INCORPORACIÓN E IMPLEMENTACIÓN AL SISTEMA DE RECOLECCIÓN DE DATOS DE LA SUPERINTENDENCIA DE ALIANZA PÚBLICO PRIVADA (SDR SAPP)

SECCIÓN 1
OBJETIVO

La presente normativa tiene como objetivo establecer los lineamientos para la implementación del servicio de interconectividad entre la SAPP y los agentes regulados.

SECCIÓN 2
ALCANCE Y ÁMBITO DE APLICACIÓN

En esta normativa se formulan los lineamientos para estandarizar la implementación de servicios de interoperabilidad entre la Superintendencia de Alianza Público Privada (SAPP) y los agentes regulados.

Estas entidades deben dar cumplimiento de los puntos 7 (Servicios Web), 8 (Seguridad), 9 (Disponibilidad), y 10 (Políticas) mínimamente.

Los lineamientos contenidos en esta normativa establecen estándares técnicos mínimos a ser implementados por todos los agentes regulados, sin perjuicio del trabajo desarrollado por aquellas que ya hayan asumido como parámetros rectores, normas y estándares nacionales e internacionales vigentes o de otra naturaleza en materia de interoperabilidad.

Tomando en cuenta la naturaleza dinámica de la tecnología, las entidades podrán implementar versiones superiores y/o con mejoras en las características, sin dejar de considerar todos los puntos que se detallan en este documento.

La SAPP analizará periódicamente la necesidad de actualización de esta normativa para su consideración e implementación.

SECCIÓN 3
NATURALEZA DEL SERVICIO DE INTEROPERATIVIDAD

Cada servicio de interoperabilidad presenta ciertas características que definen su naturaleza de acuerdo al tipo de datos que proporcionan. En este marco, se recomienda que la entidad obligada a implementar éste servicio de interoperabilidad identifique primero el tipo de servicio que consumirá con la finalidad de conocer el comportamiento que este tendrá sobre los datos solicitados. Los tipos de servicios de interoperabilidad son de lectura o transaccional, individual o masivo, los cuales se describen a continuación:

3.1 TIPO DE SERVICIO DE CARGA/ENVÍO O TRANSACCIONAL

Cuando el servicio de interoperabilidad permite solamente la carga o envío de los datos y no realiza modificación de los mismos en la fuente primaria, el tipo de servicio de interoperabilidad es sólo de carga.

Un tipo de servicio de interoperabilidad de carga puede incluir el procesamiento y la formación de una respuesta dedicada.

Cuando el servicio de interoperabilidad permite la creación de los datos, el tipo de servicio es transaccional.

Es importante mencionar que en el caso de identificar un servicio de tipo transaccional se aplicarán mayores medidas de seguridad en su implementación, como se verá más adelante en el punto 8.2 (Seguridad de los datos).

3.2 TIPO DE SERVICIO INDIVIDUAL O MASIVO

Cuando el agente regulado utiliza el servicio de interoperabilidad para cargar/enviar solamente un conjunto de datos relacionados y estructurados entre sí (por ejemplo, los datos de una persona como su nombre, número de cédula de identidad, fecha de nacimiento), el tipo del servicio de interoperabilidad es individual.

En cambio, cuando el agente regulado utiliza el servicio de interoperabilidad para cargar o enviar un listado de un conjunto de datos relacionados y estructurados, se considera a este tipo de servicio como masivo (por ejemplo, un listado de personas).

SECCIÓN 4
SEMÁNTICA

La interoperabilidad requiere que todos los participantes hablen y apliquen un lenguaje común para intercambiar los datos, de modo que estos se entiendan de la misma manera.

Es necesario definir las características de los datos que se desean intercambiar mediante el servicio de interoperabilidad:

4.1 OBJETO

Un objeto es la abstracción de un elemento físico o conceptual del que pueden identificarse los atributos, los metadatos de esos atributos, las relaciones y sus ámbitos (los contextos en que tiene sentido este objeto).

Los objetos se definirán de manera consensuada entre los agentes regulados y la SAPP con el fin de otorgarles un mismo significado.

4.2 CÓDIGO

Para identificar a los objetos de una misma manera se necesita definir un código de identificación único y consensuado o utilizar los códigos ya definidos, si existieran.

En caso de crearse un código nuevo, se debe definir tanto su estructura como sus características, dicha definición estará a cargo del agente regulado y la SAPP de manera separada o conjuntamente.

La finalidad de este código es la identificación univoca de un objeto que permite relacionarlo con otro para posibilitar el cruce de información entre bases de datos.

SECCIÓN 5
SERVICIOS WEB

Se recomienda utilizar los siguientes lineamientos al implementar servicios de interoperabilidad:

5.1 DEFINICIÓN DE PARÁMETROS DE ENTRADA/SALIDA

La SAPP establece los parámetros de entrada y salida del servicio de acuerdo a su naturaleza.

Cada parámetro será definido claramente y describirá su propósito; esta definición facilitará, posteriormente, la generación de la documentación respectiva.

5.2 VALIDACIÓN DE LOS MENSAJES

La validación de los mensajes entre los sistemas se realiza para verificar que la estructura de los objetos que se utilizan en el servicio de interoperabilidad sea la correcta.

Validar los mensajes entre los sistemas, evita problemas de funcionamiento no previstos cuando los agentes regulados consumen el servicio.

La SAPP valida la estructura de los mensajes entre los sistemas, tanto de los parámetros de entrada como los de salida.

5.3 VERSONAMIENTO

En ocasiones es necesario tener varias versiones de un mismo servicio. Esto puede ocurrir cuando el servicio presenta nuevas características de funcionamiento (o en el caso de necesitar otros parámetros de entrada).

SAPP generará una nueva versión de los servicios de interoperabilidad como mejora del sistema a los agentes regulados que ya usan el servicio y así mantener un histórico de los datos recibidos y las versiones utilizadas.

El versionamiento debe considerarse desde el inicio de la implementación.

5.4 MANEJO DE ERRORES

Todos los posibles problemas que presenten en los servicios de interoperabilidad están identificados, de modo que los agentes regulados interpreten los motivos de las fallas.

Los mensajes de error emitidos por el servicio de interoperabilidad utiliza los códigos estándar HTTP (400, 403, 415, 500 etc.) y una descripción que permita comprenderlo de manera clara.

Los códigos de errores y descripciones establecidos para el servicio de interoperabilidad siempre serán apegados a la normativa estándar del protocolo HTTP, conforme a los descritos en la sección de anexos punto 13.3.1 Instructivo carga mediante API RestFul.

