****

**Manual de consumo de servicio de Notificaciones – Ambiente de Desarrollo**

***API Genérica***

**Tabla de contenido**

Historial de versiones 3

Información del proyecto 4

Aprobaciones 4

Resumen ejecutivo 4

Request 4

Response 4

# Historial de versiones

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Fecha** | **Versión** | **Autor** | **Organización** | **Descripción** |
| **22/11/2018** | **1.0** | **Nadir Palacios** | **Santander** | **Creación del Documento** |
| **01/05/2019** | **2.0** | **Emmanuel De la Isla** | **Santander** | **Adecuación del Documento** |
|  |  |  |  |  |
|  |  |  |  |  |

# Información del proyecto

|  |  |
| --- | --- |
| Empresa / Organización | Santander |
| Proyecto | Notificaciones |
| Fecha de preparación | 22/11/2018 |
| Cliente | Santander |
| Gerente / Líder de proyecto | Mayra Flores |

# Resumen

El presente documento “Manual de uso” ha sido elaborado con el propósito de incluir los detalles a considerar en el consumo del servicio de API genérica del Notificador.

# Servicio Token OAuth

El servicio de Token OAuth provee el mecanismo para validar la autorización a los recursos destino de API Genérica utilizando JWT

* **AMBIENTE**

Desarrollo

* **URL**

https://webapigateway.dev.mx.corp/santander-mexico/desarrollo/oauth/password/token

* **MÉTODO**

POST

* **REQUEST**
  + **BODY (form-data) (KEY/VALUE)**
    - scope / string
    - grant\_type / string
    - token / string
    - client\_id / string
    - client\_secret / secret

| **Campo** | **Descripción** |
| --- | --- |
| scope | **Descripción:** Ámbito de la autorización solicitada  **Type:** String  **Valor:** "notifications.send audit.write" |
| grant\_type | **Descripción:** Tipo de elemento de autorización solicitado  **Type:** String  **Valor:**   * En ambiente de desarrollo vale: “password”. * En PRE y PRO: “client\_credentials” |
| token | **Descripción:** Token de solicitud de token OAuth.  **Type:** String  Solamente se usa en desarrollo. En PRE y PRO se envía vacío.  **Formato:** Alfanumérico en base64 |
| client\_id | **Descripción: ID del consumidor**  **Type:** String  **Valor:**   * Ambiente desarrollo: “**f99ff54e-958f-4d4c-b81e-c1f9901314b6**” * PRE y PRO: El equipo de Notificaciones lo comunicará más adelante. |
| client\_secret | **Descripción:** Clave para consumir el servicio OAuth de generación de tokens  **Type:** String  **Valor:**   * Ambiente desarrollo: **rD0pH2vX0vI1uC7nS6vT0mO3aH1aL0nJ1pX4eC3rH6yU4rN4wI** * PRE y PRO: El equipo de Notificaciones lo comunicará más adelante. |

* **RESPONSE**
  + **200**

{

"token\_type":"string",

"access\_token":"string",

"expires\_in":0,

"scope":"string"

}

* **Request para ambiente de desarrollo**
  + **BODY (form-data) (KEY/VALUE)**
    - scope / notifications.send audit.write
    - grant\_type / password
    - token / 
    - client\_id / f99ff54e-958f-4d4c-b81e-c1f9901314b6
    - client\_secret / rD0pH2vX0vI1uC7nS6vT0mO3aH1aL0nJ1pX4eC3rH6yU4rN4wI



# Servicio API Genérica

El servicio de API genérica provee un mecanismo definido y claro por el que las iniciativas pertinentes puedan hacer el uso de envío de notificaciones PUSH, Email y SMS a través de proveedores externos.

* **AMBIENTE**

Desarrollo

* **URL:** https://webapigateway.dev.mx.corp/santander-mexico/desarrollo/notifications/v2.0/businessSupport/documentManagementAndArchive/correspondence/alertCorrServices/notices
* **MÉTODO:**

