas de autorización al vencimiento de cada cuota.

Transacción Sucesiva:

Complementa de forma inseparable la operación anterior.

El titular no está presente y por tanto es siempre iniciada por el comercio.

Debe realizarse según las condiciones de la transacción recurrente original en cuanto a importe, cuotas y fecha límite. Estos extremos serán validados por el Cyberpac, que rechazará la transacción en caso de encontrar algún error.

Esta transacción se trata contablemente, produciendo un apunte en la cuenta del titular para cada cuota y enviándose a "la Caixa" para su abono al comercio.

Las transacciones sucesivas conservan las mismas condiciones de seguridad respecto a la transacción recurrente original. Para su realización es necesario solicitar una nueva petición de autorización para cada cuota.

Autorizaciones en diferido recurrentes

Útiles en aquellos casos en los que el comercio desea ofrecer la suscripción del titular a un servicio y, adicionalmente, realizar una gestión del riesgo (en función de los parámetros definidos por el comercio virtual y/o su entidad) de sus operaciones antes de servir la mercancía o prestar el servicio.

El funcionamiento de la autorización en diferido recurrente es igual a la transacción recurrente. La única diferencia está en que se genera una autorización en diferido por el importe de la primera cuota.

El comercio tiene 72 horas, una vez realizada la autorización recurrente en diferido, para confirmarla por el importe de la primera cuota, o anularla en función del análisis de riesgo efectuado. Si expirado este plazo no se ha confirmado o anulado la transacción, el sistema la anula de forma automática.

Al vencimiento de cada cuota, el comercio enviará autorizaciones en diferido sucesivas.

Autorizaciones en diferido sucesivas

Complementa de forma inseparable la operación anterior.

El titular no está presente y por tanto es siempre iniciada por el comercio.

Debe realizarse según las condiciones de la autorización en diferido recurrente original en cuanto a importe, cuotas y fecha límite. Estos extremos serán validados por el Cyberpac, que rechazará la transacción en caso de encontrar algún error.

Esta transacción se trata contablemente, produciendo un apunte en la cuenta del titular para cada cuota y enviándose a "la Caixa" para su abono al comercio.

Autenticación:

Este tipo de operación puede ser utilizado por el comercio cuando el importe de la venta no puede ser determinado con exactitud en el momento de producirse la misma.

La operativa es similar a la de preautorizaciones, si bien aunque en este caso solo se lleva a cabo la primera parte de la operación, es decir la autenticación del titular.

Por lo tanto no se produce solicitud de autorización, por lo que la transacción no es contable y no produce retenciones en cuenta al titular.

Posteriormente y dentro de los siguientes 45 días el comercio enviará una confirmación de autenticación que completará la operación original.

Confirmación de autenticación:

Complementa de forma inseparable la operación anterior.

El titular no está presente y por tanto es siempre iniciada por el comercio.

Su importe puede ser diferente al de la operación original (incluso MAYOR), y debe realizarse en los 45 días siguientes a la autenticación original.

Esta transacción se trata contablemente produciendo un apunte en la cuenta del titular y enviándose a "la Caixa" para su abono al comercio.

Las confirmaciones de autenticación conservan las mismas condiciones de seguridad respecto a la autenticación original.

El Cyberpac validará la existencia de la operación rechazando la operación en caso de existir algún error.

A continuación se inserta una tabla donde se resumen las principales características de cada operación:

Tipo de Operación	Iniciada por	¿Contable?	Operación Original Validaciones	Operación Segura
Autorización	Titular	SÍ		Cuando se reúnan condiciones
Preautorización	Titular	NO		Cuando se reúnan condiciones
Confirmación de Preautorización	Comercio	SÍ	Preautorización 7 días Importe < o =	Mismas que la original
Anulación de Preautorización	Comercio	NO	Preautorización 7 días Importe =	
Devolución Automática	Comercio	SÍ	Autorización Suma de importes devueltos < o = 360 días.	
Pago por Referencia	Titular	SÍ		
Recurrente	Titular	SÍ		Cuando se reúnen condiciones
Sucesiva	Comercio	SÍ	Recurrente Importe, cuotas y fecha límite	Mismas que la original
Autenticación	Titular	NO		Cuando se reúnan condiciones
Confirmación de Autenticación	Comercio	SÍ	Autenticación 45 días	Mismas que la original

4. Perfiles de funcionamiento del comercio

El comercio puede personalizar el comportamiento del Cyberpac en función de sus propios criterios. Para ello se han definido una serie de parámetros que pueden ser variados a petición. Únicamente la moneda seleccionada no puede ser modificada una vez que el terminal ha sido dado de alta.

- **Moneda: las opciones disponibles son:**
 - Euros.
 - Dólares
 - Libras:
 - Yenes
- **E-Mail del comercio**, al que se enviará la información pertinente.
- **Notificación ON-LINE:** si el comercio desea recibir en tiempo real una comunicación con los datos de la transacción, por cada una de las peticiones que se gestionan en su TPV, deberá tener en cuenta esta opción. En el ANEXO III se recoge una descripción más amplia de su significado y las posibles opciones.
- **Sincronización:** este parámetro permite cuatro valores: Síncrona/Asíncrona/SíncronaSOAP/SíncronaSOAPconWSDL. Su utilidad está relacionada con la notificación "on-line" descrita en el apartado anterior. El valor Síncrona implica que el resultado de la autorización primero se envía al comercio y a continuación al cliente y con el valor Asíncrona el resultado de la autorización se comunica a la vez al comercio y al cliente. Con el valor SíncronaSOAP la notificación que se envía al comercio es una petición SOAP a un servicio que deberá tener publicado el comercio. Con este tipo de notificación el SIS no da respuesta al titular hasta que recibe la respuesta del comercio. En el caso en el que la respuesta SOAP tenga un valor KO o se produzca un error en el proceso de notificación se dará una respuesta negativa al titular y, en el caso en el que sea necesario, se enviará una anulación de la operación. Este tipo de notificación solo se aplicará a los siguientes tipos de operaciones: Autorización, Preautorización, Transacción Recurrente y Autenticación. Para las demás operaciones la notificación se enviará de forma síncrona. En el ANEXO IX se explica detalladamente este tipo de sincronización. El último tipo de notificación es igual a la SíncronaSOAP, pero en este caso el servidor SOAP que desarrolla el cliente se ajusta a las especificaciones de una WSDL que se adjunta en el ANEXO IX de este documento. Dentro del tipo de sincronizaciones SOAP, se recomienda esta última, que garantiza un entendimiento perfecto entre servidor y cliente.
- **Personalización del Terminal:** las pantallas que se muestran al cliente durante el proceso de pago, pueden ser personalizadas con el logotipo del comercio. Para ello, el comercio deberá acceder al apartado "comercios", opción "consultas" de la aplicación Canales, y dar de alta el logotipo que desee incorporar.
- **URL_OK/URL_CANCEL:** durante el proceso del pago, y una vez que se muestra al cliente la pantalla con el resultado del mismo, es posible redirigir su navegador a una URL para las transacciones autorizadas y a otra si la transacción ha sido denegada. A estas se las denomina URL_OK y URL_CANCEL, respectivamente. Se trata de dos URL que deben ser proporcionadas por el comercio, son opcionales y se ejecutan cuándo el titular pulsa sobre el botón "continuar" o cierra la ventana del recibo de compra.

- **Parámetros en las URL:** si el comercio desea recibir vía GET en las URL_OK y URL_CANCEL, los mismos datos que se envían en la notificación “on-line”, deberá seleccionar esta opción. Por defecto la opción es NO.

- **Idioma:** los idiomas de las páginas HTML que se muestran en el Cyberpac forman parte de la personalización de las mismas. Por ello, el único límite a los idiomas en el Cyberpac lo determinan las páginas HTML que “la Caixa” o el propio comercio habilitan. Actualmente los idiomas disponibles son los siguientes:

- Castellano-001
- Inglés-002
- Catalán-003
- Francés-004
- Alemán-005
- Italiano-007
- Portugués-009

- **Métodos de pago:** esta configuración únicamente puede definirla “la caixa”, que seleccionará aquel o aquellos métodos más adecuados para garantizar una correcta operativa de cada comercio:

Pago seguro: “la Caixa” le habilitará las diferentes opciones que ofrecen los organismos internacionales, VISA y MasterCard principalmente, para garantizar la seguridad de las transacciones, autenticando las operaciones realizadas con tarjeta segura. “la Caixa” solicita a la entidad emisora de la tarjeta la identificación de su titular por los métodos establecidos entre ellos (pin, usuario/password, llamada,...). La entidad emisora identifica a su cliente.

Puede ocurrir en algún caso que la entidad emisora y el titular de la tarjeta todavía no hayan pactado ningún método de autenticación, por lo que la identificación del cliente no siempre se realiza, si bien desde el punto de vista del comercio (al estar este conectado al Cyberpac - SIS) la transacción sigue efectuándose bajo la tecnología de compra segura, aunque el cliente no se haya autenticado (es decir, el titular nunca podrá retroceder la operación por “yo no he sido”).

Al no ser identificado el titular por su entidad financiera, el titular podría solicitar la retrocesión de la operación, que no tendría efectos económicos para el comercio ni “la Caixa”, pero sí como contador de fraude.

Cabría la posibilidad que un comercio tuviera un número muy elevado de peticiones de retrocesiones por parte de los emisores (por ejemplo, por un ataque fraudulento), superando un determinado % sobre la facturación del comercio. En este caso, las marcas (Visa/Master) penalizan al comercio con elevadas multas, además de estar sujeto a las retrocesiones de todas las operaciones de un determinado período

Operativa con titular Seguro: La diferencia con la operativa anterior, es que si la entidad emisora de la tarjeta no identifica a su cliente y deja progresar la transacción, será “la Caixa” quien deniegue la operación.

Con esta opción, el cliente siempre debería identificarse ante su entidad financiera, con lo que se evitaría cualquier petición de retrocesión por parte de los emisores, y por lo tanto, no cabría el peligro de la imposición de multas ni retrocesiones.

Esta opción está especialmente indicada para comercios que tengan mucha operativa con tarjetas extranjeras, y que pertenezcan a determinados sectores como joyería, electrodomésticos, informática, equipos telefónicos, lotería. Para estos casos existe la posibilidad de la activación de titular seguro únicamente para las tarjetas extranjeras.

Puede solicitar esta modalidad vía correo electrónico a comercios@lacaixa.es indicando número de comercio.

Pago segundo intento: Se intenta el pago como seguro y si la entidad emisora de la tarjeta no lo puede identificar y deniega la autenticación, el pago se realiza como no seguro sin autenticación (el comercio es responsable del posible fraude), de forma automática y transparente tanto para el comercio como para el cliente.

Esta operativa debe solicitarse a través de su oficina habitual.

Pago no seguro: Nunca se intenta la autenticación del titular de la tarjeta. En este caso el comercio asume el riesgo de todas las operaciones realizada.

Esta operativa debe solicitarse a través de su oficina habitual.

