ANEXO A

Requerimientos básicos en la gestión de la seguridad de la información

Los siguientes requerimientos, son los considerados básicos para la gestión de la seguridad de la información al momento de iniciar las operaciones como Operador de Servicios Electrónicos, por lo que deben ser de cumplimiento obligatorio y han sido seleccionados de la Norma Internacional ISO/IEC 27002 – 2013 Code of Practice for Information Security Controls.

La guía de implementación de la referida norma, deberá ser tomada en cuenta de forma imperativa, para el propósito de cumplimiento de estos requerimientos.

Ámbito/Categoría/Control

5. POLÍTICAS DE SEGURIDAD

5.1 Dirección de la Gerencia para la seguridad de la información.
Objetivo: Proporcionar dirección y apoyo de la gerencia para la seguridad de la información en concordancia con los requisitos del negocio y las leyes y regulaciones relevantes.

5.1.1 Políticas para la seguridad de la información.
Conjunto de políticas para la seguridad de la información que deberán ser definidas y aprobadas por la gerencia, publicadas y comunicadas a los empleados y a las partes externas relevantes.

5.1.2 Revisión de las políticas de seguridad de la información.
Las políticas para la seguridad de la información deben ser revisadas a intervalos planificados o si ocurren cambios significativos para asegurar su conveniencia, adecuación y continua efectividad.

6. ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION

6.1Organización interna.
Objetivo: establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.

6.1.1 Roles y responsabilidad de seguridad de la información.
Todos los roles y responsabilidades de seguridad de la información deberán estar definidas y asignados.

6.1.2 Segregación de deberes o funciones.
Las funciones y áreas de responsabilidad que pudieran entrar en conflicto, deben ser segregadas para reducir oportunidades de modificación no autorizada o no intencional, o por el mal uso de los activos de la organización.

6.2 Dispositivos móviles y teletrabajo.
Objetivo: Asegurar la seguridad del teletrabajo y el uso de los dispositivos móviles.

6.2.1 Política de dispositivos móviles.
Contar con políticas y medidas de seguridad de soporte que deberán ser adoptadas para gestionar los riesgos introducidos por el uso de dispositivos móviles.

7. SEGURIDAD DE LOS RECURSOS HUMANOS

7.1 Antes del empleo.
Objetivo: Asegurar que los empleados y contratistas entienden sus responsabilidades y son competentes para los roles que se les ha asignado.

7.1.1 Selección.
Las verificaciones de los antecedentes de todos los candidatos a ser empleados deberán ser llevadas a cabo en concordancia con las leyes, regulaciones y ética relevantes, los que deberán ser ~~en~~ un número proporcional a las necesidades del negocio, a la clasificación de la información a la que se tendrán acceso y a los riesgos percibidos.

7.1.2 Términos y condiciones del empleo.
Los acuerdos contractuales con los empleados y contratistas deben contemplar las responsabilidades de éstos y de la organización respecto de la seguridad de la información.

Ámbito/Categoría/Control

7.2 Durante el empleo.

Objetivo: Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.

7.2.1 Responsabilidad de la Alta Gerencia.

La gerencia debe requerir a todos los empleados y contratistas aplicar la seguridad de la información en concordancia con las políticas y procedimientos establecidos por la organización.

7.2.2 Conciencia, educación y capacitación sobre la seguridad de la información.

Todos los empleados de la organización, y cuando fuera relevante, los contratistas, deben recibir educación y capacitación sobre la conciencia de la seguridad de la información; así como actualizaciones regulares sobre las políticas y procedimientos de la organización, acorde con la función del trabajo que cumplen.

7.2.3 Proceso disciplinario.

Se deberá contar con un proceso disciplinario formal y comunicarlo, para tomar acción contra empleados que hayan cometido una infracción a la seguridad de la información.

7.3 Terminación y cambio de empleo.

Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.