POST

* **REQUEST:**
  + **HEADER (parameter) (KEY/VALUE)**
    - Content-Type / string
    - Accept / string
    - x-ibm-client-id /string
    - X-Santander-Session-Id / string
    - branchID / string
    - msgRqHdr /string

| **Campo** | **Descripción** |
| --- | --- |
| Content-Type | **Descripción:** Tipo de contenido  **Valor:** “application/json” |
| accept | **Descripción:** Tipo de contenido que acepta la respuesta  **Valor:** “application/json” |
| x-ibm-client-id | **Descripción:** ID del consumidor. Mismo ID que se utiliza en el servicio de Token Oauth (campo client\_id).  **Valor:**  Para DEV vale: "f99ff54e-958f-4d4c-b81e-c1f9901314b6"  Para PRE y PRO: El equipo de Notificaciones lo comunicará más adelante. |
| Authorization | **Descripción:** Token OAuth proporcionado por el endpoint de autorización.  **Valor:** "Bearer ***<token OAuth>***" |
| X-Santander-Session-Id | **Descripción:** ID de sesión/mensaje. Hay que informarlo siempre, aunque sea sin valor.  **Valor:** “session\_id” |
| branchID | **Descripción:** Cualquier valor. Hay que informarlo siempre, aunque sea sin valor. Aplica para el caso de sucursales.  **Valor:** “” |
| msgRqHdr | **Descripción:** JSON que informa del channelID y de la IP del que emite la notificación. "{\"channelId\":\"***channelId***\",\"clientIPAddress\":\"***x.x.x.x***\"}"  **channelId:** Este dato es proporcionado por el equipo de notificaciones  **clientIp:** Dirección IP del servidor donde se está generando la petición |

* + **BODY (application/json)**

{

"alertInfo": {

"partyKeys": {

"partyIdMask": "String",

"partyId": "String"

},

"cardKeys": {

"cardNum": "String"

},

"acctKeys": {

"acctId": "String"

},

"alertScheduleDt": "String",

"deliveryInstruction": {

"deliveryMethod": 0

},

"alertIdTemplate": "String",

"idEvent": 0,

"alertMsg": "String",

"phoneNum": {

"phone": "String"

},

"alertData": [

{

"alertDataKey": "String",

"alertDataValue": "String",

"alertDataType": "String"

}

]

}

}

| **Campo** | **Descripción** |
| --- | --- |
| partyId | **Descripción:** Buc cliente. Hay que informarlo siempre, aunque sea sin valor. Para el caso de no clientes se debe informar con el valor “-1”. Se debe informar al menos uno de los valores (partyId, partyIdMask, cardNum, acctId) |
| partyIdMask | **Descripción:** Buc cliente tokenizado a 43 caracteres. Hay que informarlo siempre, aunque sea sin valor. Se debe informar al menos uno de los valores (partyId, partyIdMask, cardNum, acctId) |
| cardNum | **Descripción:** Número de tarjeta del cliente. Hay que informarlo siempre, aunque sea sin valor. Se debe informar al menos uno de los valores (partyId, partyIdMask, cardNum, acctId) |
| acctId | **Descripción:** Número de cuenta del cliente. Hay que informarlo siempre, aunque sea sin valor. Se debe informar al menos uno de los valores (partyId, partyIdMask, cardNum, acctId) |
| alertScheduleDt | **Descripción:** Fecha de envío  **Formato:** dd/MM/yyyy hh24:mm:ss |
| deliveryMethod | **Descripción:** Identifica el tipo de mensaje (SMS, EMAIL, PUSH)  **Valor:**   * 1: SMS * 3: EMAIL * 5: PUSH * 11: SMS (texto sin plantilla) * 13: RBM (SMS enriquecido) * 15: Blaster (VOZ) |
| alertIdTemplate | **Descripción:** ID que identifica la **plantilla** del mensaje a enviar. Dato proporcionado por equipo Notificaciones Santander. |
| idEvent | **Descripción:** ID del tipo de evento del mensaje (normativa, transaccional, informativa, etc.). Dato proporcionado por equipo Notificaciones Santander. |
| alertMsg | **Descripción:** En caso de ser un deliveryMethod 6, aquí se incluye el texto del mensaje a enviar |
| phone | **Descripción:** Número de celular del usuario |
| emailAddr | **Descripción:** Dirección de Email del usuario. |
| alertDataKey  alertDataValue  alertDataType | **Descripción:** Array de mapas de 3 campos que definen las características del mensaje. El ejemplo proporcionado corresponde a un envío de sms. El campo “alertDataType” siempre vale “PARAMETRO”. Para el caso que se tengan parámetros en la plantilla |



* **RESPONSE:**
  + **200**

{

"status":{

"statusCode":"String",

"serverStatusCode":"String",

"severity":"String",

"statusDesc":"String",

"additionalStatus":{

"statusCode":"String",

"serverStatusCode":"String",

"severity":"String",

"statusDesc":"String" //En caso que la plantilla sea que requiera un Código de verificación o bien la generación de un OTP en este campo se regresa el valor

}

},

"rqUID":”String”

}

****

* **Ejemplo**

****

**NOTA:** Los siguientes datos varían entre ambientes y son específicos por cada plantilla/mensajes. Se deben solicitar al equipo de Notificaciones.