▪ **Operativa pago fraccionado:**

Esta modalidad únicamente está operativo con tarjetas de “la Caixa”

1) El comercio no envía ningún código de fraccionamiento. Si la tarjeta del titular es una tarjeta de crédito de “la Caixa” y el comercio no tiene códigos de fraccionamiento, se presenta una pantalla para que el titular decida si quiere fraccionar el pago con cargo a la tarjeta, SOLO si el importe de la operación es superior a 40 euros.

2) El comercio envía el código de fraccionamiento en los datos de conexión al SIS. Se ha creado un campo para este fin: `Ds_Merchant_PartialPayment` para que el comercio envíe el código de fraccionamiento. Si el comercio envía este código, y tiene este código de fraccionamiento asociado, se permitirá sólo en el pago con tarjetas de crédito de la Caixa. Para disponer de esta capacidad el comercio debe solicitarlo en su oficina habitual.

3) El comercio no envía ningún código de fraccionamiento. Si la tarjeta del titular es una tarjeta de crédito de la Caixa y el comercio tiene códigos de fraccionamiento asociados con cargo al comercio, se presenta una pantalla para que el titular seleccione una de las opciones de fraccionamiento con cargo al comercio.

Para disponer de esta capacidad el comercio debe solicitarlo en su oficina habitual.

▪ **Multidivisa:**

1) El servicio Multidivisa, permite al titular de la tarjeta, saber en el mismo momento de la compra el importe que finalmente le cargará su entidad por la misma, no dependiendo por tanto de ningún proceso posterior de conversión de divisas.

2) Los comercios no disponen de esta opción por defecto, por lo que deberá solicitar la activación de esta funcionalidad a través de su oficina gestora.

5. Instrucciones de conexión al Cyberpac

Para poder ofrecer el pago con tarjeta a través del Cyberpac deberá realizar unas pequeñas modificaciones en el servidor de su comercio en Internet.

1.-Además de los métodos de pago distintos de tarjeta con los que ya puede estar trabajando, deberá incluir un botón de pago a través del Cyberpac junto al resto de opciones.

2.-En el momento que el cliente pulse el botón de pago, el comercio rellenará un formulario web con los datos de la transacción, cuya descripción técnica detallada figura en el ANEXO I, y lo enviará a la siguiente dirección:

<https://sis-t.sermepa.es:25443/sis/realizarPago> (entorno de pruebas).

<https://sis.sermepa.es/sis/realizarPago> (entorno de real).

La ventana o frame donde se abra el Cyberpac ha de tener barras de desplazamiento para poder adaptarse a las diferentes páginas de autenticación que pudieran mostrarse al titular en los procesos posteriores.

La identificación del comercio y terminal se realizará mediante alta por parte de “la Caixa” en el módulo de administración del Cyberpac y las transacciones serán securizadas de forma individual mediante una firma digital que realizará el comercio, cuyo funcionamiento técnico se explica en el ANEXO II.

3.-A partir de este punto, el Cyberpac gestionará completamente la autorización sin que sea necesaria la intervención del comercio. En todo momento la operativa se ajustará a la personalizada para cada comercio.

6. Plan de pruebas

Una vez el comercio ha realizado la conexión al Cyberpac y visualiza la pantalla de petición de tarjeta, se recomienda la realización de las siguientes pruebas operativas con el fin de poder conocer el funcionamiento del Cyberpac.

Estas pruebas deberán efectuarse en el entorno de pruebas, para lo cual es preciso tener habilitado el acceso a los puertos 25443 y 26443, con el número de tarjeta siguiente:

Tarjeta: 4548812049400004

Fecha de caducidad: 12/08

CIP: 123456

1.- Pruebas de compra: conectándose al Cyberpac, realice una operación de compra con los datos proporcionados. Al final de la operación el Cyberpac le mostrará una pantalla con los datos de la operación y el resultado de la misma.

2.- Prueba de devoluciones: los comercios conectados al SIS podrán realizar devoluciones a través del módulo de administración del SIS tal y como se detalla en el apartado 10.2 de la presente guía. Otra alternativa consiste en enviar el formulario de pago con el tipo de operación `Ds_Merchant_TransactionType=3`. En ambos casos recibirá una confirmación de la devolución efectuada.

3.- Comprobación de las operaciones en el módulo de administración del SIS: accediendo al módulo de administración del SIS en entorno de pruebas, podrá comprobar el detalle de las operaciones efectuadas a través del Cyberpac, tal y como se indica en el apartado 10.2 y 10.3 de la guía. Accediendo al apartado de “Consultas” podrá visualizar el detalle de las operaciones y accediendo al apartado de “Totales” podrá consultar el acumulado de las operaciones.

La descripción de los códigos de respuesta al efectuar una consulta de detalle de las operaciones, figura en la página 19 de la presente guía.

7. Operación de compra: punto de vista del titular

Una vez que el titular tiene los productos en su cesta de la compra, se conecta al Cyberpac para realizar el pago pulsando sobre el botón de pago. La conexión al Cyberpac requiere el acceso desde navegadores con una intensidad de cifrado igual o superior a 128 bits. Las versiones 6.0 y superiores de Iexplorer y, 4.7.x. y superiores de Netscape soportan, por defecto, ese nivel de cifrado.

En función de la configuración de su comercio y según los métodos de pago que "la Caixa" le haya ofrecido, el propio Cyberpac se encargará de solicitar al titular los datos del pago para poder tramitar el mismo con la Entidad Emisora de éste.

Una vez realizado el pago, el titular verá la siguiente pantalla con el resultado de la operación y la última línea indicará el estado de la operación. De la misma manera, dispondrá del número de pedido para cualquier duda o aclaración que se requiera en el futuro.

Ejemplo de operación autorizada:



 **Cyberpac**

Pago a favor de:
LIBRERIA REINA MERCEDES

Comprobante del pago con tarjeta

Datos del pedido

Núm. pedido	Importe total
11196236966	190,00 Euros

Resultado de la operación

El pago ha sido aceptado con los datos siguientes:

Número de la tarjeta: 454881*****
Fecha/hora: 28/11/2007 09:01

Haga clic en "Continuar" para volver a LIBRERIA REINA MERCEDES

8. Identificación de anomalías durante el proceso de compra

El SIS incluye fuertes validaciones y controles para detectar posibles errores en la entrada de datos o situaciones anómalas del sistema.

Ante cualquier entrada al Cyberpac SIS, se realizan las validaciones pertinentes de los datos de entrada. Si los datos de entrada no son correctos, se genera un código de error y no se permite continuar con la operación. Normalmente estas situaciones se producen durante el tiempo que duran las pruebas de integración de un nuevo comercio.

Aunque la integración del comercio sea correcta, siempre se pueden producir situaciones inesperadas como por ejemplo la detección de pedidos repetidos o incluso alguna posible anomalía en el sistema.

Dependiendo del error producido, el mensaje mostrado al titular será diferente. Los posibles códigos de error que pueden darse se muestran en el ANEXO V.

Para localizar el valor se deben seguir los siguientes pasos:

1. Abrir con el bloc de notas (por ejemplo) el código fuente de la página donde se ha producido el error. En la barra de tareas de la página del navegador: Ver → Código fuente.
2. Una vez que tenemos el código fuente abierto buscar el error que se ha producido. En la barra de tareas del bloc de notas: Edición → Buscar.
3. Introducir en la caja de texto 'buscar' el siguiente literal: SIS0.
4. Aparecerá un literal del tipo: <!--SIS0051:-->.
5. De este modo tendremos identificado el error que se ha producido.

9. Módulo de administración del Cyberpac SIS

Accediendo a la dirección de Internet:

<https://sis-t.sermepa.es:25443/canales> (entorno de pruebas)

O

<https://sis.sermepa.es/canales> (entorno real)

podrá realizar las operaciones administrativas y de gestión de las operaciones de su comercio en Internet.

Le aparecerá una página donde tendrá que introducir el usuario y contraseña que previamente le habrá facilitado su entidad adquirente, así como el idioma en que desea realizar la consulta (castellano, catalán o francés).



Usuario

Password

[¿Ha olvidado la contraseña?](#)

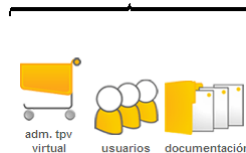
Aceptar

Una vez confirmado que el usuario y la contraseña introducidos son correctos, tendrá acceso a la aplicación administrativa de los TPVs virtuales y de gestión de usuarios.



Administración

Usuario 008043853-002



Si accede a la administración del Cyberpac, se presentará la página siguiente:



- Consultas
- Totales
- Contraseña

Consulta de Detalle

Tipo de Fecha: Operaciones

desde(dd/mm/aaaa): 28 / 11 / 2007

hasta(dd/mm/aaaa): 28 / 11 / 2007

Por nº de pedido: Todos

Estado: Todos

Forma de pago: Todos

Tipo Operación: Todas menos devoluciones, Autorización, Preautorización, Confirmación de preautorización

Descripción:

IP.: . . .

Registros por página: 7

Importe:

Aceptar

9.1 Confirmación de una venta

A través del módulo de administración del Cyberpac, podrá confirmar las operaciones de compra autorizadas independientemente del método de pago con tarjeta utilizado. Este servidor web le permite:

- Consultar el detalle de las operaciones (360 últimas sesiones).
- Devolución de ventas parcial o total (operaciones de los 360 últimos días).
- Consultar los totales de sesión.


Además, de forma opcional, el comercio podrá solicitar la respuesta "on-line" de las operaciones realizadas. Para ello tendrá que facilitar una URL donde recibir estas respuestas en el formulario web que envía al realizar la solicitud de autorización (ver el campo Ds_Merchant_MerchantURL en el ANEXO I).

Esta URL será un CGI, Servlet, etc. desarrollado en el lenguaje que el comercio considere adecuado para integrar en su Servidor (C, Java, Perl, PHP, ASP, etc.), capaz de interpretar la respuesta que le envíe el Cyberpac.

En el ANEXO III se describe técnicamente este proceso en detalle.

Consultas y administración de operaciones

En el apartado de "Consultas" del módulo de administración, deberá introducir una fecha de inicio y fin del período que desea consultar para localizar una operación. Si conoce el número de pedido de la operación puede introducirlo y la búsqueda será más rápida. Una vez haya rellenado los datos anteriores, presione el botón "Aceptar". Le aparecerá la siguiente pantalla donde se muestran las operaciones encontradas con los datos de búsqueda seleccionados. Pueden realizar consultas en las operaciones realizadas en los últimos 365 días. Estos datos pueden ser exportados en un formato MS. Excel. (XLS).