5.5 CODIFICACIÓN

Los agentes regulados tienen que interpretar de la misma manera los caracteres utilizados para la transmisión de mensajes entre sistemas y archivos de carga manual (Excel), siempre utilizar la codificación (encoding) UTF8 en todos los servicios de interoperabilidad.

5.6 ZONA HORARIA

Todos los servicios de interoperabilidad utilizan la misma zona horaria, esto con el fin de que todos los agentes regulados conciban los tiempos de la misma manera. Para el caso del Estado Hondureño se utilizá GMT-6.

SECCIÓN 6
SEGURIDAD

Seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información; también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad.

6.1 SEGURIDAD DE LA CAPA DE TRANSPORTE

Es necesario contar con protocolos de seguridad en el canal o medio por el cual se transmitirá la información, esto para evitar que ajenos puedan verla o modificarla. Existen diversas tecnologías para este fin, como ser:

6.1.1 TLS (TRANSPORT LAYER SECURITY O SEGURIDAD DE LA CAPA DE TRANSPORTE)

El protocolo TLS permite la identificación y autenticación de las entidades a nivel del protocolo de transporte, consiguiendo que la comunicación sea confidencial y que la información enviada y/o recibida esté íntegra.

Este protocolo provee un medio seguro para comunicarse, siendo su principal propósito la confidencialidad de la información transferida. La integridad de la información intercambiada se logra autenticando los mensajes entre sistemas en cada transmisión.

Es recomendable siempre utilizar TLS en procesos de interoperabilidad que requieren algún tipo de autenticación y/o confidencialidad, ya sea con claves obtenidas de una entidad certificadora o con claves autogeneradas, dado que su implementación en general es sencilla de realizar, comparada con otras tecnologías.

6.1.2 VPN (VIRTUAL PRIVATE NETWORK O RED PRIVADA VIRTUAL)

Una VPN es un canal privado cifrado de comunicación. Se trata de un ambiente de comunicaciones donde el ingreso es restringido y habilitado solo para las partes que quieren comunicarse; es decir, que el canal no puede ser visto ni entendido por ajenos.

Una VPN ofrece un canal seguro de transmisión sobre una red no segura, con las siguientes propiedades: confidencialidad, integridad y autenticación. Todas estas propiedades son añadidas a la seguridad propia del servicio de interoperabilidad (el servicio de interoperabilidad podría tener autenticación y autorización).

Esta tecnología se utiliza cuando se requiere transmitir información sensible, dado que al existir diversas tecnologías para la implementación de VPNs, la conexión entre productos de distintos proveedores suele ser compleja.

*Ésta es la tecnología que la SAPP ha adoptado para la transmisión de datos por parte de los agentes regulados. La SAPP entregará a cada agente regulado una VPN que será utilizada para poder realizar la transmisión de datos de manera segura, íntegra y confidencial.

6.2 SEGURIDAD DE LOS DATOS

6.2.1 AUTENTICACIÓN Y AUTORIZACIÓN

La autenticación es la verificación de la identidad de la entidad consumidora (agentes regulados), mientras que la autorización es la verificación de los permisos que tiene dicha entidad sobre un recurso específico.

La SAPP siempre realiza primero la autenticación y luego la autorización. Esto se verifica en cada petición de la entidad consumidora (agentes regulados) hacia el servicio de interoperabilidad expuesto por la SAPP.

La autenticación y autorización se efectúa de la siguiente manera:

6.2.1.1 AUTENTICACIÓN BÁSICA (BASIC AUTH)

La autenticación básica es el método más simple, utiliza un usuario y contraseña para identificar al usuario de la entidad consumidora (Agentes regulados).

Es importante mencionar que la SAPP ha implementado procedimientos de uso y ciclo de vida de las contraseñas, lo cual obligará a los agentes regulados a modificar sus claves de acceso en rangos de tiempo adecuados.

6.3 AUDITORÍA

La auditoría es la revisión y comprobación de las acciones realizadas para reconstruir una serie de eventos que generaron un hecho específico. La manera más común para efectuar estas auditorías es a través de registros de eventos (logs) en servidores seguros y solamente accesibles por personal autorizado.

La SAPP implementa y utiliza los registros de eventos con toda la información posible. En este marco, lo mínimo que contienen son: información temporal, información de la aplicación que está realizando el registro del evento, quién realizó el evento (datos del agente regulado), el tipo de evento que se haya realizado y la solicitud y respuesta del servicio.

No se incluye en los registros de eventos información sensible del agente regulado (contraseña por ejemplo), rutas a archivos o cadenas de conexión a la base de datos, ya que esto constituye un riesgo de seguridad.

SECCIÓN 7
DISPONIBILIDAD

La SAPP garantizará que el servicio de interoperabilidad esté disponible de forma continua y sin interrupción, así mismo las entidades consumidoras (agentes regulados) deberán implementar características que permitan garantizar un flujo continuo de datos en tiempo real con los servicios web SAPP.

A continuación se detallan las características más importantes sobre la disponibilidad de los servicios Web SAPP:

7.1 REDUNDANCIA

Para garantizar el estado de los servicios de interoperabilidad es recomendable eliminar los puntos únicos de fallo. Esto se logra incorporando componentes redundantes (servidores, enrutadores, energía, software, microservicios, refrigeración, IPs, nombre de dominio y otros), para que en caso de catástrofes o incidencias, el componente pueda reemplazar las tareas del otro que hubiese presentado fallas. Es recomendable poner en práctica este punto para que así se tolere la pérdida o desperfectos funcionales de algún componente de la infraestructura.

No siempre es posible eliminar todos los puntos únicos de fallo debido al costo que esto implica (hacer una evaluación de riesgo contra costo); sin embargo, de acuerdo a la criticidad del servicio de interoperabilidad, se recomienda contar con un inventario de toda la infraestructura necesaria para el funcionamiento del servicio y evaluar qué componentes son los que tienen más probabilidad de fallo, para comenzar a aplicar la redundancia.

Cabe mencionar que existen arquitecturas de software que facilitan la redundancia de los elementos más utilizados de un servicio de interoperabilidad, como los microservicios.

7.2 PRUEBAS DE RENDIMIENTO

Es recomendable que los servicios de interoperabilidad sean sometidos a un conjunto de pruebas de rendimiento para verificar su escalabilidad, fiabilidad y uso de recursos. Se recomienda utilizar los siguientes tipos:

- Pruebas de carga: realizadas para monitorear el comportamiento de la aplicación bajo una cantidad de peticiones alta. Esto nos permite conocer el límite de peticiones que pueden ser respondidas, lo que a su vez permitirá establecer un límite de consultas o utilizar un balanceador de carga, para mejorar el rendimiento del servicio de interoperabilidad evitando su interrupción para los consumidores.
- Pruebas de estrés: con estas pruebas se puede verificar que el servicio de interoperabilidad responda de manera adecuada cuando sobrepasa las condiciones normales de consumo.

