

ANEXO III

DOCUMENTO DE ESPECIFICACIONES TÉCNICAS PARA EL ENVÍO DEL PAQUETE DE DATOS SEPA.

1. Introducción

El presente documento reúne las especificaciones técnicas relativas al envío y recepción de datos al “Sistema Electrónico de Publicidad de Precios Argentinos (SEPA)”, creado por la Resolución N° 12 de fecha 12 de febrero de 2016 de la SECRETARÍA DE COMERCIO del MINISTERIO DE PRODUCCIÓN.

El documento describe el mecanismo de transmisión de datos a utilizar, sus características tecnológicas, las condiciones de seguridad establecidas y las instrucciones necesarias para su utilización.

2. Glosario

Paquete de Datos SEPA: Hace referencia al conjunto de archivos de datos de sucursales, productos, precios, etcétera, que el comercio debe informar según la normativa.

Canal de Información: Hace referencia al medio por el cual el comercio informa los datos sobre sucursales, productos, precios, etcétera, según la normativa.

Amazon Web Services (AWS): Amazon Web Services es un proveedor de servicios de computación en la web, dentro de cuya infraestructura está implementado el “Sistema Electrónico de Publicidad de Precios Argentinos (SEPA)”.

S3: Hace referencia al servicio de almacenamiento de datos en la web que ofrece Amazon Web Services y que es utilizado por el “Sistema Electrónico de Publicidad de Precios Argentinos (SEPA)” para recibir en forma segura los paquetes de datos enviados por los comercios.

Compartimiento de Datos (bucket): Hace referencia al compartimiento de datos de uso exclusivo del comercio dentro del servicio de almacenamiento S3 de Amazon Web Services implementado por la SUBSECRETARÍA DE COMERCIO INTERIOR de la SECRETARÍA

DE COMERCIO del MINISTERIO DE PRODUCCIÓN para recibir los Paquetes de Datos SEPA.

Identificador Único: Hace referencia al identificador único otorgado por la Autoridad de Aplicación a un comercio.

Secure Sockets Layer (SSL): Protocolo criptográfico de transmisión de datos por una red que usualmente es utilizado para proveer comunicaciones seguras en Internet.

Dirección IP (Internet Protocol): Es un número que identifica a un dispositivo conectado a Internet.

Algoritmo de Resumen: Hace referencia a un algoritmo criptográfico que permite obtener una cadena de caracteres relativamente corta que actúa como resumen de un conjunto de datos de mayor tamaño.

Message-Digest Algorithm 5 (MD5): Hace referencia al Algoritmo de Resumen del Mensaje 5, conocido usualmente como MD5. Se utiliza como una forma de corroborar la integridad de un paquete de datos.

API REST: Interfaz de Programación de Aplicaciones (Application Programming Interface) de Transferencia de Estado Representacional (Representational State Transfer). Refiere a un tipo de interfaz que permite utilizar servicios web fácilmente para la programación de aplicaciones y que es ampliamente utilizado en Internet.

3. Canal de Información

La SUBSECRETARÍA DE COMERCIO INTERIOR recibirá los Paquetes de Datos SEPA transferidos por cada uno de los sujetos obligados y adheridos utilizando el servicio de almacenamiento de datos conocido como S3 del proveedor de servicios Web, Amazon Web Services.

Dentro de dicho servicio de almacenamiento de datos, cada comercio poseerá un Compartimiento de Datos de uso exclusivo (llamado bucket en inglés, según la documentación en línea de Amazon Web Services), al cual transmitirá su Paquete de Datos diariamente y de acuerdo con lo establecido por el Anexo II de la presente medida.

Cada comercio tendrá únicamente permiso de escritura sobre su propio Compartimiento de Datos (o bucket) y no tendrá permiso de lectura sobre ninguno de ellos. Es decir, ningún otro comercio puede escribir datos en un Compartimiento de Datos que no le corresponda y ningún comercio puede leer datos de un Compartimiento de Datos, en ningún caso, incluyendo el propio.