Usuario 008043853-002      




Usuario 008043853-002 Administrador del comercio COMERCIO DE PRUEBAS CAIXA - 008043853

Consultas

Totales

Contraseña

Página 1 de 1

Fecha Hora	Tipo Operación Num. Pedido	Resultado Nº Autorización o Cod. Respuesta	Importe	Tipo Pago	Importe Devoluciones	Consultar Devoluciones	Generar Devolución	País Tarjeta	Crédito/ Débito	IP	Usuario
28-11-2007 09:03:32	Autorización 28110790240	Autorizada 172490	60,30Euros	S				SPAIN	--	195.235.196.10	
28-11-2007 09:10:11	Autorización 28110790919	Autorizada 172496	60,30Euros	S				SPAIN	--	195.235.196.10	
28-11-2007 09:13:42	Autorización 28110791245	Autorizada 172501	60,30Euros	S				SPAIN	--	195.235.196.10	

Tipos de Pago:

S: VISA/MASTER Seguro N: VISA/MASTER No Seguro Y: PAGO POR REFERENCIA
 a: Pago AMEX j: Pago JCB d: Pago DINERS

Los códigos de respuesta que se muestran en campo "Resultado Nº Autorización o código de respuesta" en el módulo de administración del SIS y para operaciones denegadas son los siguientes:

CÓDIGO	SIGNIFICADO
101	Tarjeta caducada
102	Tarjeta en excepción transitoria o bajo sospecha de fraude
106	Intentos de PIN excedidos
125	Tarjeta no efectiva
129	Código de seguridad (CVV2/CVC2) incorrecto
180	Tarjeta ajena al servicio
184	Error en la autenticación del titular
190	Denegación sin especificar Motivo
191	Fecha de caducidad errónea
202	Tarjeta en excepción transitoria o bajo sospecha de fraude con retirada de tarjeta
904	Comercio no registrado en FUC
9912/912	Emisor no disponible
9064	Número de posiciones de la tarjeta incorrecto
9078	No existe método de pago válido para esa tarjeta
9093	Tarjeta no existente
9218	El comercio no permite op. seguras por entrada /operaciones
9253	Tarjeta no cumple el check-digit
9256	El comercio no puede realizar preautorizaciones
9257	Esta tarjeta no permite operativa de preautorizaciones
9261	Operación detenida por superar el control de restricciones en la entrada al SIS
9913	Error en la confirmación que el comercio envía al Cyberpac (solo aplicable en la opción de sincronización SOAP)
9914	Confirmación "KO" del comercio (solo aplicable en la opción de sincronización SOAP)
9928	Anulación de autorización en diferido realizada por el SIS (proceso batch)
9929	Anulación de autorización en diferido realizada por el comercio

Las dos últimas columnas de la pantalla anterior, "Consultar Devoluciones", y "Generar Devoluciones" permiten, respectivamente, consultar las devoluciones realizadas o generar devoluciones de la operación que se muestra.

Para poder consultar o realizar una devolución se pulsará el botón rojo correspondiente. Éste solo estará disponible en operaciones autorizadas y solo se podrán generar devoluciones si la operación original no tiene una devolución por el importe total de la misma.

No a todos los usuarios con acceso a la administración de las operaciones de su comercio en Internet les está permitido el poder realizar devoluciones. Los usuarios y el nivel de acceso a las funciones administrativas serán proporcionadas por "la Caixa" de acuerdo con sus necesidades. Pueden solicitar esta funcionalidad a través de comercios@lacaixa.es.

Si su usuario está autorizado y desea realizar una devolución parcial o total de una de las operaciones seleccionadas, pulse el botón rojo de la columna generar devolución que corresponda a la operación deseada y le aparecerá la página siguiente.

Usuario 008043853-002



Usuario 008043853-002 Administrador del comercio COMERCIO DE PRUEBAS CAIXA - 008043853

Consultas

Totales

Contraseña

Generar Devolución

Fecha Hora	Tipo Operación	Resultado N° Autorización	Num. Pedido	Importe	Importe devuelto	Importe Devolución
28-11-2007 09:03:32	Autorización	Autorizada 172490	28110790240	60,30 Euros		<input type="text"/> Euros

Aceptar

Cancelar

Deberá introducir el importe a devolver (el importe devuelto nunca deberá sobrepasar el de la operación original) y pulsar el botón aceptar.

A continuación le mostrará una página ticket de devolución como la siguiente, pudiéndola imprimir o archivar si lo desea.



Usuario 008043853-002 Administrador del comercio COMERCIO DE PRUEBAS CAIXA - 008043853

Consultas

Totales

Contraseña

Resultado de la devolución

Importe: 0,30 Euros
Comercio: COMERCIO DE PRUEBAS CAIXA
Código Comercio: 8043853
Terminal: 2
Número de Pedido: 28110790240
Fecha: 28-11-2007
Hora: 09:26:43

Devolución aceptada

Imprimir

Aceptar

Aquellos comercios con operativa de preautorizaciones o autorizaciones en diferido, podrán generar confirmaciones y anulaciones de las mismas a partir del módulo de administración del Cyberpac. Asimismo, si el comercio trabaja con la operativa de autenticaciones, podrá emplear el módulo de administración para generar las confirmaciones de autenticación.

9.2 Consulta de totales

Pulsando el botón de “Totales”, que aparece en la parte izquierda de la página, el sistema solicitará la sesión cuyos totales desea consultar. La consulta de totales está disponible:


- Sin desglose (360 últimas sesiones).
- Con desglose marca tarjeta.



Introduciendo el rango de fechas deseado, aparecerá a continuación una nueva pantalla conteniendo información de los importes agregados de las operaciones realizadas en ese período, así como del número de dichas operaciones. Vendrán diferenciadas por cada tipo de operación. Se indica el número de cada una de ellas, separando las autorizadas y denegadas.

9.3 Cambio de contraseña

Con el fin de poder utilizar una contraseña que le sea más fácil de recordar o por motivos de seguridad, podrá cambiar su contraseña periódicamente. Para poder hacer este cambio deberá acudir al apartado “usuarios” y rellenar la nueva “Contraseña” que haya seleccionado.



Usuario 008043853-002 Administrador del comercio COMERCIO DE PRUEBAS CAIXA - 008043853

Consultas

Totales

Contraseña

Cambio de contraseña

Contraseña actual:

Nueva contraseña:

Confirmar contraseña:

Una vez rellenado el formulario, pulse aceptar. El módulo de administración confirmará el cambio realizado.

10. Consultas operativas y de funcionamiento

Si usted tiene alguna consulta referente al Cyberpac, deberá contactar con su oficina.

Las consultas relativas a petición de documentación del Cyberpac, solicitud de datos de alta, definición de los métodos de pago, consulta de datos de configuración del comercio, consultas de usuarios de comercio... deberán ser siempre tramitadas a través de su oficina habitual.

Centro de atención para la conexión de Cyberpac:

En el entorno de pruebas:

E-mail: soportevirtual@sermepa.es

Teléfono: 902 106 223

En el entorno de Producción:

E-mail: virtualcom@sermepa.es

Teléfono: 902 198 747

Con el fin de atenderles de la forma más ágil al trasladar cualquier problema o incidencia con operaciones al centro de atención al cliente les recomendamos que indiquen en el momento de trasladar la consulta:

- Fecha operación.
- Hora.
- Código de comercio.
- Número de pedido.
- URL a la que envía la petición el comercio.
- Descripción incidencia.

De cualquier forma, el centro de atención al cliente no engloba la prestación de servicios de consultoría (consultas acerca del código a desarrollar para conectarse al Cyberpac).

11. Envío de transacciones al Cyberpac mediante XML

Existe la posibilidad de enviar la transacción mediante XML permitiendo automatizar el envío de transacciones por ejemplo un grupo de devoluciones.

Es muy importante tener en cuenta que este recurso es válido solo para cierto tipo de transacciones definidas en el ANEXO VII ya que al no estar presente el titular no podrá autenticarse.

La comunicación se realizará mediante un envío del documento XML a la dirección indicada del SIS. El sistema de SERMEPA interpretará el documento XML y realizará las validaciones pertinentes, para a continuación procesar la operación. Dependiendo del resultado de la operación, se monta un documento XML de respuesta con el resultado de la misma.

El documento XML se transmitirá mediante un envío con POST a las direcciones:

Integración: <https://sis-t.sermepa.es:25443/sis/operaciones>

Real: <https://sis.sermepa.es/sis/operaciones>

El envío se realizará simulando la petición realizada por un formulario con un único input llamado “entrada”. El valor de “entrada” será el documento XML, el cual debe estar en formato x-www-form-urlencoded.

Se definen dos tipos de mensaje en el ANEXO VII:

1. DATOSENTRADA: Mensaje de solicitud enviado.
2. RETORNOXML: Respuesta del SIS a la petición.

12. Anexos técnicos

ANEXO I: Datos del formulario de pago a través del Cyberpac

El formulario de compra a través de Cyberpac deberá contener los datos que se muestran en la tabla, dicho formulario se enviará mediante un POST. El comercio facilitará la información de la compra a la siguiente dirección del servidor web:

<https://sis-t.sermepa.es:25443/sis/realizarPago> (entorno de pruebas).

<https://sis.sermepa.es/sis/realizarPago> (entorno de real).

El cual gestionará la autorización de las operaciones. Los datos imprescindibles para la gestión de la autorización están marcados como obligatorios en la tabla siguiente.

(En los campos *Ds_Merchant_Currency*; *Ds_Merchant_Terminal*; *Ds_Merchant_ConsumerLanguage* la longitud se considera máxima por lo que no es imprescindible el relleno con ceros a la izquierda; la firma ha de ser generada con los campos exactamente como se envíen).

DATO	NOMBRE DEL DATO	Long. / Tipo	COMENTARIOS
Importe	<i>Ds_Merchant_Amount</i>	12 / Núm.	Obligatorio. Para Euros las dos últimas posiciones se consideran decimales.
Moneda	<i>Ds_Merchant_Currency</i>	4 / Núm.	Obligatorio. Valor 978 para Euros, 840 para Dólares y 826 para libras esterlinas. 4 se considera su longitud máxima
Número de Pedido	<i>Ds_Merchant_Order</i>	12 / A-N.	Obligatorio. Los 4 primeros dígitos deben ser numéricos, para los dígitos restantes solo utilizar los siguientes caracteres ASCII Del 30 = 0 al 39 = 9 Del 65 = A al 90 = Z Del 97 = a al 122 = z
Descripción del producto	<i>Ds_Merchant_ProductDescription</i>	125 / A-N	Obligatorio. 125 se considera su longitud máxima. Este campo se mostrará al titular en la pantalla de confirmación de la compra.
Nombre y apellidos del titular	<i>Ds_Merchant_Titular</i>	60 / A-N	Obligatorio. Su longitud máxima es de 60 caracteres. Este campo se mostrará al titular en la pantalla de confirmación de la compra.
Identificación de comercio: código FUC	<i>Ds_Merchant_MerchantCode</i>	9 / N.	Obligatorio. Código FUC asignado al comercio.
URL del comercio para la notificación "on-line"	<i>Ds_Merchant_MerchantURL</i>	250 / A-N.	Obligatorio si el comercio tiene notificación "on-line". URL del comercio que recibirá un post con los datos de la transacción.
URLOK	<i>Ds_Merchant_UriOK</i>	250 / A-N.	Opcional: si se envía será utilizado como URLOK ignorando el configurado en el módulo de administración en caso de tenerlo.
URL KO	<i>Ds_Merchant_UriKO</i>	250 / A-N.	Opcional: si se envía será utilizado como URLKO ignorando el configurado en el módulo de administración en caso de tenerlo
Identificación de comercio: denominación comercial	<i>Ds_Merchant_MerchantName</i>	25 / A-N.	Será el nombre del comercio que aparecerá en el ticket del cliente (opcional).
Idioma del titular	<i>Ds_Merchant_ConsumerLanguage</i>	3 / Núm.	El Valor 0, indicará que no se ha determinado el idioma del cliente (opcional). Otros valores posibles son:

			Castellano-001, Inglés-002, Catalán-003, Francés-004, Alemán-005, Portugués-009. 3 se considera su longitud máxima
Firma del comercio	<i>Ds_Merchant_MerchantSignature</i>	4N	Obligatorio. Ver operativa en ANEXO II.
Número de terminal	<i>Ds_Merchant_Terminal</i>	3 / Núm.	Obligatorio. Número de terminal que le asignará su banco. Por defecto valor "001". 3 se considera su longitud máxima
Importe total	<i>Ds_Merchant_SumTotal</i>	12 / Núm.	Opcional. Representa la suma total de los importes de las cuotas. Las dos últimas posiciones se consideran decimales.
Tipo de transacción	<i>Ds_Merchant_TransactionType</i>	1 / Num	Campo opcional para el comercio para indicar qué tipo de transacción es. Los posibles valores son: 0 – Autorización 1 – Preautorización 2 – Confirmación 3 – Devolución Automática 4 – Pago Referencia 5 – Transacción Recurrente 6 – Transacción Sucesiva 7 – Autenticación 8 – Conf. de Autenticación 9 – Anulación de Preautorización O – Autorización en diferido P – Confirmación de autorización en diferido Q – Anulación de autorización en diferido R – Autorización recurrente inicial diferido S – Autorización recurrente sucesiva diferido
Datos del comercio	<i>Ds_Merchant_MerchantData</i>	1024 / A-N	Campo opcional para el comercio para ser incluidos en los datos enviados por la respuesta "on-line" al comercio si se ha elegido esta opción.
Frecuencia	<i>Ds_Merchant_DateFrequency</i>	5 / N	Frecuencia en días para las transacciones recurrentes y recurrentes diferidas (obligatorio para recurrentes)
Fecha límite	<i>Ds_Merchant_ChargeExpiryDate</i>	10 / A-N	Formato yyyy-MM-dd fecha límite para las transacciones Recurrentes (Obligatorio para recurrentes y recurrentes diferidas)
Código de Autorización	<i>Ds_Merchant_AuthorisationCode</i>	6 / Num	Opcional. Representa el código de autorización necesario para identificar una transacción recurrente sucesiva en las devoluciones de operaciones recurrentes sucesivas. Obligatorio en devoluciones de operaciones recurrentes.
Fecha de la operación recurrente sucesiva	<i>Ds_Merchant_TransactionDate</i>	10 / A-N	Opcional. Formato yyyy-MM-dd. Representa la fecha de la operación recurrente sucesiva, necesaria para identificar la transacción en las devoluciones de operaciones recurrentes sucesivas. Obligatorio para las devoluciones de operaciones recurrentes y de operaciones recurrentes diferidas.

ANEXO II: Firma del comercio

Se dotará al comercio de una clave, que se utilizará para firmar los datos aportados por el mismo, pudiendo verificarse no solo la identificación del comercio, sino que los datos no han sido alterados en ningún momento. Se utilizará como algoritmo de securización el Hash SHA-1, que garantiza los requisitos mínimos de seguridad en cuanto a la autenticación del origen. La clave se proporcionará para ser incluida en la web del comercio.

Este mismo algoritmo se utilizará para asegurar al comercio la autenticidad de los datos de la respuesta, en caso de que se proporcione URL de notificación por parte del comercio.

La firma electrónica del comercio se deberá calcular de la forma siguiente si está configurado con el **tipo de clave SHA1 completo** en el Cyberpac SIS (a través de su entidad financiera podrá confirmar el tipo de clave definido en su comercio):

Digest=SHA-1(Ds_Merchant_Amount + Ds_Merchant_Order +Ds_Merchant_MerchantCode +
DS_Merchant_Currency + CLAVE SECRETA)

En el caso de que la transacción se trate de un **PAGO RECURRENTE INICIAL** la firma se calculará:

Digest=SHA-1(Ds_Merchant_Amount + Ds_Merchant_Order +Ds_Merchant_MerchantCode +
DS_Merchant_Currency + Ds_Merchant_SumTotal + CLAVE SECRETA)

Para aquellos comercios con **tipo de clave SHA1 completo ampliado**, (necesario para poder realizar devoluciones o anulaciones de preautorizaciones), o que deseen incrementar el nivel de seguridad, se deben añadir los campos tipo de operación (Ds_Merchant_TransactionType) y URL de notificación "on-line" (Ds_Merchant_MerchantURL). Si el comercio no tiene URL de notificación "on-line", se deja este campo en blanco. **El tipo de clave SHA1 completo ampliado no está disponible en versiones de php inferiores a la versión 4.3.0.**

Hay dos posibles casos:

- Transacción normal:

La firma electrónica del comercio se deberá calcular de la forma siguiente:

Digest=SHA-1(Ds_Merchant_Amount + Ds_Merchant_Order +Ds_Merchant_MerchantCode +
DS_Merchant_Currency +Ds_Merchant_TransactionType + Ds_Merchant_MerchantURL + CLAVE SECRETA)

- Transacción PAGO RECURRENTE INICIAL:

La firma electrónica del comercio se deberá calcular de la forma siguiente:

Digest=SHA-1(Ds_Merchant_Amount + Ds_Merchant_Order +Ds_Merchant_MerchantCode +
DS_Merchant_Currency + Ds_Merchant_SumTotal + Ds_Merchant_TransactionType +
Ds_Merchant_MerchantURL + CLAVE SECRETA)

NOTA: los campos que entran a formar parte de la firma descrita anteriormente solamente son válidos si la operación se envía por la entrada realizarPago, no por la entrada XML. Para consultar los datos a añadir para dicha entrada, consulte el Anexo VII.

Ejemplo (de firma convencional):

IMPORTE=1235 (va multiplicado por 100 para ser igual que el Ds_Merchant_Amount).

NÚMERO DE PEDIDO=29292929

CÓDIGO COMERCIO=201920191

MONEDA=978

CLAVE SECRETA=h2u282kMks01923kmqpo

Cadena resultado: 123529292929201920191978h2u282kMks01923kmqpo

Resultado SHA-1: c8392b7874e2994c74fa8bea3e2dff38f3913c46

Existen ejemplos de conexión con el TPV en distintos lenguajes de programación.

Donde, “importe” corresponde a Ds_Merchant_Amount del formulario web, “pedido” a Ds_Merchant_Order, “comercio” a Ds_Merchant_MerchantCode, “moneda” a Ds_Merchant_Currency, “Bdclave” a la clave secreta del comercio, que **NUNCA DEBE SER TRANSMITIDA**. Las variables en “C” (importe, moneda,...) son las cadenas mientras que en el formulario web figuran como campos ocultos.

En caso de problemas al acceder al TPV (datos erróneos):

- Una vez que se ha generado la firma no se deben modificar los datos de ningún modo ya que el TPV los utiliza para validar la firma y si lo que recibimos no es exactamente lo que se utilizó para generar la firma no pasa la validación.
- El Importe vendrá multiplicado por 100, sin decimales y sin ceros a la izquierda.
- El número de pedido será diferente cada transacción y las 4 primeras posiciones han de ser numéricas.
- Si aparece en pantalla un mensaje de Datos Erróneos:
- Comprobar que el comercio (FUC/TERMINAL) está dado de alta en el módulo de administración del entorno al que se está enviando la transacción.
- Verificar que la clave que está utilizando para hacer la firma es la que está asignada al comercio en el módulo de administración del Cyberpac.

“la Caixa” podrá suministrarle la información de configuración del comercio (código de comercio, terminal, clave, tipo de clave etc.)

Referencias SHA-1:

- Estándar de Hash Seguro, FIPS PUB 180-1.
<http://www.itl.nist.gov/fipspubs/fip180-1.htm>
<http://csrc.nist.gov/publications/fips/fips180-1/fips180-1.pdf>
- Lista de Implementaciones Validadas del SHA-1
<http://csrc.nist.gov/cryptval/dss/dsaval.htm>
- Las especificaciones del Estándar del Hash Seguro (Algoritmo SHA-1):
<http://csrc.nist.gov/cryptval/shs.html>
- ¿Qué es SHA y SHA-1?
<http://www.rsasecurity.com/rsalabs/faq/3-6-5.html>

ANEXO III: Contestación “on-line” del Cyberpac al comercio

Esta opción esta disponible para aquellos comercios que necesitan una verificación inmediata de la transacción para su gestión. Solo se podrá realizar cuando la sincronización tome valor: Síncrona o Asíncrona. Actualmente, existen 8 formas de realizar la contestación “on-line” al comercio configurables desde el módulo de administración por su entidad financiera:

1. Email comercio.

2. Formulario http. Si falla email comercio: el comercio recibe un POST mediante http al Ds_Merchant_MerchantURL. Si no llega el POST se envía un email al comercio.

3. Formulario http+email comercio: el comercio recibe un POST mediante http al Ds_Merchant_MerchantURL y un email al correo indicado en el módulo de administración.

4. Formulario http: el comercio recibe un POST mediante http al Ds_Merchant_MerchantURL.

5. Email comercio. Si falla email entidad: se envía un email al comercio; si éste no llega se envía un email a la entidad adquirente.

6. Formulario http. Si falla email comercio. Si falla email entidad: el comercio recibe un POST mediante http al Ds_Merchant_MerchantURL. Si no llega el POST se envía un email al comercio; y si éste no llega se envía un email a la entidad adquirente.

7. Formulario http+email comercio. Si falla email entidad: el comercio recibe un POST mediante http al Ds_Merchant_MerchantURL y un email al correo indicado en el módulo de administración; si el email o el HTTP no llega al comercio se envía un email a la entidad adquirente.

8. Sin notificación “on-line”: el comercio no recibe ningún tipo de respuesta “on-line”.

9. Formulario http+ email comercio operaciones autorizadas. Si falla email entidad: el comercio recibe un POST mediante http al Ds_Merchant_MerchantURL, y un email al correo indicado en el módulo de administración en el caso de operaciones autorizadas. Si el email o el http no llegan al comercio se envía un email a la entidad adquirente.

1.- Respuesta http:

Recomendamos el uso de este método, ya que garantiza la respuesta de forma inmediata.

La respuesta http es un proceso independiente de la conexión con el navegador del cliente y **no tiene ningún reflejo en pantalla del mismo.** Evidentemente, en el lado del comercio, deberá haber un proceso que recoja esta respuesta http.