**Código de Verificación (OTP)**

En caso que la plantilla que se invoque esté configurada y generé el código de verificación, este valor es regresado en el campo ya mencionado antes "statusDesc" del response del servicio, esto solo es en caso que la notificación sea exitosa “NTFMX101”. El valor que regresa el código de verificación tiene una encriptación estandar (MessageDigest md = MessageDigest.getInstance("SHA-256")), usando una clave para encriptar y descencriptar, la clave usada para el ambiente de desarrollo es “notificaciones01”, para ambientes de PRE y PRO se les asignará una especifica por ambiente. A continuación se muestra un código estandar ejemplo para la descencriptación:

**public** **static** String desCipher(String textoEncriptado, String secretKey) **throws** Exception {

String base64EncryptedString = "";

**try** {

byte[] message = Base64.decodeBase64(URLDecoder.decode(textoEncriptado, "UTF-8").getBytes("utf-8"));

MessageDigest md = MessageDigest.getInstance("SHA-256");

byte[] digestOfPassword = md.digest(secretKey.getBytes("utf-8"));

byte[] keyBytes = Arrays.copyOf(digestOfPassword, 24);

SecretKey key = new SecretKeySpec(keyBytes, "AES");

Cipher decipher = Cipher.getInstance("AES");

decipher.init(2, key);

byte[] plainText = decipher.doFinal(message);

base64EncryptedString = new String(plainText, "UTF-8");

} **catch** (Exception ex) {

*LOGGER*.error("CipherJupiter.desCipher() " + ex.getMessage());

**throw** **new** Exception("Desde la aplicación que deseas acceder no tiene acceso");

}

**return** base64EncryptedString;

}

DeliveryMethod = x

AlertIdTemplate = xxxxx

idEvent = xxxx

channelId = xxxx

Para el resto de respuestas, además del código HTTP 200 se anexará un estado de la siguiente tabla como información adicional del estado.

|  |  |  |
| --- | --- | --- |
| Catálogo de Mensajes | | |
| ID Mensaje | **Detalle** | **Descripción** |
| NTFMX101 | OK | SMS OK, EMAIL QUEUE, PUSH OK |
| NTFMX102 | Error Interno |  |
| NTFMX103 | Telefono Invalido | Cuando no se tiene registro del Numero Celular |
| NTFMX104 | Email Invalido | Cuando no se tiene registro del Email. |
| NTFMX105 | No permitido | Por regla de negocio no es posible ejecutar la notificación. Banderas |
| NTFMX106 | Parámetros Incorrectos | Se especificara el parámetro que no se valida. |
| NTFMX107 | Plantilla Invalida | Cuando la plantilla enviada no es la correcta o no existe. |
| NTFMX108 | Cliente sin tokenizacion | Cuando el cliente a notificar no tiene BUC Tokenizado, la notificación no es enviada ya que no habría trazabilidad. |
| NTFMX109 | Fallo en Base de Datos | Cuando se tiene un fallo interno con la base de datos. |
| NTFMX110 | Credenciales Incorrectas | Contactar al área de notificaciones para la aclaracion |
| NTFMX111 | Error Envío Email | Error al encolar email |
| NTFMX112 | Combinación incorrecta | Los datos: channelId|deliveryMethod|alertIdTemplate|idEvent no tienen un registro valido para notificación |
| NTFMX113 | SMS Repetido | SMS Repetido |
| NTFMX114 | Relación incorrecta | No existe relación de Evento|Plantilla |
| NTFMX115 | Email  Repetido | Email repetido |
| NTFMX116 | Cliente no enrolado | No se encuentra enrolado el cliente |
| NTFMX117 | Sin BUC | No existe el BUC |
| NTFMX118 | Sin cuenta | No existe la cuenta / contrato |
| NTFMX119 | Sin plastico | No existe el plástico |
| NTFMX120 | No tiene toquenización | Cliente sin toquenización |
| NTFMX121 | Distinto dato de contactabilidad | El dato de contactabilidad por SMS no es válido, pero si tiene EMAIL como medio adicional |
| NTFMX122 | Distinto dato de contactabilidad | El dato de contactabilidad por EMAIL no es válido, pero si tiene SMS como medio adicional |
| NTFMX123 | No cuenta con contactabilidad | No se cuenta con SMS ni con EMAIL para contactar |
| NTFMX124 | Dato de contactabilidad sin relacion | Dato de contactabilidad no relacionado al cliente |
| NTFMX125 | Error Envío Email Adjuntos | No fue posible enviar el email con adjunto |