Con base en las mediciones de los resultados de las pruebas de rendimiento (carga y estrés), tomar decisiones en cuanto a los elementos que necesitarán redundancia, ya sean de software o hardware.

Además es posible verificar el rendimiento de los servicios de interoperabilidad realizando un análisis de los tiempos de respuesta en los registros de eventos.

7.3 BALANCEO DE CARGA

La infraestructura encargada de proveer los servicios de interoperabilidad debe tener la capacidad de distribuir el trabajo entre los recursos con los que cuenta, a fin de evitar problemas en el momento de gestionar una cantidad considerable de solicitudes. Esta necesidad puede ser satisfecha con servidores de proxy reverso (reverse proxy), balanceadores de carga, enrutadores o grupos de servidores (clusters).

Se recomienda aplicar el balanceo de carga en los servicios de interoperabilidad que se espera tengan una cantidad alta de entidades consumidoras. Hay que evaluar la cantidad de solicitudes que el servicio de interoperabilidad puede manejar en base a pruebas de rendimiento y de acuerdo a ese límite establecer nuevos recursos que permitan manejar una mayor cantidad de solicitudes.

Si bien esto aumentará la cantidad de solicitudes que se puede manejar, es conveniente revisar si el servicio de interoperabilidad no tiene algún problema que evite que pueda responder a más solicitudes, como conexiones no cerradas a la base de datos, no limpiar recursos en la memoria, consultas lentas a la base de datos u otros que pudieran estar afectando el rendimiento del servicio de interoperabilidad. La principal desventaja es que se necesita una mayor configuración para poner en marcha el balanceo de carga y el costo que esto implica.

SECCIÓN 8
POLÍTICAS

8.1 ASPECTOS LEGALES

Los aspectos legales que enmarcan la presente normativa se desprenden de la norma jurídica creadora de la institución reguladora de los proyectos y contratos constituidos bajo la modalidad de Alianza Público-Privada (Superintendencia de Alianza Público-Privada, SAPP), norma legal misma, que con su carácter general se vuelve aplicable a todos los agentes regulados implicando de esa manera su estricto cumplimiento al tenor de lo establecido en la Ley de Promoción de Alianza Público-Privada, su Reglamento y en los respectivos contratos:

8.2 OBLIGACIONES

Las obligaciones de los agentes regulados así como las obligaciones del Ente Regulador nacen de la Ley y de los Contratos, la inobservancia a dichos cuerpos legales constituye motivo para la aplicación de sanciones contractuales, administrativas u otras que las leyes aplicables establezcan para la eficaz regulación de los proyectos y contratos cuyos objetivos sean la construcción de infraestructura y prestación de servicios públicos.

8.3 RESPONSABILIDADES

Los agentes regulados deberán brindar todas las facilidades necesarias para que se ejecuten las facultades de supervisión y consecuente regulación por parte de la Superintendencia de Alianza Público-Privada, garantizando en todo caso, el resguardo de la confidencialidad de la información, misma que deberá ser íntegra y fidedigna. En caso contrario podrán ser objeto de sanción administrativa y, cuando así corresponda de denuncia ante el Ministerio Público.

8.4 VIGENCIA

La presente Normativa es de acción inmediata y su vigencia será por tiempo indefinido volviéndose de estricto cumplimiento a partir de la fecha en que se haga del conocimiento del agente regulado.

SECCIÓN 9
CATÁLOGO DE SERVICIOS

El catálogo de servicios deberá ser consultado en línea, accediendo al Sistema de Recolección de Datos de la SAPP (SRD-SAPP), el cual muestra un Panel con el listado de los diferentes “modelos de datos/mantas de datos” que se solicitan a los diferentes agentes regulados. Vea la sección de anexos, la sección 13.1, los instructivos técnicos para tener una idea clara de cómo ver el catálogo de modelo de datos.
Sección 10

SECCIÓN 10
TÉRMINOS Y DEFINICIONES

Agente Regulado. Entiéndase por agente regulado todas aquellas personas naturales o jurídicas relacionadas directa o indirectamente con la ejecución de obras públicas y/o prestación de servicios públicos bajo la modalidad de alianza público privada, es decir: concesionarios, supervisores, banco fiduciario, etc.
Algoritmo. Conjuntos de reglas definidas para encontrar la solución a un problema.
API. Es un conjunto de reglas y especificaciones que los programas de software pueden seguir para comunicarse entre ellos.
Administrador de APIs. Api Gateway, servicio administrable que permite la publicación, mantenimiento y monitoreo de servicios web. Es un punto único de entrada para todos los clientes que permite el redireccionamiento de las solicitudes a uno o varios servicios internos.
Autenticación. Característica que permite identificar y validar la identidad de un usuario, servicio o proceso.
Autorización. Es el proceso de dar permisos a un usuario para realizar alguna acción.
Confidencialidad. Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
Datos. Caracteres, números o símbolos recogidos para su tratamiento informático, análisis estadístico o referencia.
Dato Sensible. Se entiende por datos sensibles aquellos que contienen información vinculada a la privacidad, intimidad, honra, honor, propia imagen, dignidad, información de sectores económicos estratégicos e información catalogada como secreta, reservada o confidencial, cuya divulgación, de alguna manera, afecte a su titular o al Estado Hondureño.
Disponibilidad. Propiedad de acceso y uso de información a entidades autorizadas cuando estas lo requieran.
Entidad publicadora. Entidad responsable de la publicación del servicio de interoperabilidad.
Entidad consumidora. Entidad consumidora del servicio de interoperabilidad.
Idempotencia. Es la propiedad que indica que en caso de realizarse la misma solicitud varias veces a un servicio de interoperabilidad el resultado será el mismo en cuanto al estado del sistema.
Integridad. Propiedad que salvaguarda la exactitud y completitud de la información.
Interoperabilidad. Es la capacidad de intercambiar y compartir datos entre sistemas o

Componentes informáticos.

Metadatos. Son los datos que describen la calidad, contenido, condición y otras características de otros datos.

No repudio. Garantía de que un mensaje electrónico de datos o un documento digital ambos firmados digitalmente, no puedan ser negados en su autoría y contenido.

Portal Web. Es una fuente de información que provee el acceso a una serie de recursos y servicios relacionados a un mismo tema.