El protocolo utilizado en las respuestas puede ser http o https, el formato de este mensaje es un formulario HTML, enviado con el método POST, y cuyos campos son los siguientes (en los campos Ds_Currency; Ds_Terminal; Ds_ConsumerLanguage la longitud se considera máxima por lo que no es imprescindible el relleno con ceros a la izquierda; la firma será generada con los campos exactamente como se envían):

DATO	NOMBRE DEL DATO	LONG/TIPO	COMENTARIOS
Fecha	<i>Ds_Date</i>	<i>dd/mm/yyyy</i>	Fecha de la transacción
Hora	<i>Ds_Hour</i>	<i>HH:mm</i>	Hora de la transacción
Importe	<i>Ds_Amount</i>	<i>12 / Núm.</i>	Mismo valor que en la petición.
Moneda	<i>Ds_Currency</i>	<i>4 / Núm.</i>	Mismo valor que en la petición. 4 se considera su longitud máxima.
Número de pedido	<i>Ds_Order</i>	<i>12 / A-N.</i>	Mismo valor que en la petición.
Identificación de comercio: código FUC	<i>Ds_MerchantCode</i>	<i>9 / N.</i>	Mismo valor que en la petición.
Terminal	<i>Ds_Terminal</i>	<i>3 / Núm.</i>	Número de terminal que le asignará su banco. 3 se considera su longitud máxima.
Firma para el comercio	<i>Ds_Signature</i>	<i>40 / A-N</i>	Ver a pie de página las instrucciones para su cálculo.
Código de respuesta	<i>Ds_Response</i>	<i>4 / Núm.</i>	Ver tabla siguiente
Datos del comercio	<i>Ds_MerchantData</i>	<i>1024 / A-N</i>	Información opcional enviada por el comercio en el formulario de pago.
Pago Seguro	<i>Ds_SecurePayment</i>	<i>1 / Núm.</i>	0 – Si el pago NO es seguro 1 – Si el pago es seguro
Tipo de operación	<i>Ds_TransactionType</i>	<i>1 / A-N</i>	Tipo de operación que se envió en el formulario de pago
País del titular	<i>Ds_Card_Country</i>	<i>3/Núm</i>	País de emisión de la tarjeta con la que se ha intentado realizar el pago. En el siguiente enlace es posible consultar los códigos de país y su correspondencia: http://unstats.un.org/unsd/methods/m49/m49alpha.htm
Código de autorización	<i>Ds_AuthorisationCode</i>	<i>6/ A-N</i>	Código alfanumérico de autorización asignado a la aprobación de la transacción por la institución autorizadora.
Idioma del titular	<i>Ds_ConsumerLanguage</i>	<i>3 / Núm</i>	El valor 0, indicará que no se ha determinado el idioma del cliente. (opcional). 3 se considera su longitud máxima.
Tipo de Tarjeta	<i>Ds_Card_Type</i>	<i>1 / A-N</i>	Valores posibles: C – Crédito D - Débito

Al igual que el ANEXO II se explica el procedimiento de cálculo de la firma que protege los datos de la transacción que el comercio ha generado, en caso de que éste desee recibir una respuesta “on-line” a las peticiones, el sistema le proporcionará una firma que garantiza a su vez la integridad de las respuestas.

El algoritmo será el mismo y la fórmula a tener en cuenta para el cálculo será:

Digest=SHA-1(Ds_Amount + Ds_Order + Ds_MerchantCode + Ds_Currency + Ds_Response + CLAVE SECRETA)

La conexión utilizada para comunicar la confirmación "on-line" entre el Cyberpac y el comercio puede ser SSL. Opcionalmente el comercio puede activar un filtro para limitar la recepción de la confirmación "on-line" solo desde el Cyberpac para evitar comunicaciones fraudulentas.

El Cyberpac por defecto puede comunicar a los puertos 80, 443, 8080 y 8081 del comercio. Otros puertos deberán ser consultados.

Una vez que el comercio recibe el formulario, el código de respuesta (ds_response) tendrá los siguientes valores posibles:

CÓDIGO	SIGNIFICADO
0000 a 0099	Transacción autorizada para pagos y preautorizaciones
0900	Transacción autorizada para devoluciones y confirmaciones
101	Tarjeta caducada
102	Tarjeta en excepción transitoria o bajo sospecha de fraude
104	Operación no permitida para esa tarjeta o terminal
116	Disponible insuficiente
118	Tarjeta no registrada
129	Código de seguridad (CVV2/CVC2) incorrecto
180	Tarjeta ajena al servicio
184	Error en la autenticación del titular
190	Denegación sin especificar Motivo
191	Fecha de caducidad errónea
202	Tarjeta en excepción transitoria o bajo sospecha de fraude con retirada de tarjeta
912/9912	Emisor no disponible
Cualquier otro valor	Transacción denegada

Nota: solo en el caso de las preautenticaciones (preautorizaciones separadas), se devuelve un 0 si está autorizada y el titular se autentica y, un 1 si está autorizada y el titular no se autentica.

El Cyberpac efectúa el envío de las notificaciones on-line para las operaciones de compra autorizadas y denegadas por la entidad emisora de la tarjeta, así como en aquellas situaciones en las que el proceso de compra ha sido interrumpido al haberse producido uno de los siguientes errores:

SIS0051 -> Pedido repetido. Se envía notificación con código 913.

SIS0078 -> Método de pago no disponible para su tarjeta. Se envía notificación con código 118

SIS0093 -> Tarjeta no válida. Se envía notificación con código 180.

SIS0094 -> Error en la llamada al MPI sin controlar. Se envía notificación con código 184

SIS0218 -> El comercio no permite preautorización por la entrada XML.

SIS0256 -> El comercio no puede realizar preautorizaciones.

SIS0257 -> Esta tarjeta no permite operativa de preautorizaciones.

SIS0261 -> Operación detenida por superar el control de restricciones en la entrada al SIS.

SIS0270 -> El comercio no puede realizar autorizaciones en diferido.

SIS0274 -> Tipo de operación desconocida o no permitida por esta entrada al SIS.

El resto de errores del Cyberpac SIS mencionados en el ANEXO V de la presente guía, no se notifican. Asimismo, tampoco se envía notificación en aquellos casos en los que la operación no termine, por ejemplo por que el usuario no indica la tarjeta o cierra el navegador antes de que finalice la autenticación.

2.- Método e-mail:

El formato de contestación es exactamente igual que en el método anterior.

Cyberpac

<TPVirtual@sermepa.es>

20/08/2007 12:247

Para:

cc:

Asunto: Confirmación On Line del Cyberpac

Fecha: 20/08/2007 Hora: 12:47;

Ds_SecurePayment: 1;

Ds_Card_Type: C;

Ds_Card_Country: 724;

Ds_Amount: 45;

Ds_Currency: 978;

Ds_Order: 070820124150;

Ds_MerchantCode: 999008881;

Ds_Terminal: 001;

Ds_Signature: E2E5A14D690B869183CF3BA36E2B6005BB21F9C5;

Ds_Response: 0000;

Ds_MerchantData: Alfombrilla para raton;

Server URL: sis-i.sermepa.es:25443;

Ds_TransactionType: 0;

Ds_ConsumerLanguage=1;

Ds_AuthorisationCode: 004022

También se podrá solicitar que el TPV al finalizar la transacción y pulsar el titular en el botón cerrar del recibo de compra, vaya a una ruta especificada por el comercio. Ofrecemos la posibilidad de ir a 2 rutas distintas en función de si la transacción es autorizada o no. Estas son las rutas UrlOK y UrlCancel.

Las rutas UrlOK y UrlCancel pueden recibir por GET los mismos datos que se envían mediante la respuesta http.

Si tienen interés en utilizar esta posibilidad deberán comunicar las URL de la opción UrlOK y UrlCancel que se desean dar de alta a través de su entidad financiera o enviarlas en el formulario de pago tal y como indica el ANEXO I.

ANEXO IV: Formato del archivo de transacciones

El módulo de Administración del Cyberpac permite exportar un archivo con la información de las operaciones para que el comercio pueda tratarlo con su aplicación preferida y procesar la información.

Al exportar el archivo desde la aplicación, esta permite cambiarle el nombre en el momento que el cliente selecciona la ruta donde desea guardarlo. El archivo contiene la información mostrada en la tabla de consultas.

Los datos van separados por un;

La separación entre filas se marca con un salto de carro.

La primera fila contiene nombres de campos y las restantes los datos correspondientes a cada fila mostrada en la tabla de consultas.

Por ejemplo:

Tras una consulta que diera como resultado tres operaciones, 2 el día 19 y una el día 20 el archivo descargado sería:

Fecha;Hora;Tipo Operación;Autorización;Pedido;Importe (Ptas);Importe Devolución (Ptas);Importe (Euros);Importe Devolución (Euros);

03/09/2002;00:00:31;Autorización;Denegada ;235838;75;0;0,45;0;

A continuación se describe como se podría importar el archivo descargado en Microsoft Excel 00:

- Se debe abrir el archivo desde MS-Excel 00.
- Al asistente de Excel le tendrá que especificar que el archivo es de tipo "Delimitado" y que comience a importar desde la fila 2 mientras que el formato sea Windows(ANSI).
- A continuación tendrá que especificar como el carácter separador al "punto y coma" en lugar del tabulador que esta seleccionado por defecto.
- A continuación puede pulsar el botón "Terminar" para concluir el proceso o puede seguir para especificar el formato de cada columna.

En MS-Access 00 el mismo proceso consiste en:

- Crear o Abrir una Base de Datos.
- Obtener Datos Externos en el menú de Archivo y especifica el archivo que haya descargado y eligiendo como tipo de archivo TXT.
- Especifique el tipo como Delimitado.
- Especifique como separador al "punto y coma" y elija también "Primera fila contiene nombre de campos".
- A continuación especifique el nombre de la tabla o cree una tabla nueva para almacenar los datos.
- Compruebe el tipo de columna Pedido este especificado como tipo de dato Texto.
- A continuación puede permitir a Access que agregue la clave principal.

- Al menos que quiera personalizar algún otro detalle, los datos quedarán importados en la tabla.

ANEXO V – Tabla de códigos de error del Cyberpac

ERROR	DESCRIPCIÓN	MENSAJE (ANEXO VI)
SIS0007	Error al desmontar el XML de entrada	MSG0008
SIS0008	Error falta Ds_Merchant_MerchantCode	MSG0008
SIS0009	Error de formato en Ds_Merchant_MerchantCode	MSG0008
SIS0010	Error falta Ds_Merchant_Terminal	MSG0008
SIS0011	Error de formato en Ds_Merchant_Terminal	MSG0008
SIS0014	Error de formato en Ds_Merchant_Order	MSG0008
SIS0015	Error falta Ds_Merchant_Currency	MSG0008
SIS0016	Error de formato en Ds_Merchant_Currency	MSG0008
SIS0017	Error no se admiten operaciones en pesetas	MSG0008
SIS0018	Error falta Ds_Merchant_Amount	MSG0008
SIS0019	Error de formato en Ds_Merchant_Amount	MSG0008
SIS0020	Error falta Ds_Merchant_MerchantSignature	MSG0008
SIS0021	Error la Ds_Merchant_MerchantSignature viene vacía	MSG0008
SIS0022	Error de formato en Ds_Merchant_TransactionType	MSG0008
SIS0023	Error Ds_Merchant_TransactionType desconocido	MSG0008
SIS0024	Error Ds_Merchant_ConsumerLanguage tiene mas de 3 posiciones	MSG0008
SIS0025	Error de formato en Ds_Merchant_ConsumerLanguage	MSG0008
SIS0026	Error No existe el comercio / terminal enviado	MSG0008
SIS0027	Error Moneda enviada por el comercio es diferente a la que tiene asignada para ese terminal	MSG0008
SIS0028	Error Comercio / terminal está dado de baja	MSG0008
SIS0030	Error en un pago con tarjeta ha llegado un tipo de operación que no es ni pago ni preautorización	MSG0000
SIS0031	Método de pago no definido	MSG0000
SIS0033	Error en un pago con móvil ha llegado un tipo de operación que no es ni pago ni preautorización	MSG0000
SIS0034	Error de acceso a la Base de Datos	MSG0000
SIS0037	El número de teléfono no es válido	MSG0000
SIS0038	Error en java	MSG0000
SIS0040	Error el comercio / terminal no tiene ningún método de pago asignado	MSG0008
SIS0041	Error en el cálculo de la HASH de datos del comercio.	MSG0008
SIS0042	La firma enviada no es correcta	MSG0008
SIS0043	Error al realizar la notificación on-line	MSG0008
SIS0046	El bin de la tarjeta no está dado de alta	MSG0002
SIS0051	Error número de pedido repetido	MSG0001
SIS0054	Error no existe operación sobre la que realizar la devolución	MSG0008
SIS0055	Error existe más de un pago con el mismo número de pedido	MSG0008
SIS0056	La operación sobre la que se desea devolver no está autorizada	MSG0008
SIS0057	El importe a devolver supera el permitido	MSG0008
SIS0058	Inconsistencia de datos, en la validación de una confirmación	MSG0008
SIS0059	Error no existe operación sobre la que realizar la confirmación	MSG0008
SIS0060	Ya existe una confirmación asociada a la preautorización	MSG0008
SIS0061	La preautorización sobre la que se desea confirmar no está autorizada	MSG0008
SIS0062	El importe a confirmar supera el permitido	MSG0008
SIS0063	Error. Número de tarjeta no disponible	MSG0008
SIS0064	Error. El número de tarjeta no puede tener más de 19 posiciones	MSG0008
SIS0065	Error. El número de tarjeta no es numérico	MSG0008
SIS0066	Error. Mes de caducidad no disponible	MSG0008
SIS0067	Error. El mes de la caducidad no es numérico	MSG0008