7.3.1 Terminación o cambio de responsabilidades del empleo.

Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos luego de la terminación o cambio de empleo, deberán ser definidos, comunicados al empleado o contratista y forzar su cumplimiento.

8. GESTIÓN DE ACTIVOS

8.3 Manejo de los medios de almacenamiento.

Objetivo: Prevenir la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en medios.

8.3.2 Disposición de medios.

La información y sus medios de almacenamiento deberán eliminarse mediante procedimientos formales, cuando ya no se requieran.

9. CONTROL DE ACCESOS

9.1 Requisitos de la empresa para el control de accesos.

Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la información.

9.1.1 Política de control de accesos.

Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de la seguridad de la información.

9.2 Gestión de acceso de usuario.

Objetivo: Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.

9.2.1 Registro y baja de usuarios.

Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de acceso.

9.2.2 Aprovisionamiento de acceso a usuarios.

Un proceso formal de aprovisionamiento de acceso a usuarios deberá ser implementado para asignar o revocar los derechos de acceso, de todos los tipos de usuarios para todos los sistemas y servicios.

9.2.3 Gestión de los derechos de acceso privilegiados.

La asignación y uso de derechos de acceso privilegiado debe ser restringida y controlada.

9.2.5 Revisión de derechos de acceso de usuarios.

Los propietarios de los activos deben revisar los derechos de acceso de usuarios en intervalos regulares de tiempo.

9.4 Control de acceso a sistemas y aplicaciones.

Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.

9.4.1 Restricción del acceso a la información.

El acceso a la información y a las funciones del sistema de aplicación debe ser restringido, en concordancia con la política de control de acceso.

9.4.3 Sistema de Gestión de contraseñas.

Ámbito/Categoría/Control
Los sistemas de gestión de contraseñas deben ser interactivos y asegurar contraseñas de calidad.
9.4.5 Control de acceso al código fuente de los programas. El acceso al código fuente de los programas debe ser restringido
10. CRIPTOGRAFIA
10.1 Controles criptográficos. Objetivo: Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.
10.1.1 Política de uso de los controles criptográficos. Contar con una política sobre el uso de controles criptográficos para la protección de la información
10.1.2 Gestión de claves. Contar con una política sobre el uso, protección y tiempo de vida de las claves criptográficas a través de todo su ciclo de vida.
11. SEGURIDAD FÍSICA Y AMBIENTAL
11.1 Áreas seguras. Objetivo: Impedir el acceso físico no autorizado, daño e interferencia a la información, así como a las instalaciones donde ésta es procesada.
11.1.1 Perímetro de seguridad física. Los perímetros de seguridad deben ser definidos y utilizados para proteger a las áreas que contienen información crítica o sensible y a las instalaciones donde se procesa dicha información.
11.1.2 Controles físicos de entrada. Las áreas seguras deben estar protegidas por medio de controles apropiados de ingreso, para asegurar que solo personal autorizado puede ingresar.
11.1.3 Asegurar áreas, oficinas e instalaciones. Se deberá diseñar e implementar mecanismos de seguridad en las oficinas, áreas e instalaciones, donde se almacena o se procesa la información.
11.1.4 Protección contra las amenazas externas y ambientales. Se deberá diseñar e implementar mecanismos de protección física contra desastres naturales, ataques maliciosos o accidentes
11.2 Equipamiento. Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos e interrupción de las operaciones de la organización.
11.2.7 Disposición (eliminación) o reutilización segura de equipos. Todos los elementos del equipo que contengan medios de almacenamiento deberán ser verificados para asegurar que cualquier dato sensible y software con licencia se haya eliminado o se haya sobre escrito de manera segura, antes de su puesta a disposición o reutilización
11.2.8 Equipo de usuario desantendido. Los usuarios deben asegurar que el equipo desatendido tenga la protección apropiada.
11.2.9 Política de escritorio limpio y pantalla limpia. Se debe adoptar una política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como una política de pantalla limpia para las instalaciones de procesamientos de la información.