Punto único de fallo. Es una parte del sistema que en caso de fallar detendría el funcionamiento de todo el sistema. Puede ser cualquier dispositivo de red, servidor, software u otro.

Semántica. Significado de una unidad lingüística. En interoperabilidad es el significado o interpretación de los datos.

Servicio de interoperabilidad. Es cualquier servicio ofrecido a través de la red, diseñado para soportar interacción máquina a máquina para el intercambio de datos.

Trazabilidad. Capacidad de llevar un registro de las acciones y eventos de un sistema, servicio y/o proceso.

URI. Uniform Resource Identifier o identificador uniforme de recursos, sirve para identificar recursos en una red (internet).

SRD-SAPP. Sistema de Recolección de Datos de la SAPP

JSON. JavaScript Object Notation, por sus siglas en inglés, es un formato de texto ligero para el intercambio de datos.

Versionamiento. El versionado de servicios es una práctica por la cual, al producirse un cambio en el API de un servicio (no tiene por qué ser únicamente un API REST), se libera una nueva versión de ese servicio de manera que la versión nueva y la anterior conviven durante un periodo de tiempo.

Agentes regulados. Se consideran Agentes, las distintas dependencias del Estado y las personas jurídicas de naturaleza privada, que contractualmente intervengan en un modelo de participación público privada, entre estos, los descritos en el Artículo uno de este Reglamento, y cualquier otro que a criterio de La SAPP sea calificado como tal.

SECCIÓN 11
ANEXOS

11.1.1 CONFIGURACIÓN CLIENTE SSL VPN

Puede instalar el software VPN móvil con software cliente SSL en equipos con estos sistemas Operativos:

- Microsoft Windows XP SP2 (32 bits)
- Microsoft Windows 7 y 8 (32 bits y 64 bits)
- Microsoft Windows Server 2003 (32 bits)
- Mac OS X v10.6, v10.7, v10.8, v10.9

Si el equipo cliente tiene Windows XP, debe iniciar sesión con una cuenta que tenga derechos de administrador para instalar Mobile VPN con software de cliente SSL.

Los derechos de administrador no son necesarios para conectarse después de que el cliente SSL ha sido instalado y configurado. En Windows XP Professional, el usuario debe ser miembro del grupo Operadores de configuración de red para ejecutar el cliente SSL.

Si el equipo cliente tiene Mac OS X, no se requieren derechos de administrador para instalar o utilizar el cliente SSL.

11.1.2 DESCARGUE EL SOFTWARE DEL CLIENTE

- Windows: WG-MVPN-SSL.exe
- Mac: WG-MVPN-SSL_11_12_4.dmg

https://drive.google.com/open?id=0BxyTjmpR2oalaUhhNEhmaUNzbUk

11.1.3 INSTALAR EL SOFTWARE DEL CLIENTE

Para Microsoft Windows:

1. Haga doble clic en WG-MVPN-SSL.exe.
2. Se inicia el Mobile VPN with SSL Client Setup Wizard.
3. Acepte la configuración predeterminada en cada pantalla del asistente.
4. Si desea agregar un icono de escritorio o un icono de inicio rápido, seleccione la casilla
5. de verificación del asistente que coincida con la opción. No es necesario un icono de escritorio o de inicio rápido.
6. Finalizar y salir del asistente.

Para Mac OS X:

1. Haga doble clic en WG-MVPN-SSL.dmg.
2. Se crea un volumen llamado WatchGuard Mobile VPN en su escritorio.
3. En el volumen de WatchGuard Mobile VPN, haga doble clic en WatchGuard Mobile VPN con SSL Installer <version> .mpkg.
4. Se inicia el instalador del cliente.
5. Acepte los ajustes predeterminados en cada pantalla del instalador.
6. Termine y salga del instalador.
7. Después de descargar e instalar el software cliente, el software de cliente VPN móvil se conecta automáticamente al dispositivo XTM. Cada vez que se conecta al dispositivo XTM, el software cliente comprueba si hay actualizaciones de configuración.

11.1.4 OTRAS OPCIONES DE CONEXIÓN

Hay otras dos opciones de conexión disponibles en el cliente sólo si el administrador las ha habilitado en el dispositivo al que se conecta.

Volver a conectar automáticamente

Active la casilla de verificación Reconectar automáticamente si desea que la VPN móvil con cliente SSL se vuelva a conectar automáticamente cuando se pierda la conexión.

Recordar contraseña

Seleccione la casilla de verificación Recordar contraseña si desea que la VPN móvil con cliente SSL recuerde la contraseña que escribió para la próxima vez que se conecte.

11.1.5 VPN MÓVIL CON CONTROLES DE CLIENTE SSL

Cuando se ejecuta la VPN móvil con cliente SSL, aparece el icono de VPN de WatchGuard Mobile con SSL en la bandeja del sistema (Windows) o en el lado derecho de la barra de menús (Mac OS X). El estado de la conexión VPN se muestra por el aspecto de la lupa del icono.

Icono	Significado de estado
	La conexión VPN no está establecida.
	Se ha establecido la conexión VPN. Puede conectarse de forma segura a los recursos detrás del dispositivo XTM.
	El cliente está en proceso de conexión o desconexión.

Para ver la lista de controles del cliente, haga clic con el botón derecho en el icono VPN móvil con SSL en la bandeja del sistema (Windows) o haga clic en el icono VPN móvil con SSL en la barra de menús (Mac OS X). Puede elegir entre estas acciones:

- **Conectar / desconectar:** Inicie o detenga la VPN móvil con conexión SSL.
- **Estado:** Consulte el estado de la VPN móvil con conexión SSL.
- **Ver los registros:** Abra el archivo de registro de conexión.
- **Propiedades:** Windows - Seleccione Iniciar programa en inicio para iniciar el cliente cuando se inicie Windows. Escriba un número para el nivel de registro para cambiar el nivel de detalle incluido en los registros. Mac OS X - muestra información detallada sobre la VPN móvil con conexión SSL. También puede establecer el nivel de registro.
- **Acerca de:** Se abre el cuadro de diálogo WatchGuard Mobile VPN con información sobre el software cliente.
- **Salir (Windows) o Salir (Mac OS X):** Desconecta del dispositivo XTM y apague el cliente.

11.2 ACCEDIENDO AL PORTAL WEB DEL SRD-SAPP

Una vez haya configurado y aplicado el acceso de su VPN así como se describe en el Anexo 13.1 Configuración Cliente SSL VPN, debe dirigirse al portal Web del Sistema de Recolección de Datos de la SAPP (SRD-SAPP), aquí encontrará todas las mantas/modelos de datos que se le solicitan.