ERROR	DESCRIPCIÓN	MENSAJE (ANEXO VI)
SIS0068	Error. El mes de la caducidad no es válido	MSG0008
SIS0069	Error. Año de caducidad no disponible	MSG0008
SIS0070	Error. El Año de la caducidad no es numérico	MSG0008
SIS0071	Tarjeta caducada	MSG0000
SIS0072	Operación no anulable	MSG0000
SIS0074	Error falta Ds_Merchant_Order	MSG0008
SIS0075	Error el Ds_Merchant_Order tiene menos de 4 posiciones o más de 12	MSG0008
SIS0076	Error el Ds_Merchant_Order no tiene las cuatro primeras posiciones numéricas	MSG0008
SIS0077	Error el Ds_Merchant_Order no tiene las cuatro primeras posiciones numéricas. No se utiliza	MSG0000
SIS0078	Método de pago no disponible	MSG0005
SIS0079	Error al realizar el pago con tarjeta	MSG0000
SIS0081	La sesión es nueva, se han perdido los datos almacenados	MSG0007
SIS0084	El valor de Ds_Merchant_Conciliation es nulo	MSG0008
SIS0085	El valor de Ds_Merchant_Conciliation no es numérico	MSG0008
SIS0086	El valor de Ds_Merchant_Conciliation no ocupa 6 posiciones	MSG0008
SIS0089	El valor de Ds_Merchant_ExpiryDate no ocupa 4 posiciones	MSG0008
SIS0092	El valor de Ds_Merchant_ExpiryDate es nulo	MSG0008
SIS0093	Tarjeta no encontrada en la tabla de rangos	MSG0006
SIS0094	La tarjeta no fue autenticada como 3D Secure	MSG0004
SIS0097	Valor del campo Ds_Merchant_CComercio no válido	MSG0008
SIS0098	Valor del campo Ds_Merchant_CVentana no válido	MSG0008
SIS0112	Error El tipo de transacción especificado en Ds_Merchant_Transaction_Type no esta permitido	MSG0008
SIS0113	Excepción producida en el servlet de operaciones	MSG0008
SIS0114	Error, se ha llamado con un GET en lugar de un POST	MSG0000
SIS0115	Error no existe operación sobre la que realizar el pago de la cuota	MSG0008
SIS0116	La operación sobre la que se desea pagar una cuota no es una operación válida	MSG0008
SIS0117	La operación sobre la que se desea pagar una cuota no está autorizada	MSG0008
SIS0118	Se ha excedido el importe total de las cuotas	MSG0008
SIS0119	Valor del campo Ds_Merchant_DateFrequency no válido	MSG0008
SIS0120	Valor del campo Ds_Merchant_ChargeExpiryDate no válido	MSG0008
SIS0121	Valor del campo Ds_Merchant_SumTotal no válido	MSG0008
SIS0122	Valor del campo Ds_Merchant_DateFrequency o no Ds_Merchant_SumTotal tiene formato incorrecto	MSG0008
SIS0123	Se ha excedido la fecha tope para realizar transacciones	MSG0008
SIS0124	No ha transcurrido la frecuencia mínima en un pago recurrente sucesivo	MSG0008
SIS0132	La fecha de Confirmación de Autorización no puede superar en mas de 7 días a la de Preautorización.	MSG0008
SIS0133	La fecha de Confirmación de Autenticación no puede superar en mas de 45 días a la de Autenticación Previa.	MSG0008
SIS0139	Error el pago recurrente inicial está duplicado	MSG0008
SIS0142	Tiempo excedido para el pago	MSG0000
SIS0197	Error al obtener los datos de cesta de la compra en operación tipo pasarela	MSG0000
SIS0198	Error el importe supera el límite permitido para el comercio	MSG0000
SIS0199	Error el número de operaciones supera el límite permitido para el comercio	MSG0008
SIS0200	Error el importe acumulado supera el límite permitido para el comercio	MSG0008
SIS0214	El comercio no admite devoluciones	MSG0008
SIS0216	Error Ds_Merchant_CVV2 tiene mas de 3 posiciones	MSG0008
SIS0217	Error de formato en Ds_Merchant_CVV2	MSG0008
SIS0218	El comercio no permite operaciones seguras por la entrada /operaciones	MSG0008
SIS0219	Error el número de operaciones de la tarjeta supera el límite	MSG0008

ERROR	DESCRIPCIÓN	MENSAJE (ANEXO VI)
	permitido para el comercio	
SIS0220	Error el importe acumulado de la tarjeta supera el límite permitido para el comercio	MSG0008
SIS0221	Error el CVV2 es obligatorio	MSG0008
SIS0222	Ya existe una anulación asociada a la preautorización	MSG0008
SIS0223	La preautorización que se desea anular no está autorizada	MSG0008
SIS0224	El comercio no permite anulaciones por no tener firma ampliada	MSG0008
SIS0225	Error no existe operación sobre la que realizar la anulación	MSG0008
SIS0226	Inconsistencia de datos, en la validación de una anulación	MSG0008
SIS0227	Valor del campo Ds_Merchant_TransactionDate no válido	MSG0008
SIS0229	No existe el código de pago aplazado solicitado	MSG0008
SIS0252	El comercio no permite el envío de tarjeta	MSG0008
SIS0253	La tarjeta no cumple el check-digit	MSG0006
SIS0254	El número de operaciones de la IP supera el límite permitido por el comercio	MSG0008
SIS0255	El importe acumulado por la IP supera el límite permitido por el comercio	MSG0008
SIS0256	El comercio no puede realizar preautorizaciones	MSG0008
SIS0257	Esta tarjeta no permite operativa de preautorizaciones	MSG0008
SIS0258	Inconsistencia de datos, en la validación de una confirmación	MSG0008
SIS0261	Operación detenida por superar el control de restricciones en la entrada al SIS	MSG0008
SIS0270	El comercio no puede realizar autorizaciones en diferido	MSG0008
SIS0274	Tipo de operación desconocida o no permitida por esta entrada al SIS	MSG0008

ANEXO VI – Tabla de mensajes de error del Cyberpac

En la siguiente tabla se muestran los mensajes que se muestran al titular ante los diferentes errores. Solo se incluyen los textos en castellano, se debe tener en cuenta que estarán traducidos al idioma utilizado por el titular.

CÓDIGO	MENSAJE
MSG0000	El sistema está ocupado, inténtelo más tarde
MSG0001	Número de pedido repetido
MSG0002	El BIN de la tarjeta no está dado de alta en FINANET
MSG0003	El sistema está arrancando, inténtelo en unos momentos
MSG0004	Error de Autenticación.
MSG0005	No existe método de pago válido para su tarjeta.
MSG0006	Tarjeta ajena al servicio.
MSG0007	Faltan datos. Por favor, compruebe que su "navegador" acepta cookies.
MSG0008	Error en datos enviados. Contacte con su comercio.

ANEXO VII – Mensajes XML

1. Especificación del documento DATOSENTRADA.

Este mensaje se envía para solicitar una operación al SIS:

Versión 1.0 :

<!ELEMENT DATOSENTRADA

(DS_Version,
DS_MERCHANT_AMOUNT,
DS_MERCHANT_CURRENCY,
DS_MERCHANT_ORDER,
DS_MERCHANT_MERCHANTCODE,
DS_MERCHANT_MERCHANTURL,
DS_MERCHANT_MERCHANTNAME ?,
DS_MERCHANT_CONSUMERLANGUAGE ?,
DS_MERCHANT_MERCHANTSIGNATURE,
DS_MERCHANT_TERMINAL,
DS_MERCHANT_TRANSACTIONTYPE,
DS_MERCHANT_MERCHANTDATA ?,
DS_MERCHANT_PAN?,
DS_MERCHANT_EXPIRYDATE ?,
DS_MERCHANT_CVV2 ?)>

<!ELEMENT DS_Version (#PCDATA)>

<!ELEMENT DS_MERCHANT_AMOUNT (#PCDATA)>

<!ELEMENT DS_MERCHANT_CURRENCY (#PCDATA)>

<!ELEMENT DS_MERCHANT_ORDER (#PCDATA)>

<!ELEMENT DS_MERCHANT_MERCHANTCODE (#PCDATA)>

<!ELEMENT DS_MERCHANT_MERCHANTURL (#PCDATA)>

<!ELEMENT DS_MERCHANT_MERCHANTNAME (#PCDATA)>

<!ELEMENT DS_MERCHANT_CONSUMERLANGUAGE (#PCDATA)>

<!ELEMENT DS_MERCHANT_MERCHANTSIGNATURE (#PCDATA)>

<!ELEMENT DS_MERCHANT_TERMINAL (#PCDATA)>

<!ELEMENT DS_MERCHANT_TRANSACTIONTYPE (#PCDATA)>

<!ELEMENT DS_MERCHANT_MERCHANTDATA (#PCDATA)>

<!ELEMENT DS_MERCHANT_PAN (#PCDATA)>

<!ELEMENT DS_MERCHANT_EXPIRYDATE (#PCDATA)>

<!ELEMENT DS_MERCHANT_CVV2 (#PCDATA)>

Donde:

- DS_Version: Versión de la DTD utilizada para validar el mensaje XML
- DS_MERCHANT_AMOUNT: ver ANEXO I.
- DS_MERCHANT_CURRENCY: ver ANEXO I.
- DS_MERCHANT_ORDER: ver ANEXO I.
- DS_MERCHANT_MERCHANTCODE: ver ANEXO I.
- DS_MERCHANT_MERCHANTURL: ver ANEXO I.
- DS_MERCHANT_MERCHANTNAME: ver ANEXO I.
- DS_MERCHANT_CONSUMERLANGUAGE : ver ANEXO I.
- DS_MERCHANT_MERCHANTSIGNATURE:
SHA1 de los campos Ds_Merchant_Amount + Ds_Merchant_Order +Ds_Merchant_MerchantCode +
Ds_Merchant_Currency + DS_MERCHANT_PAN+
DS_MERCHANT_CVV2 +DS_MERCHANT_TRANSACTIONTYPE + CLAVE SECRETA.
DS_MERCHANT_PAN solo se incluirá si se envía en el mensaje.
DS_MERCHANT_CVV2 solo se incluirá si se envía en el mensaje.