Ámbito/Categoría/Control

12. SEGURIDAD EN LAS OPERACIONES

12.1 Procedimientos Operacionales y Responsabilidades.

Objetivo: Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.

12.1.1 Documentación de procedimientos operacionales.

Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que los necesitan.

12.1.2 Gestión de cambios.

Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afecten la seguridad de la información, deben ser controlados.

12.1.4 Gestión de la capacidad.

El uso de recursos debe ser monitoreado, afinado y se debe hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.

12.1.4 Separación de los ambientes de desarrollo, pruebas y operación.

Los entornos de desarrollo, pruebas y operaciones deben de estar separados para reducir los riesgos de acceso no autorizado o cambios al entorno operativo.

12.2 Protección contra código malicioso.

Objetivo: Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra códigos maliciosos.

12.2.1 Controles contra el código malicioso.

Se deberá implementar controles de detección, prevención y recuperación para proteger la información contra códigos maliciosos, en combinación con una concientización apropiada a de los usuarios.

12.3 Respaldo.

Objetivo: Proteger contra la pérdida de datos.

12.3.1 Respaldo de la información.

Se deberán realizar copias de respaldo de la información, del software y de las imágenes del sistema y probadas regularmente, en concordancia con una política de respaldo definida.

12.4 Registros y monitoreo.

Objetivo: Registrar eventos y generar evidencia.

12.4.1 Registro de eventos.

Se deberán producir, mantener y revisar regularmente los registros (logs) de eventos de actividades de usuarios, excepciones, fallas e incidencias de seguridad de la información.

12.4.4 Sincronización de relojes.

Los relojes de todos los sistemas de procesamiento de la información relevantes dentro de una organización o dominio de seguridad, deberán estar sincronizados a una fuente de tiempo de referencia única.

12.7 Consideraciones de auditoría de sistemas de información.

Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.

12.7.1 Controles de auditoría de sistemas de información.

Los requisitos de las auditorías y las actividades que involucran la verificación de sistemas operacionales deben ser cuidadosamente planificados y acordados para minimizar la interrupción de los procesos del negocio.

13. SEGURIDAD EN LAS TELECOMUNICACIONES

13.1 Gestión de la seguridad en las redes.

Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo.

13.1.1 Controles de red.

Las redes deberán ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.

13.2 Transferencia de información.

Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

13.2.1 Políticas y procedimientos de transferencia de información.

Deberá aplicarse políticas, procedimientos y controles de transferencia formales, para proteger la información a través del uso de todo tipo de instalaciones de comunicación.