Para acceder al portal web debe seguir los siguientes pasos:

1. Conectar su cliente VPN, junto con las credenciales de acceso que le ha enviado La SAPP.
2. Utilizar un navegador Web, preferiblemente Chrome en sus versiones más recientes, puede utilizar también Firefox, Edge o Safari pero no se recomienda.
3. Acceder a la dirección WEB http://192.168.60.251/
4. Aparecerá la pantalla de inicio de sesión, aquí deberá usar las credenciales de acceso que la SAPP le ha enviado y que son para el acceso al Sistema de Recolección de Datos (SRD-SAPP)
5. Al autenticarse correctamente, el sistema lo redirigirá al “Panel principal/Dashboard” que muestra los diferentes modelos de datos (Mantas de datos) que se le solicitan, y el estado de envío de los mismos.
6. Puede hacer click en cada uno de los Modelos de datos de su Dashboard para ingresar a ver los detalles como ser:
    a. Nombre
    b. Descripción
    c. Campos que se solicitan:
        i. Formato
        ii. Orden
        iii. Validaciones
    d. Periodicidad de carga
    e. Descripción de carga por medio de API Restful
    f. Sección para la carga manual por medio de un archivo de Excel.

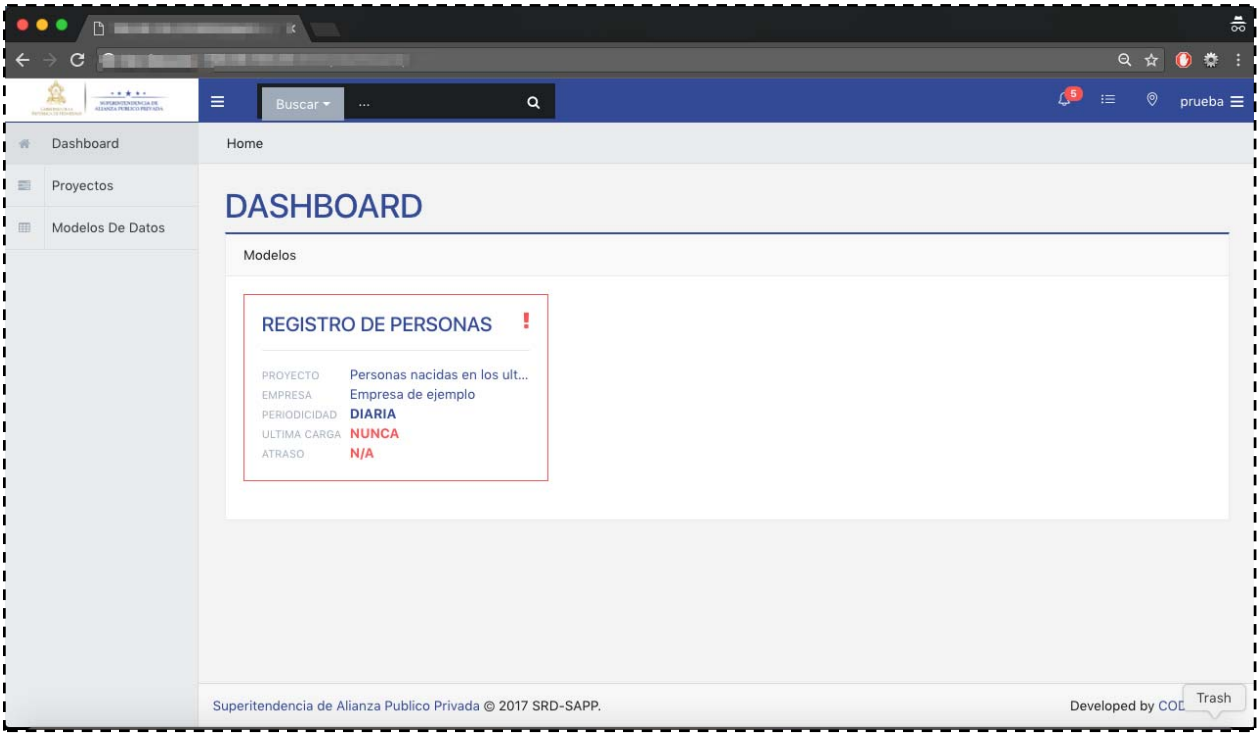
11.3 INSTRUCTIVO TÉCNICO

Una vez ha identificado el modelo de datos que desea cargar al sistema, deberá desarrollar los procedimientos y algoritmos necesarios para la integración y automatización con los servicios Web SAPP, considerando los tiempos de carga (Periodicidad), Campos solicitados (formato, restricciones y ordenamiento) que se describen en el detalle de cada modelo en el portal Web.

Considerando el siguiente ejemplo, en el cual se solicita la carga de datos de registros de personas nacidas entre los años 1988 y 2018, describimos el modelo de datos de la siguiente manera:

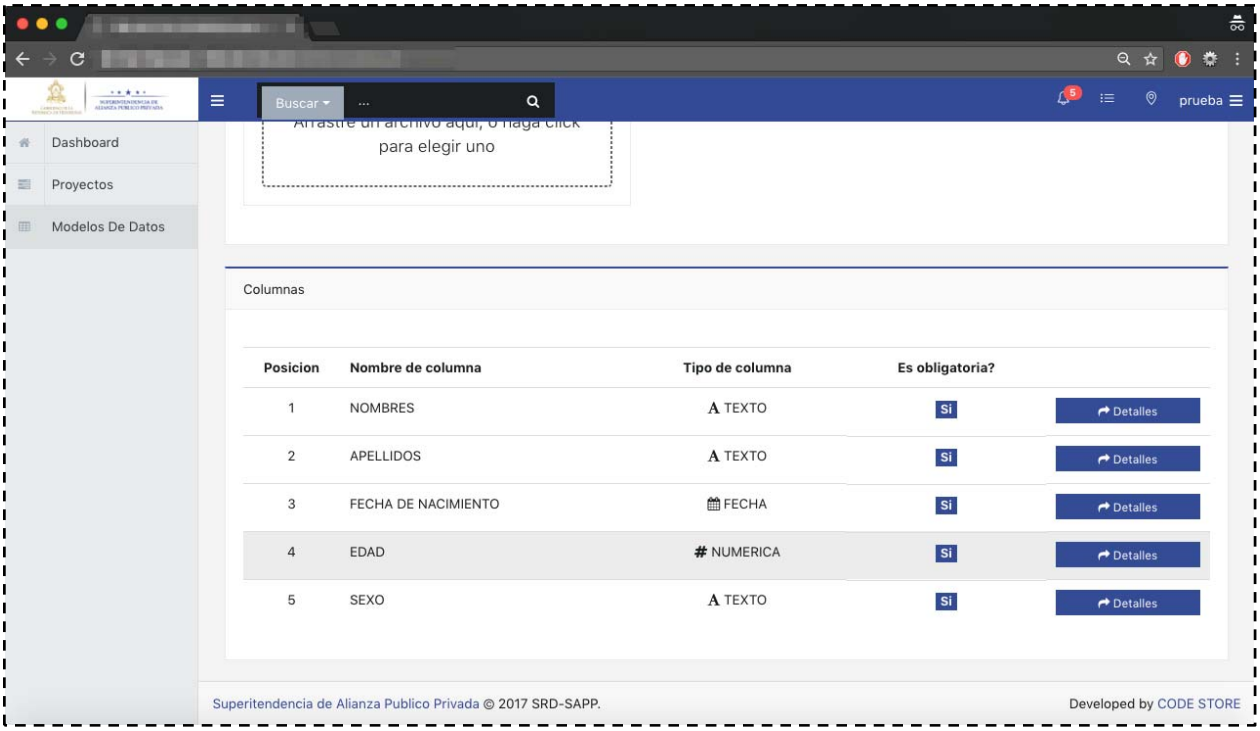
Orden	Nombre del campo	Tipo de campo	Restricciones
1	Nombres	TEXTO	Expresión regular: `^[a-zA-Z áÁéÉíÍóÓúÚ]+$`
2	Apellidos	TEXTO	Expresión regular: `^[a-zA-Z áÁéÉíÍóÓúÚ]+$`
3	Fecha de nacimiento	FECHA	Mínimo: 1988-01-01 Máximo: 2018-12-31
4	Edad	NUMÉRICO	Mínimo: 1 Máximo: 30
5	Sexo	TEXTO	Lista de valores definidos: - masculino - femenino

Pantalla Dashboard



Detalle de un modelo de datos

Detalle de los campos solicitados



Detalles de las restricciones de cada campo/columna


Columna Fecha
Nombre *
FECHA DE NACIMIENTO
Obligatoria *
Si
Usar Hora? *
No
Fecha minima
01/01/1988
Fecha maxima
31/12/2018
Opciones
Cerrar


Columna Numerica
Nombre *
EDAD
Obligatoria *
Si
Valor minimo
1
Valor maximo
30
Decimales *
0
Opciones
Cerrar

11.3.1 INSTRUCTIVO CARGA MEDIANTE API RESTFUL

Una vez haya visualizado los detalles del modelo de datos/manta de datos que desea implementar la carga mediante la API Restful, siguiente el ejemplo del modelo de datos “Registro de personas”, le brindamos unos ejemplos de diferentes estructuras en diferentes lenguajes que realiza el POST a la API del modelo de datos.

11.3.1.1 EJEMPLOS DE LA PETICIÓN POST

HTTP

```
POST /api/modelos/1/cargar/json HTTP/1.1
Host: 127.0.0.1
Content-Type: application/json
Authorization: Basic c3JkX2FkbWluOlNhcHAxMjMk
Cache-Control: no-cache

[{
"col0" : "Carmen Amarillis",
"col1" : "Lara Espinoza",
"col2" : "1988-11-13",
"col3" : "29",
"col4" : "femenino"
},{
"col0" : "Wilfredo 25",
"col1" : "$Rodriguez",
"col2" : "2020-02-14",
"col3" : 25.99,
"col4" : "no sabe"
}]
```

Usando PHP con HttpRequest

```
<?php

$request = new HttpRequest();
$request->setUrl('http://127.0.0.1/api/modelos/1/cargar/json');
$request->setMethod(HTTP_METH_POST);

$request->setHeaders(array(
  'Cache-Control' => 'no-cache',
  'Authorization' => 'Basic c3JkX2FkbWluOlNhcHAxMjMk',
  'Content-Type' => 'application/json'
));

$request->setBody('[{
"col0" : "Carmen Amarillis",
"col1" : "Lara Espinoza",
"col2" : "1988-11-13",
"col3" : "29",
"col4" : "femenino"
},{
"col0" : "Wilfredo 25",
"col1" : "$Rodriguez",
"col2" : "2020-02-14",
"col3" : 25.99,
"col4" : "no sabe"
}]');

try {
  $response = $request->send();

  echo $response->getBody();
} catch (HttpException $ex) {
  echo $ex;
}
```

Usando PHP con CURL

```
<?php

$curl = curl_init();

curl_setopt_array($curl, array(
  CURLOPT_PORT => "80",
  CURLOPT_URL => "http://127.0.0.1/api/modelos/1/cargar/json",
  CURLOPT_RETURNTRANSFER => true,
  CURLOPT_ENCODING => "",
  CURLOPT_MAXREDIRS => 10,
  CURLOPT_TIMEOUT => 30,
```

```
  CURLOPT_HTTP_VERSION => CURL_HTTP_VERSION_1_1,
  CURLOPT_CUSTOMREQUEST => "POST",
  CURLOPT_POSTFIELDS => "[{\n\"col0\" : \"Carmen
Amarillis\",\n\"col1\" : \"Lara Espinoza\",\n\"col2\" : \"1988-11-
13\",\n\"col3\" : \"29\",\n\"col4\" : \"femenino\"\n},{\n\"col0\" :
\"Wilfredo 25\",\n\"col1\" : \"$Rodriguez\",\n\"col2\" : \"2020-02-
14\",\n\"col3\" : 25.99,\n\"col4\" : \"no sabe\"\n}]",
  CURLOPT_HTTPHEADER => array(
    "Authorization: Basic c3JkX2FkbWluOlNhcHAxMjMk",
    "Cache-Control: no-cache",
    "Content-Type: application/json",
    "Postman-Token: 119f244e-4b92-5413-6032-e8e0796f94b4"
  ),
));

$response = curl_exec($curl);
$err = curl_error($curl);

curl_close($curl);

if ($err) {
  echo "cURL Error #:" . $err;
} else {
  echo $response;
}
```