- DS_MERCHANT_TERMINAL: ver ANEXO I.
- DS_MERCHANT_TRANSACTIONTYPE: solo se permiten los tipos:
 - 2- Confirmación
 - 3- Devolución Automática
 - 6- Transacción Sucesiva
 - 8- Confirmación de Autenticación
 - 9- Anulaciones de preautorizaciones
 - 1-Preautorización (válido solo si el comercio trabaja únicamente en modo no seguro)
 - O – Autorización en diferido
 - P - Confirmación de autorización en diferido
 - Q - Anulación de autorización en diferido
 - R – Autorización recurrente inicial diferido
 - S – Autorización recurrente sucesiva diferido
- DS_MERCHANT_MERCHANTDATA: ver ANEXO I.
- DS_MERCHANT_PAN: número de tarjeta.
- DS_MERCHANT_EXPIRYDATE: fecha caducidad (AAMM).
- DS_MERCHANT_AUTHORISATIONCODE: solo válido para devoluciones de transacciones recurrentes sucesivas. Ver ANEXO I.
- DS_MERCHANT_TRANSACTIONDATE: solo válido para devoluciones de transacciones recurrentes sucesivas. Ver ANEXO I.
- DS_MERCHANT_CVV2: Código CVV2/CVC2 de la tarjeta (Dato opcional). En caso de que se incluya, se debe añadir a la firma, de la siguiente manera:

firma = SHA1(datos + clave_entidad)

Donde 'datos' es una cadena formada por:

datos=importe + pedido + comercio + moneda

- Si es una autorización o preautorización: datos = datos + tarjeta

- Si además de ser pago tradicional, se envía CVV2:

datos = datos + CVV2

Por último, siempre se le añade el tipo de operación:

datos = datos + tipo_operación

A continuación se muestra un ejemplo del mensaje:

```
<DATOSENTRADA>
  <DS_Version>
    0.1
  </DS_Version>
  <DS_MERCHANT_CURRENCY>
    978
  </DS_MERCHANT_CURRENCY>
  <DS_MERCHANT_MERCHANTURL>
    https://pruebaCom.jsp
  </DS_MERCHANT_MERCHANTURL>
  <DS_MERCHANT_TRANSACTIONTYPE>
    2
  </DS_MERCHANT_TRANSACTIONTYPE>
  <DS_MERCHANT_MERCHANTDATA>
    Alfombrilla+para+raton
  </DS_MERCHANT_MERCHANTDATA>
```

```
<DS_MERCHANT_AMOUNT>
    45
</DS_MERCHANT_AMOUNT>
<DS_MERCHANT_MERCHANTNAME>
    Comercio de Pruebas
</DS_MERCHANT_MERCHANTNAME>
<DS_MERCHANT_MERCHANTSIGNATURE>
    a63dfa507e549936f41f4961ccdace126b8ecdea
</DS_MERCHANT_MERCHANTSIGNATURE>
<DS_MERCHANT_TERMINAL>
    1
</DS_MERCHANT_TERMINAL>
<DS_MERCHANT_MERCHANTCODE>
    999008881
</DS_MERCHANT_MERCHANTCODE>
<DS_MERCHANT_ORDER>
    114532
</DS_MERCHANT_ORDER>
</DATOSENTRADA>
```

2. Especificación del documento RETORNOXML.

Este mensaje es el que SERMEPA enviará como resultado de la operación en el SIS: Versión 0.0

```
<!ELEMENT RETORNOXML (DS_Version ?,CODIGO,(OPERACION|RECIBIDO ))>
    <!ELEMENT DS_Version (#PCDATA)>
    <!ELEMENT CODIGO (#PCDATA)>
    <!ELEMENT OPERACION (Ds_Amount, Ds_Currency, Ds_Order, Ds_Signature, Ds_MerchantCode, Ds_Terminal,
Ds_Response, Ds_AuthorisationCode,Ds_TransactionType, Ds_SecurePayment, Ds_Reference ?, Ds_Language ?,
Ds_CardNumber ?, Ds_ExpiryDate ?, Ds_MerchantData ?, Ds_MerchantDTD)>
    <!ELEMENT Ds_Amount (#PCDATA)>
    <!ELEMENT Ds_Currency (#PCDATA)>
    <!ELEMENT Ds_Order (#PCDATA)>
    <!ELEMENT Ds_Signature (#PCDATA)>
    <!ELEMENT Ds_MerchantCode (#PCDATA)>
    <!ELEMENT Ds_Terminal (#PCDATA)>
    <!ELEMENT Ds_Response (#PCDATA)>
    <!ELEMENT Ds_AuthorisationCode (#PCDATA)>
    <!ELEMENT Ds_TransactionType (#PCDATA)>
    <!ELEMENT Ds_SecurePayment (#PCDATA)>
    <!ELEMENT Ds_Reference (#PCDATA)>
    <!ELEMENT Ds_Language (#PCDATA)>
    <!ELEMENT Ds_CardNumber (#PCDATA)>
    <!ELEMENT Ds_ExpiryDate (#PCDATA)>
    <!ELEMENT Ds_MerchantData (#PCDATA)>
    <!ELEMENT RECIBIDO (#PCDATA)>
```

Donde:

- DS_Version: versión de la DTD utilizada para validar el XML.
- CÓDIGO: indica si la operación ha sido correcta o no (no indica si ha sido autorizada, solo si se ha procesado). Un 0 indica que la operación ha sido correcta. En el caso de que sea distinto de 0, tendrá el código del error y no aparecerá la información de la operación.
CÓDIGO no es Ds_Response una operación puede tener un CÓDIGO = 0 y ser Denegada (Ds_Response distinto de 0).
- Ds_Amount: importe de la operación.
- Ds_Currency: moneda de la operación.
- Ds_Order: pedido de la operación.
- Ds_Signature: firma de la operación, se calcula con los campos.
Ds_Amount + Ds_Order + Ds_MerchantCode + Ds_Currency + Ds_Response + Ds_CardNumber + Ds_TransactionType + Ds_SecurePayment + Clave.
- El campo Ds_CardNumber solo formará parte de la firma en caso de que se envíe la tarjeta. Si la tarjeta se envía asteriscada, el campo Ds_CardNumber también formará parte de la firma con el valor asteriscado.
- Ds_MerchantCode: código de comercio de la operación.
- Ds_Terminal: número de terminal de la operación.
- Ds_Response: valor que indica el resultado de la operación. Indicará si ha sido autorizada o no. Sus valores posibles son los de PRICE.
- Ds_AuthorisationCode: código de autorización en caso de existir.
- Ds_TransactionType: tipo de operación realizada.
- Ds_MerchantData: ver ANEXO I.
- Ds_SecurePayment: ver ANEXO III.
- Ds_Reference: campo opcional para pago por referencia.
- Ds_Language: indica idioma enviado por el comercio.
- Ds_CardNumber: número de tarjeta de crédito (solo se envía si la entidad así lo ha definido).
- Ds_ExpiryDate: año y mes de caducidad de la tarjeta AAMM (solo se envía si la entidad así lo ha definido).
- Ds_CardType: indica si la tarjeta con la que se ha efectuado la operación es de crédito o débito.
- RECIBIDO: es una cadena de texto que contiene el XML que el comercio nos envió mediante POST en el campo entrada.

El campo DS_Version solo aparecerá en caso de que la operación haya sido correcta ya que es un valor que nos envía el comercio en caso de no ser correcta el dato irá en el campo RECIBIDO.

El hecho de que enviemos el dato OPERACION o RECIBIDO depende también de que la operación sea correcta o no.

A continuación se muestran 3 ejemplos del mensaje:

1- Operación correcta y Autorizada:

```
<RETORNOXML>
  <DS_Version>1.0</DS_Version>
  <CODIGO>0</CODIGO>
  <OPERACION>
    <Ds_Amount>100</DS_Amount>
    <Ds_Currency>978</DS_Currency>
    <Ds_Order>0001</DS_Order>
    <Ds_Signature>EEFF45687hgth</DS_Signature>
    <Ds_MerchantCode>999008881</DS_MerchantCode>
    <Ds_Terminal>1</DS_Terminal>
    <Ds_Response>0</DS_Response>
    <Ds_AuthorisationCode>222FFF</Ds_AuthorisationCode>
    <Ds_TransactionType>2</Ds_TransactionType>
    <Ds_SecurePayment>1</Ds_SecurePayment>
    <Ds_MerchantData>Mis Datos</Ds_MerchantData>
  </OPERACION>
</RETORNOXML>
```

2 - Operación correcta y denegada (190 Denegada por la entidad):

```
<RETORNOXML>
  <DS_Version>1.0</DS_Version>
  <CODIGO>0</CODIGO>
  <OPERACION>
    <Ds_Amount>100</DS_Amount>
    <Ds_Currency>978</DS_Currency>
    <Ds_Order>0001</DS_Order>
    <Ds_Signature>EEFF45687hgth</DS_Signature>
    <Ds_MerchantCode>999008881</DS_MerchantCode>
    <Ds_Terminal>1</DS_Terminal>
    <Ds_Response>190</DS_Response>
    <Ds_AuthorisationCode>222FFF</Ds_AuthorisationCode>
    <Ds_TransactionType>2</Ds_TransactionType>
    <Ds_SecurePayment>1</Ds_SecurePayment>
    <Ds_MerchantData>Mis Datos</Ds_MerchantData>
  </OPERACION>
</RETORNOXML>
```

3 - Operación incorrecta (051 N° de Pedido Repetido). Nunca será autorizada:

```
<RETORNOXML>
  <CODIGO>SIS0051</CODIGO>
  <RECIBIDO>
<DATOSENTRADA>
  <DS_MERCHANT_CURRENCY>
    978
  </DS_MERCHANT_CURRENCY>
  <DS_MERCHANT_MERCHANTURL>
    https://pruebaCom.jsp
  </DS_MERCHANT_MERCHANTURL>
  <DS_MERCHANT_TRANSACTIONTYPE>
    2
  </DS_MERCHANT_TRANSACTIONTYPE>
  <DS_MERCHANT_MERCHANTDATA>
    Alfombrilla+para+raton
  </DS_MERCHANT_MERCHANTDATA>
  <DS_MERCHANT_AMOUNT>
    45
  </DS_MERCHANT_AMOUNT>
  <DS_MERCHANT_MERCHANTNAME>
    Comercio de Pruebas
  </DS_MERCHANT_MERCHANTNAME>
  <DS_MERCHANT_MERCHANTSIGNATURE>
    a63dfa507e549936f41f4961ccdace126b8ecdea
  </DS_MERCHANT_MERCHANTSIGNATURE>
  <DS_MERCHANT_TERMINAL>
    1
  </DS_MERCHANT_TERMINAL>
  <DS_MERCHANT_MERCHANTCODE>
    999008881
  </DS_MERCHANT_MERCHANTCODE>
  <DS_MERCHANT_ORDER>
    114532
  </DS_MERCHANT_ORDER>
  <DS_Version>
    1.0
  </ DS_Version >
</DATOSENTRADA>
</RECIBIDO>
</RETORNOXML>
```

ANEXO VIII – Sincronización SOAP

Este nuevo método de sincronización permite al comercio recibir una notificación de la transacción en un servicio SOAP. Si el comercio no tiene privilegios para activar este permiso con su usuario, deberá solicitar la activación a través de su entidad. Esta sincronización es una notificación en sí, por lo que no tiene sentido rellenar el campo de notificación online, ya que no se tomará en cuenta.