El nombre del Compartimiento de Datos de cada comercio se corresponde con el siguiente formato: “comercio-sepa-comercio_id”.

Donde comercio_id es el identificador único del comercio provisto por la Autoridad de Aplicación al momento del alta en el “Sistema Electrónico de Publicidad de Precios Argentinos (SEPA)”.

4. Requerimientos generales

A continuación, se describen algunos requerimientos generales que tiene el Canal de Información a los fines de garantizar la integridad de los datos y la autenticidad tanto del comercio como de la información transmitida.

a. Seguridad de la conexión

Para garantizar la seguridad en la transmisión, los Paquetes de Datos SEPA deberán ser enviados utilizando una conexión segura bajo el protocolo de comunicación segura SSL (“Secure Sockets Layer”).

En caso de que un paquete de datos no sea enviado utilizando una conexión segura bajo el protocolo SSL, el mismo será rechazado y el canal de información enviará el error “400 Bad Request”.

b. Rango de IPs

Los comercios tienen la opción de proveer a la Autoridad de Aplicación un rango de Direcciones IP desde donde se enviará el paquete de datos. En caso de optar por añadir esta capa

extra de seguridad, todo envío generado desde un dispositivo no perteneciente a una Dirección IP dentro de ese rango será rechazado, devolviendo el error “403 Access Denied”.

c. Integridad de los paquetes enviados

Para asegurar la integridad de los paquetes enviados, el comercio deberá aplicar un Algoritmo de Resumen de mensajes MD5 al Paquete de Datos SEPA. Este permitirá al canal de información corroborar que el paquete recibido coincide con el paquete enviado por el comercio. El resultado del Algoritmo de Resumen debe estar codificado en base64.

En la sección “Algoritmo de Resumen de Mensaje MD5” se proveerán las instrucciones necesarias para una sencilla implementación de este requerimiento.

En caso de enviar una codificación errónea, el paquete será rechazado, devolviendo el error “400 Bad Request”.

d. Rango horario

Los Paquetes de Datos SEPA serán recibidos en DOS (2) rangos horarios, para cumplir con lo establecido en el Anexo II de la presente medida.

1. Desde las DIECISÉIS HORAS (16:00 hs.) del día anterior hasta las SEIS HORAS (06:00 hs.) del día de publicación, para el envío diario.
2. Desde las OCHO HORAS (08:00 hs.) hasta las DIEZ HORAS (10:00 hs.) del día de publicación, en caso de enviar un paquete de datos rectificatorio.

Todo paquete enviado fuera de estos rangos horarios será rechazado por el Canal de Información, devolviendo el mensaje de error “403 Access Denied”.

5. Instrucciones

1. Alta en Amazon Web Services (AWS).

1.a. Crear cuenta en AWS

En primer lugar, el comercio deberá crear una cuenta en el proveedor de servicios en la nube Amazon Web Services. En caso de que el comercio ya posea una cuenta propia, no es necesario crear una nueva.

Las credenciales de acceso a la cuenta de AWS son de uso exclusivo del comercio y no deberá compartirlas con la Autoridad de Aplicación ni con terceros, bajo ninguna circunstancia.

Las políticas de protección y actualización de claves son responsabilidad de los sujetos obligados.

La creación de una cuenta en AWS exige introducir una tarjeta de crédito como parte del proceso de alta. Sin embargo, el envío de datos diarios no generará costo alguno para los comercios. El costo de las transferencias es abonado por el propietario de los compartimientos de datos (o buckets), para el caso, la Autoridad de Aplicación.

1.b. Crear usuario en el servicio de Gestión de Identidad y Acceso (IAM)

En este punto, el comercio ya poseerá una cuenta de administrador (usualmente denominada como “root account” en inglés y en la documentación de Amazon Web Services) en AWS. En los próximos pasos, el comercio necesitará tener por lo menos un usuario de Gestión de Identidad y Acceso (“IAM user” en inglés).