Ámbito/Categoría/Control
13.2.4 Acuerdos de confidencialidad o no divulgación. Los requisitos para los acuerdos de confidencialidad o no divulgación, que reflejan las necesidades de la organización para la protección de la información, deberán ser identificados, revisados regularmente y documentados.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN
14.1 Requisitos de seguridad de los sistemas de información. Objetivo: Garantizar que la seguridad de la información es una parte integral de los sistemas de información a través del ciclo de vida completo. Esto también incluye los requisitos para sistemas de información que proporcionen servicios sobre redes públicas.
14.1.1 Análisis y especificación de los requisitos de seguridad de la información. Los requisitos relacionados a la seguridad de la información deberán ser incluidos dentro de los requisitos para nuevos sistemas de información o mejoras a los sistemas existentes.
14.1.3 Protección de transacciones en servicios de aplicación. La información involucrada en las transacciones de los servicios de aplicación debe ser protegida para prevenir la transmisión incompleta, ruteo incorrecto, alteración no autorizada de mensajes, divulgación no autorizada, duplicación o respuesta no autorizada de mensajes.
14.2 Seguridad en los procesos de desarrollo y soporte. Objetivo: Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
14.2.1 Política de desarrollo seguro de software. Los desarrollos de software y sistemas dentro de la organización deben contar con reglas establecidas.
14.2.9 Pruebas de aceptación del sistema. Los nuevos sistemas de información, actualizaciones y nuevas versiones, deben contar con programas de pruebas y criterios de aceptación.
15. RELACIONES CON PROVEEDORES
15.1 Seguridad de la información con el proveedor. Objetivo: Asegurar protección a los activos de la organización que son accesibles a los proveedores.
15.1.1 Política de seguridad de la información en las relaciones con el proveedor. Requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso por parte del proveedor a los activos de la organización deben estar acordados con el proveedor y ser documentados.
15.1.2 Abordar la seguridad dentro de los acuerdos con proveedores. Se debe establecer con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proveer componentes de infraestructura tecnológica para la información; todos los requisitos relevantes de seguridad de la informacion.
15.2 Gestión de entrega del servicio por proveedores. Objetivo: Mantener un nivel de seguridad de la información y entrega de servicios acordado en línea con los acuerdos con proveedores.
15.2.1 Monitoreo y revisión de los servicios de los proveedores. Las organizaciones deberán monitorear, revisar y auditar regularmente la entrega de servicios por parte de los proveedores.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN
16.1 Gestión de incidentes de seguridad de la información y mejoras. Objetivo: Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación de debilidades y eventos de seguridad.
16.1.1 Responsabilidades y procedimientos. Se deben establecer responsabilidades de los procedimientos y de la gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
16.1.2 Reporte de eventos de seguridad de la información. Los eventos de seguridad de la información deben ser reportados a través de canales de gestión apropiados, tan rápido como sea posible.
16.1.6 Aprendizaje de los incidentes de seguridad de la información. El conocimiento adquirido a partir de analizar y resolver los incidentes de seguridad de la información, deberá ser utilizado para reducir la probabilidad o el impacto de incidentes futuros.

Ámbito/Categoría/Control
16.1.7 Colección de evidencia. La organización deberá definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
17.1 Continuidad de la seguridad de la información. Objetivo: La continuidad de seguridad de la información deberá estar embebida en los sistemas de gestión de continuidad del negocio de la organización.
17.1.1 Planificación de continuidad de seguridad de la información. La organización deberá determinar los requisitos de la seguridad de la información y de la continuidad de su gestión en situaciones adversas, por ejemplo durante una crisis o desastre.
17.1.2 Implementación de continuidad de seguridad de la información. La organización deberá establecer, documentar, implementar y mantener los procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de seguridad de la información durante una situación adversa.
17.1.3 Verificación, revisión y evaluación de continuidad de seguridad de la información. La organización deberá verificar los controles de continuidad de seguridad de la información que han establecido e implementado a intervalos regulares, para asegurarse que son válidos y efectivos durante situaciones adversas.
18. CUMPLIMIENTO.
18.1 Cumplimiento con requisitos legales y contractuales. Objetivo: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.
18.1.1 Identificación de requisitos contractuales y de legislación aplicable. Todos los requisitos legislativos, estatutarios, regulatorios y contractuales relevantes así como el enfoque de la organización para cumplir con estos requisitos, deben estar explícitamente identificados, documentados y actualizados, para cada sistema de información y para la organización.
18.1.3 Protección de registros. Los registros deberán estar protegidos ante cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.
18.2 Revisiones de la seguridad de la información. Objetivo: Asegurar que la seguridad de la información está implementada y es operada de acuerdo con las políticas y procedimientos organizativos.
18.2.1 Revisión independiente de la seguridad de la información. El enfoque de la organización para manejar la seguridad de la información y su implementación (por ejemplo objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) deberá ser revisado independientemente a intervalos planeados, o cuando ocurran cambios significativos.
18.2.2 Cumplimiento de políticas y estándares de seguridad. Los gerentes deberán revisar regularmente el cumplimiento de políticas, normas y otros requisitos de seguridad, dentro del ámbito de su competencia.
18.2.3 Revisión del cumplimiento técnico. Los sistemas de información deberán ser revisados regularmente, con la finalidad de asegurar el cumplimiento de las políticas y normas de seguridad de la información de la organización.