Si la opción SincronizaciónSOAP está habilitada para un comercio significará que el SIS enviará las notificaciones para operaciones de Autorización, Preautorización, Autorización en diferido, Transacción Recurrente y Autenticación como peticiones SOAP a un servicio que tendrá publicado el comercio. Para el resto de operaciones las notificaciones se realizarán de forma sincrónica y según la opción elegida en la configuración del comercio para las notificaciones on-line.

La principal particularidad de esta notificación es que el SIS espera una respuesta a la notificación antes de presentar el resultado de la operación al titular que está realizando la compra. En el caso en el que el comercio devuelva una respuesta con valor KO o se produzca un error durante el proceso de notificación, el SIS anulará la operación y presentará al titular un recibo con el resultado KO, es decir, el SIS supedita el resultado de la operación a la respuesta que obtenga del comercio en la notificación.

La URL del rpcrouter al que se conectará el SIS y donde estará publicado el servicio SOAP, deberá enviarla el comercio en el parámetro 'Ds_Merchant_MerchantURL' del formulario de entrada al SIS. Este campo es el que actualmente se está utilizando para la notificación http.

El servicio SOAP que deben publicar los comercios debe tener las siguientes características:

- El servicio deberá llamarse 'InotificacionSIS' y ofrecer un método llamado 'procesaNotificacionSIS'. Este método estará definido con un parámetro de entrada tipo cadena XML y otro parámetro de salida del mismo tipo. Para más información, se adjunta un fichero WSDL a partir del cual se puede construir el esqueleto del servidor y que servirá para definir los tipos de datos que se intercambiarán entre cliente y servidor, de cara a facilitar la comunicación.
- El formato de los mensajes que se intercambiarán en este servicio deberán ajustarse a la siguiente dtd:
- Mensaje de notificación enviado desde el SIS con los datos de la operación correspondiente:

```

<!ELEMENT Message (Request, Signature)>
<!ELEMENT Request (Fecha, Hora, Ds_SecurePayment, Ds_Amount, Ds_Currency, Ds_Order,
Ds_MerchantCode, Ds_Terminal, Ds_Response, Ds_MerchantData?, Ds_Card_Type?,
Ds_TransactionType, Ds_ConsumerLanguage, Ds_ErrorCode?, Ds_CardCountry?,
Ds_AuthorisationCode?)>
<!ATTLIST Request Ds_Version CDATA #REQUIRED>
<!ELEMENT Fecha (#PCDATA)>
<!ELEMENT Hora (#PCDATA)>
<!ELEMENT Ds_SecurePayment (#PCDATA)>
<!ELEMENT Ds_Amount (#PCDATA)>
<!ELEMENT Ds_Currency (#PCDATA)>
<!ELEMENT Ds_Order (#PCDATA)>
<!ELEMENT Ds_MerchantCode (#PCDATA)>
<!ELEMENT Ds_Terminal (#PCDATA)>
<!ELEMENT Ds_Response (#PCDATA)>
<!ELEMENT Ds_MerchantData (#PCDATA)>
<!ELEMENT Ds_Card_Type (#PCDATA)>
<!ELEMENT Ds_TransactionType (#PCDATA)>
<!ELEMENT Ds_ConsumerLanguage (#PCDATA)>
<!ELEMENT Ds_ErrorCode (#PCDATA)>
<!ELEMENT Ds_CardCountry (#PCDATA)>
<!ELEMENT Ds_AuthorisationCode (#PCDATA)>
<!ELEMENT Signature (#PCDATA)>
    
```

Para generar el valor del campo Signature en el mensaje de notificación del comercio aplicaremos un SHA-1 a la cadena resultante de concatenar el mensaje <Request ...>...</Request> con la clave del comercio.

Ejemplo:

Sea el siguiente mensaje:

```

<Message>
  <Request Ds_Version="0.0">
    <Fecha>01/04/2003</Fecha>
    <Hora>16:57</Hora>
    <Ds_SecurePayment>1</Ds_SecurePayment>
    <Ds_Amount>345</Ds_Amount>
    <Ds_Currency>978</Ds_Currency>
    <Ds_Order>165446</Ds_Order>
    <Ds_MerchantCode>999008881</Ds_MerchantCode>
    <Ds_Terminal>001</Ds_Terminal>
    <Ds_Card_Country>724</Ds_Card_Country>
    <Ds_Response>0000</Ds_Response>
    <Ds_MerchantData>Alfombrilla para raton</Ds_MerchantData>
    <Ds_Card_Type>C</Ds_Card_Type>
    <Ds_TransactionType>1</Ds_TransactionType>
    <Ds_ConsumerLanguage>1</Ds_ConsumerLanguage>
  </Request>
</Message>
    
```


La firma se calculará así (siendo la clave secreta qwertyasdf0123456789):

firma = SHA-1 (

```
<Request
Ds_Version="0.0"><Fecha>01/04/2003</Fecha><Hora>16:57</Hora><Ds_SecurePayment>1</Ds_SecurePayment>
<Ds_Amount>345</Ds_Amount><Ds_Currency>978</Ds_Currency><Ds_Order>165446</Ds_Order><Ds_Mercha
ntCode>999008881</Ds_MerchantCode><Ds_Terminal>001</Ds_Terminal><Ds_Card_Country>724</Ds_Card_Co
untry><Ds_Response>0000</Ds_Response><Ds_MerchantData>Alfombrilla para raton</Ds_MerchantData><Ds_Card_Type>C</Ds_CardType><Ds_TransactionType>1</Ds_TransactionType><Ds
_ConsumerLanguage>1</Ds_ConsumerLanguage></Request>qwertyasdf0123456789
```

)

resultado = c0026a953d4b4d52c360751bdad8476de311d36e

- Mensaje de respuesta del comercio a la notificación:

```
<!ELEMENT Message (Response, Signature)>
```

```
<!ELEMENT Response (Ds_Response_Merchant)>
```

```
<!ATTLIST Response Ds_Version CDATA #REQUIRED>
```

```
<!ELEMENT Ds_Response_Merchant (#PCDATA)>
```

```
<!ELEMENT Signature (#PCDATA)>
```

Los posibles valores que podrá tomar la etiqueta Ds_Response_Merchant serán:

- 'OK' cuando la notificación se ha recibido correctamente.
- 'KO' cuando se ha producido algún error.

Para generar el valor del campo Signature en el mensaje de respuesta del comercio aplicaremos un SHA-1 a la cadena resultante de concatenar el mensaje <Response>...</Response> con la clave del comercio.

Ejemplos de mensajes intercambiados en una notificación con Sincronización SOAP:

- Mensaje de notificación enviado desde el SIS:

```
<Message>
```

```
<Request Ds_Version="0.0">
```

```
<Fecha>01/04/2003</Fecha>
```

```
<Hora>16:57</Hora>
```

```
<Ds_SecurePayment>1</Ds_SecurePayment>
```

```
<Ds_Amount>345</Ds_Amount>
```

```
<Ds_Currency>978</Ds_Currency>
```

```
<Ds_Order>165446</Ds_Order>
```

```
<Ds_Card_Type>C</Ds_Card_Type>
```

```
<Ds_MerchantCode>999008881</Ds_MerchantCode>
```

```
<Ds_Terminal>001</Ds_Terminal>
```

```
<Ds_Card_Country>724</Ds_Card_Country>
```

```
<Ds_Response>0000</Ds_Response>
```

```
<Ds_MerchantData>Alfombrilla para raton</Ds_MerchantData>
```

```
<Ds_TransactionType>1</Ds_TransactionType>
```

```
<Ds_ConsumerLanguage>1</Ds_ConsumerLanguage>
```

```
</Request>
```

```
<Signature>efc52623500b6174af3216190373ba35360e99d5</Signature>
```

```
</Message>
```

■ **Mensaje de respuesta desde el comercio al SIS:**

```
<Message>
  <Response Ds_Version="0.0">
    <Ds_Response_Merchant>OK</Ds_Response_Merchant>
  </Response>
<Signature>adb300af20b477f6438a3f9fb671b3d9afccb444</Signature>
</Message>
```

WSDL para el servicio InotificacionSIS

Los comercios que deseen desarrollar un servicio SOAP deben ajustarse a esta WSDL. A partir de ella y, mediante herramientas de generación automática de código, se puede desarrollar el esqueleto del servidor SOAP de forma cómoda y rápida.

La WSDL que debe cumplir el servicio SOAP desarrollado por el cliente es la siguiente:

```
<?xml version="1.0" encoding="UTF-8"?>

<definitions name="InotificacionSIS"
  targetNamespace=https://sis.sermepa.es/sis/InotificacionSIS.wsdl
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:tns="https://sis.sermepa.es/sis/InotificacionSIS.wsdl"
  xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns="http://schemas.xmlsoap.org/wsdl/">

  <message name="procesaNotificacionSISRequest">
    <part name="XML" type="xs:string"/>
  </message>

  <message name="procesaNotificacionSISResponse">
    <part name="return" type="xs:string"/>
  </message>

  <portType name="InotificacionSISPortType">
    <operation name="procesaNotificacionSIS">
      <input message="tns:procesaNotificacionSISRequest"/>
      <output message="tns:procesaNotificacionSISResponse"/>
    </operation>
  </portType>

  <binding name="InotificacionSISBinding" type="tns:InotificacionSISPortType">
    <soap:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/http"/>
    <operation name="procesaNotificacionSIS">
      <soap:operation
        soapAction="urn:InotificacionSIS#procesaNotificacionSIS" style="rpc"/>
      <input>
        <soap:body use="encoded"
          encodingStyle=http://schemas.xmlsoap.org/soap/encoding/ namespace="InotificacionSIS"/>
      </input>
      <output>
        <soap:body use="encoded"
          encodingStyle=http://schemas.xmlsoap.org/soap/encoding/ namespace="InotificacionSIS"/>
      </output>
    </operation>
  </binding>

  <service name="InotificacionSISService">
    <port name="InotificacionSIS" binding="tns:InotificacionSISBinding">
      <soap:address location="http://localhost/WebServiceSIS/InotificacionSIS.asmx"/>
    </port>
  </service>

</definitions>
```