Usando Python 3 con Http.Client

```
import http.client
import json

conn = http.client.HTTPConnection("127,0,0,0")

payload = json.dumps(
[{
"col0" : "Carmen Amarillis",
"col1" : "Lara Espinoza",
"col2" : "1988-11-13",
"col3" : "29",
"col4" : "femenino"
},{
"col0" : "Wilfredo 25",
"col1" : "$Rodriguez",
"col2" : "2020-02-14",
"col3" : 25.99,
"col4" : "no sabe"
}]
```

```
)

headers = {
    'Content-Type': "application/json",
    'Authorization': "Basic c3JkX2FkbWluOlNhcHAxMjMk",
    'Cache-Control': "no-cache",
    }

conn.request("POST", "api,modelos,1,cargar,json", payload, headers)

res = conn.getresponse()
data = res.read()

print(data.decode("utf-8"))
```

Usando Python con Requests

```
import requests
import json

url = "http://127.0.0.1/api/modelos/1/cargar/json"

payload = json.dumps(
[{
"col0" : "Carmen Amarillis",
"col1" : "Lara Espinoza",
"col2" : "1988-11-13",
"col3" : "29",
"col4" : "femenino"
},{
"col0" : "Wilfredo 25",
"col1" : "$Rodriguez",
"col2" : "2020-02-14",
"col3" : 25.99,
"col4" : "no sabe"
}]
)
headers = {
    'Content-Type': "application/json",
    'Authorization': "Basic c3JkX2FkbWluOlNhcHAxMjMk",
    'Cache-Control': "no-cache",
    }

response = requests.request("POST", url, data=payload,
headers=headers)
```

```
print(response.text)
```

Usando Java con OK HTTP

```
OkHttpClient client = new OkHttpClient();

MediaType mediaType = MediaType.parse("application/json");
RequestBody body = RequestBody.create(mediaType, "[{\n\"col0\" :
\"Carmen Amarillis\",\n\"col1\" : \"Lara Espinoza\",\n\"col2\" :
\"1988-11-13\",\n\"col3\" : \"29\",\n\"col4\" :
\"femenino\"\n},{\n\"col0\" : \"Wilfredo 25\",\n\"col1\" :
\"$Rodriguez\",\n\"col2\" : \"2020-02-14\",\n\"col3\" :
25.99,\n\"col4\" : \"no sabe\"\n}]");
Request request = new Request.Builder()
  .url("http://127.0.0.1/api/modelos/1/cargar/json")
  .post(body)
  .addHeader("Content-Type", "application/json")
  .addHeader("Authorization", "Basic c3JkX2FkbWluOlNhcHAxMjMk")
  .addHeader("Cache-Control", "no-cache")
  .build();

Response response = client.newCall(request).execute();
```

11.3.1.2 EJEMPLOS DE DIFERENTES ERRORES DE VALIDACIÓN NO SUPERADOS

Credenciales fallidas

Status: **403 Forbidden**

```
{
    "error": "Nombre de usuario/contraseña inválidos."
}
```

Modelo de datos no encontrado

Status: **404 Not found**

```
{
    "error": "No encontrado."
}
```

Sin permisos

Status: **403 Forbidden**

```
{
    "error": "Usted no tiene permiso para realizar esta acción."
}
```

Tipo de medio incorrecto

Status: **415 Unsupported Media Type**

```
{
    "error": "Tipo de medio \"text/plain\" incompatible en la
solicitud."
}
```

Errores en los datos enviados

Status: **400 Bad Request**

```
{
    "error": "Una o mas filas contienen errores de validacion",
    "detalle": [
        {
            "numero": "0",
            "datos": {
                "col0": "Carmen Amarillis",
                "col1": "Lara Espinoza",
```

```
                "col2": "1988-11-13",
                "col3": "29",
                "col4": "femenino"
            },
            "errores": {
                "col4": [
                    "\"femenino\" no es una elección válida."
                ]
            }
        },
        {
            "numero": "1",
            "datos": {
                "col0": "Wilfredo 25",
                "col1": "$Rodriguez",
                "col2": "2020-02-14",
                "col3": "25.99",
                "col4": "no sabe"
            },
            "errores": {
                "col0": [
                    "Este valor no coincide con el patrón requerido."
                ],
                "col1": [
                    "Este valor no coincide con el patrón requerido."
                ],
                "col2": [
                    "Asegúrese de que este valor es menor o igual a
2018-12-31."
                ],
                "col3": [
                    "Asegúrese de que no haya más de 0 decimales."
                ],
                "col4": [
                    "\"no sabe\" no es una elección válida."
                ]
            }
        }
    ]
}
```


Carga exitosa

Status: **200 Ok**


```
{
    "filas_cargadas": 2
}
```

El servidor ha fallado

Status: **500 Internal Server Error**

```
Aquí el valor de retorno es html.
```

11.3.2 INSTRUCTIVO CARGA MANUAL

Una vez haya accedido a los detalles del Modelo de datos/Manta de datos que desea realizar la carga manual, deberá identificar la sección en un recuadro con la leyenda "*Arrastre un archivo aquí, o haga click para elegir uno*", para éste ejemplo vamos a usar el Modelo de datos llamado "REGISTRO DE PERSONAS":