Aspectos complementarios para la implementación:

1. Los términos a utilizar en todo lo relacionado a la materia de la seguridad de la información, son los establecidos en la norma internacional ISO/IEC 27000:2016 Overview and vocabulary y en el SC 27 Standing Document 6 (SD6): Glossary of IT Security Terminology.

2. Los procesos de desarrollo de ingeniería de sistemas y de ingeniería de software deben cumplir con lo establecido por las normas internacionales ISO/IEC 15288 e ISO/IEC 12207, respectivamente.

3. Se debe implementar una política criptográfica que cumpla con los intereses, regulaciones y restricciones del ordenamiento jurídico nacional, de manera tal que salvaguarde aspectos como la confidencialidad de la información, reserva tributaria, entre otros.

4. Se debe establecer controles criptográficos para lograr los diferentes objetivos de seguridad de la información (confidencialidad, integridad/autenticidad, no repudio, autenticación, entre otros) en la solución implementada, dentro de los cuales deben utilizar los equipos de gestión criptográfica HSM. Se debe tomar en consideración el cumplimiento de los estándares siguientes:

    a) En el caso de uso exclusivo del equipo:

    - El estándar FIPS 140-2 Nivel 2
    - El estándar Common Criteria EAL4

    b) En el caso de uso compartido del equipo:

    - El estándar FIPS 140-2 Nivel 3
    - El estándar Common Criteria EAL4

5. Se debe implementar una política y reglas de desarrollo seguro de software y de sistemas, de acuerdo con lo establecido por el protocolo o Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP), para todo el software utilizado en la solución implementada.

6. Llevar un registro de los incidentes presentados respecto de la seguridad de la información, de manera que pueda ser compartido entre los diversos actores del sistema de emisión electrónica, para reducir la probabilidad e impacto de incidentes futuros.

7. Haber realizado las pruebas de intrusión o evaluaciones de vulnerabilidad (Ethical Hacking, entre otros) realizadas dentro del marco de la revisión del cumplimiento técnico de los requerimientos establecidos para la gestión de la seguridad de los sistemas de información.

Anexo B

Aspectos técnicos - emisor electrónico

Envíos al Operador de Servicios Electrónicos

1. Sobre los envíos mediante el servicio web

Métodos para el envío

El envío se realiza a través de servicio web si se usa alguno de los métodos siguientes:

a) SendBill, el cual permite recibir un archivo ZIP con un único formato digital y devuelve un archivo Zip que contiene el CDR –OSE.

b) SendSummary, el cual permite recibir un archivo Zip con un único formato digital del Resumen Diario o Comunicación de Baja. Devuelve un ticket con el que posteriormente, utilizando el método getStatus, se puede obtener el archivo Zip que contiene el CDR – OSE.

c) GetStatus el cual permite recibir el ticket como parámetro y devuelve un objeto que indica el estado del proceso y en caso de haber terminado, devuelve adjunta el CDR - OSE.

El servicio web deberá estar protegido vía SSL y la dirección será comunicada por el Operador de Servicios Electronicos.

2. Sobre el empaquetado y nombres de los archivos generados

a) El formato digital con la firma digital debe ser empaquetado en un archivo ZIP antes de su envío al OSE.

b) Nombre del formato digital y del archivo ZIP

El formato digital y el archivo ZIP que contiene al primero debe ser generado con los nombres que se detallan a continuación:

b.1) Factura electrónica y las notas electrónicas enviadas individualmente:

Posición	Nemotécnico	Descripción
01-11	RRRRRRRRRRR	RUC del emisor electrónico
12	-	Guión separador
13-14	TT	Tipo de comprobante de pago electrónico o nota electrónica
	01	Factura electrónica
	07	Nota de crédito electrónica
	08	Nota de débito electrónica
15	-	Guión separador
16-19	FSSS	Serie de la factura electrónica o nota electrónica vinculada a ésta. Se espera que el primer carácter sea la constante “F” seguido por tres caracteres alfanuméricos.