El sistema de Gestión de Identidad y Acceso (IAM) permite controlar el acceso a recursos de la cuenta de AWS del comercio. El comercio puede asignar a usuarios IAM permisos específicos para realizar distintos tipos de acciones.

Para enviar el Paquete de Datos SEPA al sistema de almacenamiento de datos establecido por la SUBSECRETARÍA DE COMERCIO INTERIOR, es necesario que el comercio cuente con al menos un usuario que tenga acceso total al servicio de S3 de AWS.

Para seguir las instrucciones completas acerca de cómo crear un usuario IAM, se remite al comercio al siguiente link explicativo de AWS:
http://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_create.html

A continuación, se comentan brevemente los pasos que debe seguir el comercio para crear un usuario IAM con acceso total al servicio S3 de AWS:

1. Dentro de la consola de AWS, se debe seleccionar el servicio “IAM”.

2. Dentro de la sección “Users” se debe presionar en “Create New Users”.
 - a. Asegurarse de que está tildada la opción “Generate an access key for each user”.

Estas claves serán necesarias a la hora de configurar los permisos para transmitir el paquete de datos (tanto por línea de comandos como para una implementación programática).
 - b. Una vez creado el usuario, AWS muestra las credenciales de acceso por única vez, de forma tal que deben ser guardadas en forma segura en ese momento.

1.c. Asignar permisos al usuario de Gestión de Identidad y Acceso (IAM)

Para que el usuario IAM pueda, en adelante, realizar transferencias de datos al Compartimiento de Datos de S3 del comercio, debe contar con permisos de escritura para ese mismo.

Estos permisos se asignarán de la siguiente manera:

1. En la solapa de “Permissions” se debe crear un nuevo permiso para el usuario (usualmente denominado como “user policy” en la documentación de Amazon Web Services) haciendo un click sobre el botón “Create User Policy”.
2. Elegir “Custom Policy”. El nombre asignado será indistinto.
3. Dentro de “Policy Document”, utilizar el siguiente modelo reemplazando `bucket-name` por el nombre del Compartimiento de Datos del comercio, que sigue el siguiente formato: `comercio-sepa-comercio_id`. Guardar.

En caso de errores en el nombre del Compartimiento de Datos (o bucket) se recibirá el mensaje “403 Forbidden - Access Denied”.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "sepaPutPolicy",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject", "s3:PutObjectAcl"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name/*"
      ]
    }
  ]
}

```

2. Envío de credenciales al “Sistema Electrónico de Publicación de Precios Argentinos (SEPA)”.

La Autoridad de Aplicación debe asignar permisos al comercio para que este pueda realizar transferencias de datos al Compartimiento de Datos (o bucket) de S3 correspondiente. Para otorgar dichos permisos el comercio deberá remitir por nota a la SUBSECRETARÍA DE COMERCIO INTERIOR el número identificador de su cuenta de AWS (id).

Los usuarios pueden acceder al id de su cuenta de AWS a través de la solapa “My Account”.

Adicionalmente, en caso de optar por restringir el envío de datos a través de un rango de Direcciones IP previamente establecidas, estas deberán ser informadas junto con el id de cuenta de AWS.

Los datos enviados a la Autoridad de Aplicación deben ser enviados en el siguiente formato:

comercio_id	Identificador Único del comercio otorgado por la Autoridad de Aplicación.
aws_id	111111111111 (número entero -int- de 12 dígitos)
rango_ips	[1.1.1.1, 1.1.1.2] (lista -array- de ips de tamaño n)

3. Implementación de la transferencia del paquete de datos.

Cada comercio es responsable de adoptar un mecanismo para la transferencia del paquete de datos mediante el Canal de Información.

En esta sección se hace referencia a las diversas interfaces mediante las cuales es posible realizar esta tarea. En todos los casos, se recomienda implementar una rutina desatendida que ejecute la tarea automáticamente.

Opción 1: Implementación por línea de comando (opción recomendada).

Se recomienda que el envío del Paquete de Datos SEPA a través del Canal de Información se realice utilizando el servicio de AWS Command Line Interface (CLI). Esta herramienta permite administrar y automatizar los objetos del servicio de almacenamiento de datos S3 desde la línea de comando.

Instalación de AWS CLI.

1. Elegir método de instalación. Hay opciones para Windows, Linux, OS X y Unix.
2. Seguir instrucciones detalladas en la documentación.
3. Desde la consola, testear el funcionamiento del AWS CLI. > aws help.
4. Configurar credenciales. > aws configure.
 - a. El AWS Access Key ID y el AWS Secret Access Key hacen referencia a las credenciales de acceso de un usuario IAM mencionadas en la sección 1.b.

Algoritmo de Resumen de Mensaje MD5

El resultado de la aplicación del algoritmo MD5 sobre el Paquete de Datos SEPA a enviar debe estar codificado en base64 para que el paquete sea aceptado por el Compartimiento de Datos al cual se envía el paquete.

El paquete puede ser codificado directamente desde la línea de comando de la siguiente manera:

```
openssl dgst -md5 -binary sepa.zip | openssl enc -base64
```

La codificación en MD5 también puede ser realizada en múltiples lenguajes de programación.

Comando.

Una vez configurada la herramienta de línea de comandos AWS CLI y calculado el algoritmo de resumen de mensajes MD5, el comercio puede enviar el Paquete de Datos SEPA ejecutando el comando que se describe a continuación, reemplazando las variables (a) comercio_id, (b) local_path_to_file y (c) hash por sus valores correspondientes:


```
aws s3api put-object --bucket comercio-sepa-comercio_id --key sepa.zip --body  
local_path_to_file --content-md5 hash
```

Este comando se puede automatizar fácilmente configurando el sistema de programación de tareas del sistema operativo que se utilice.

Resultados.

En caso de que la transferencia se realice con éxito, el comando responderá con un código de respuesta número 0. Para más información de la respuesta obtenida puede verse la sección output de la documentación del método put-object de AWS.

En caso de que la transferencia sea rechazada, el comando responderá con el código de error correspondiente. Una lista de los posibles errores de S3 puede encontrarse en la “Documentación de Error Responses” del servicio de S3 de AWS.

Opción 2: Implementación programática.

API REST de AWS

Al servicio de S3 de AWS también se puede acceder y administrar mediante el uso de una interfaz de programación de aplicaciones de transferencia de estado representacional (usualmente conocida como API REST, en inglés). Existen librerías en diversos lenguajes de programación que facilitan el uso de esta API.

AWS SDK

AWS también provee diversos SDKs (Kit de Desarrollo de Software, en español) para administrar sus servicios. En el link <https://aws.amazon.com/es/tools/> puede encontrarse un listado de estas herramientas.

6. Confirmación de Recepción y Aprobación del Paquete

A los fines de confirmar que el comercio ha cumplimentado con el deber de informar los precios de manera diaria, y de aprobar la difusión por parte de la SUBSECRETARÍA DE COMERCIO INTERIOR de la información provista, se llevarán a cabo DOS (2) instancias de validación.

Una primera instancia, donde se comunica que el Paquete de Datos SEPA ha sido transferido con éxito al Compartimiento de Datos (o bucket) del comercio. En este caso el Canal de Información envía un código de respuesta número cero ("0").

Una segunda instancia, luego de las SEIS HORAS (06:00 hs.) y previo a las OCHO HORAS (08:00 hs.) donde se verifica que el paquete de datos contiene los archivos correspondientes con los nombres, campos, y tipos de datos correspondientes y se comunica mediante mail que el paquete ha sido aprobado o rechazado.

Repitiendo el procedimiento para la instancia rectificatoria de las DIEZ HORAS (10:00 hs.).