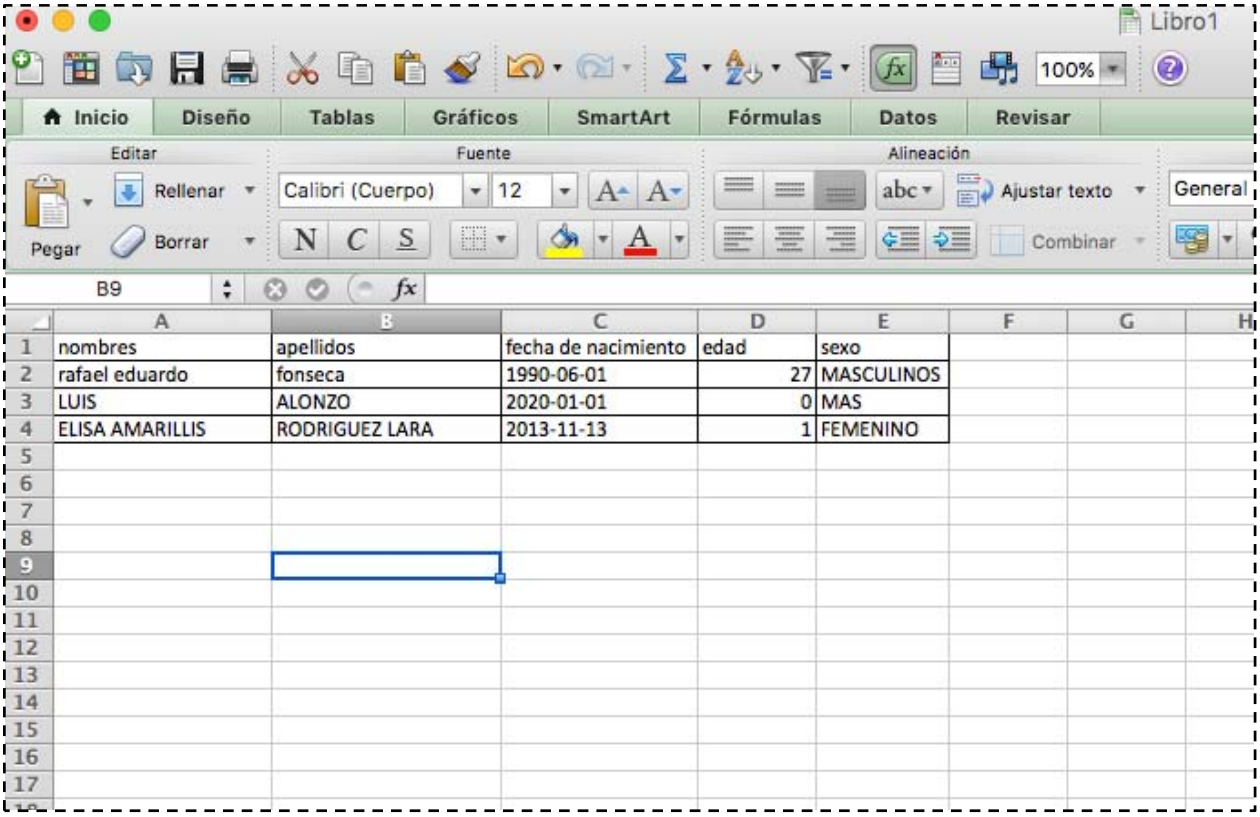
Cuando ubique la misma sección así como se muestra en la imagen anterior, tiene 2 opciones, arrastrar el archivo de Excel con los datos, o hacer clic en el control para que le muestre un explorador y ubique el Excel que desea cargar.

Especificaciones del archivo de Excel

Debe considerar los siguientes detalles para el archivo de Excel que tiene los datos a cargar en el sistema:

1. La primera línea del archivo tiene los nombres de las columnas solicitadas en el detalle del Modelo de datos del SRD-SAPP
2. El orden de las columnas debe coincidir con el ordenamiento descrito en el Modelo de datos en el SRD-SAPP
3. Se espera solamente 1 pestaña por archivo de Excel, y debe ser la primera pestaña.
4. Se espera que el archivo de Excel no tenga fragmentación entre sus líneas de datos, es decir, no pueden haber columnas o líneas completas vacías. En el caso de columnas "no requeridas" puede estar vacías.
5. Todos los campos deben estar formateados como "texto", exceptuando los numéricos.

Excel ejemplo



	A	B	C	D	E
1	nombres	apellidos	fecha de nacimiento	edad	sexo
2	rafael eduardo	fonseca	1990-06-01	27	MASCULINOS
3	LUIS	ALONZO	2020-01-01	0	MAS
4	ELISA AMARILLIS	RODRIGUEZ LARA	2013-11-13	1	FEMENINO

Descripción de las validaciones al cargar

Una vez haya seleccionado el archivo que desea cargar, el sistema mostrará un botón que dice “Cargar archivo”, si considera que seleccionó el archivo incorrecto, debe hacer clic en el texto “Escoger otro archivo”.

Los siguientes son ejemplo de cómo se muestran los errores mediante la carga manual:

Al colocar el cursor sobre la celda con error, el sistema muestra un “tooltip” que describe la validación que no ha pasado.

SECCIÓN 12
DESTRUCCIÓN, ROBO, HURTO O EXTRAVÍO DEL EQUIPO CON ACCESO

El agente regulado poseedor de equipo de cómputo con acceso autorizado al Sistema de Recolección de Datos de la Superintendencia de Alianza Público Privada (SDR SAPP) tiene la obligación de reportar a la Superintendencia de Alianza Público Privada la destrucción, robo, hurto o extravío del equipo con acceso bajo su posesión dentro del término de (2) dos días calendario, para que la Superintendencia proceda de forma inmediata a inhabilitar el acceso al equipo reportado.

Para los casos de robo, hurto o extravío deberá interponer la denuncia ante la Dirección Policial de Investigación (DPI) dentro del término de veinticuatro (24) horas después de haber ocurrido el siniestro. La omisión a la presente disposición dará lugar a la deducción de responsabilidad administrativa, civil o penal a la que hubiese lugar por parte del poseedor autorizado del equipo reportado.

SECCIÓN 13
EXIMENTE DE RESPONSABILIDAD

Siendo que la Sección 7 “Disponibilidad” establece que la Superintendencia de Alianza Público Privada garantiza que el servicio de interoperabilidad esté cien por ciento disponible de forma continua y sin interrupción, no será imputable a los agentes regulados el no envío de información requerida de conformidad a la dinámica establecida para tales efectos según la presente

normativa, cuando la imposibilidad de enviar dicha información sea originada por motivos de fuerza mayor o caso fortuito fehacientemente comprobables.

SECCIÓN 14
PERÍODO PARA LA IMPLEMENTACIÓN DE LA NORMATIVA

A partir de la vigencia de la presente normativa, la Superintendencia de Alianza Público Privada concede a los agentes regulados el término de treinta (30) días calendario para su implementación.

SECCIÓN 15
PENALIDADES POR INCUMPLIMIENTO A LA PRESENTE NORMATIVA

Cualquier incumplimiento por acción u omisión en lo que respecta al contenido de las presentes disposiciones a partir de su vigencia o en la etapa de implementación a la que se hace referencia en la Sección que antecede, dará lugar a la imposición de las sanciones correspondientes de conformidad a lo dispuesto en el Reglamento para la Aplicación de Sanciones de la Superintendencia Público Privada disponible en el siguiente enlace: http://sapp.gob.hn/wp-content/uploads/2016/10/reglamento_sanciones_sapp.pdf

SEGUNDO: Comunicar la presente resolución a los Agentes Regulados relacionados con la realización de obras o prestación de servicios mediante Alianza Público-Privada.

TERCERO: La presente Resolución de acción inmediata y entrará en vigencia a partir de su publicación en el sitio web de la Superintendencia de Alianza Público Privada.- Queda aprobado por unanimidad.- (F) DAVID IGNACIO WILLIAMS GUILLÉN, Superintendente Presidente; EMILIO CABRERA CABRERA, Superintendente; CARLOS ALEJANDRO PINEDA PINEL, Superintendente; RAMÓN ECHEVERRÍA LÓPEZ, Secretario General.