20	-	Guión separador
21-28	CCCCCCCC	Número correlativo de la factura electrónica o nota electrónica vinculado a ésta. Este campo es variante. Se espera un mínimo de 1 y máximo de 8 dígitos.
29 (*****)	.	Punto de extensión
30-32 (*****)	EEE	Extensión del archivo
	XML	Para el caso del formato XML
	ZIP	Para el caso del archivo ZIP

(*****) Las posiciones pueden variar dependiendo de la longitud del correlativo.

Ejemplo:

Nombre del archivo ZIP: ***20100066603-01-F001-1.ZIP***
Nombre del archivo XML: ***20100066603-01-F001-1.XML***

b.2) Comunicación de baja:

Posición	Nemotécnico	Descripción
01-11	RRRRRRRRRRR	RUC del emisor electrónico
12	-	Guión separador
13-14	TT	Tipo de resumen
	RA	Comunicación de Baja
15	-	Guión separador
16-23	YYYYMMDD	Fecha de la generación del archivo en formato YYYYMMDD
24	-	Guión separador
25-29	CCCCC	Numero correlativo. Este campo es variante, se espera un mínimo de 1 y máximo de 5.
30 (*****)	.	Punto de extensión
31-33(*****)	EEE	Extensión del archivo
	XML	Para el caso del formato XML
	ZIP	Para el caso del archivo ZIP

(*****) Las posiciones pueden variar dependiendo de la longitud del correlativo.

Ejemplo:

Nombre del archivo ZIP: ***20100066603-RA-20110522.ZIP***
Nombre del archivo XML: ***20100066603-RA-20110522.XML***

b.3) Resumen Diario

Posición	Nemotécnico	Descripción
01-11	RRRRRRRRRRR	RUC del emisor electrónico
12	-	Guión separador
13-14	TT	Tipo de resumen
	RC	Resumen Diario
15	-	Guión separador
16-23	YYYYMMDD	Fecha de la generación del archivo en formato YYYYMMDD. Fecha que corresponde a la fecha de emision de la boletas y notas

		vinculadas
24	-	Guión separador
25-29	CCCCC	Numero correlativo. Este campo es variante, se espera un mínimo de 1 y máximo de 5.
30 (*)	.	Punto de extensión
31-33(*) 31-34(*)	EEEE	Extensión del archivo, puede contener 4 o cuatro caracteres
	XML	Para el caso del formato XML
	ZIP	Para el caso del archivo ZIP
(*) Las posiciones pueden variar dependiendo de la longitud del correlativo. Ejemplo: Nombre del archivo ZIP: ***20100066603-RC-20110522.ZIP*** Nombre del archivo XML: ***20100066603-RC-20110522.XML***		

3. Sobre los envíos por lotes al OSE – Recibos electrónicos Servicios Públicos

Métodos para el envío

El envío se realizará a través del servicio web, utilizando los siguientes métodos asíncronos:

a) SendPack, el cual permitirá un archivo Zip con un único lote. Devuelve un ticket con el que posteriormente, utilizando el método getStatus, se puede obtener el archivo Zip que contiene el CDR – OSE.

b) GetStatus, el cual permite recibir el ticket como parámetro y devuelve un objeto que indica el estado del proceso y en caso de haber terminado, devuelve adjunta el CDR – OSE.

Validaciones de lotes

1. Se podrán recibir lotes de un máximo de 1000 XML
2. Los XML de cada lote debe cumplir con lo siguiente:

   a. Deben corresponder todos a una misma fecha de emisión.
   b. Deben corresponder a un mismo número de RUC.
   c. La firma debe corresponder al RUC del emisor o del PSE autorizado para dicho RUC.
   d. Cada XML deberá estar firmado por el emisor o por el PSE autorizado para dicho RUC.
   e. La validación para cada XML, incluido en cada lote, serán las mismas que las realizadas para los envíos unitarios de XML.
   f. No debe existir numeración duplicada en cada lote (serie y correlativo igual para mas de un documento por lote). De existir se rechaza el (los) XML duplicados.
   g. La identificación de cada lote tendrá un correlativo por día. La nomenclatura será la siguiente:

   Ruc/prefijo de lote SP/fecha/correlativo

   20100066603-LP-20110522-1
   20100066603-LP-20110522-2

El correlativo es un identificador y debe ser único, no necesariamente correlativo

3. Si algún documento no cumple con lo indicado en el numeral 2, sólo se rechazará el XML que incumple con la regla de validación, dejando procesar el resto de documentos.

4. Requisitos técnicos de los documentos electronicos

Valor resumen

El valor resumen es la cadena resumen en base 64, el cual es el resultado de aplicar el algoritmo matemático (denominado función hash) al formato XML que representa el comprobante de pago electrónico o la nota electrónica. Corresponde al valor del elemento <ds:DigestValue> de los referidos documentos.

La impresión debe cumplir las siguientes características:

a) Posición dentro de la representación impresa: Parte inferior de la representación impresa.

b) Color de impresión: Negro.

Código de barras PDF417

- **Simbología**

  Para la generación del código de barras se hará uso de la simbología PDF417 de acuerdo a la Norma ISO/IEC 15438:2010 Tecnología de la información. Técnicas de identificación automática y de captura de datos. Especificaciones de los símbolos de códigos de barras PDF417. No debe usarse las variantes:

  a) PDF417 Compactado (Compact PDF417).

  b) Micro PDF417.

  c) Macro PDF417.

- **Características técnicas**

  a) Nivel de corrección de error (Error Correction Level): nivel 5.

  b) Modo de compactación: Modo de compactación de Bytes (Byte Compaction Mode).

  c) Dimensiones mínimas de los elementos del código de barras:

  - Ancho mínimo de un módulo (X-Dimension): 0,0067 pulgadas (0,170 mm).
  - Altura de fila (Y-Dimension): 3 veces el valor del Ancho mínimo de un módulo (3 veces X-Dimension).

- **Información a consignar en el código de barras**

En el código de barras se consignará la información siguiente en la medida que exista en el comprobante de pago electrónico o la nota electrónica:

a) Número de RUC del emisor electrónico.

b) Tipo de comprobante de pago electrónico

c) Numeración conformada por serie y número correlativo.

d) Sumatoria IGV, de ser el caso.

e) Importe total de la venta, cesión en uso o servicio prestado.

f) Fecha de emisión.

g) Tipo de documento del adquirente o usuario, de ser el caso.

h) Número de documento del adquirente o usuario, de ser el caso.

i) Valor resumen a que se refiere el numeral 6.2

j) Valor de la Firma digital. Corresponde al valor del elemento <ds:SignatureValue> del comprobante de pago electrónico o nota electrónica.

La información señalada en los incisos anteriores de este numeral deberá consignarse con el mismo formato empleado en el comprobante de pago electrónico o la nota electrónica y se estructura de acuerdo al siguiente orden, siendo el separador de campo el carácter pipe ("|"):

RUC **|** TIPO DE DOCUMENTO **|** SERIE **|** NUMERO **|** MTO TOTAL IGV **|** MTO TOTAL DEL COMPROBANTE **|** FECHA DE EMISION **|** TIPO DE DOCUMENTO ADQUIRENTE **|** NUMERO DE DOCUMENTO ADQUIRENTE **|** VALOR RESUMEN **|** VALOR DE LA FIRMA **|**

Se debe respetar la cantidad de campos especificados en la estructura anterior, es decir, en caso no exista alguna información en el comprobante de pago electrónico o la nota electrónica, se deberá mantener el campo vacío como información.

- **Características de la Impresión**

La impresión debe cumplir las siguientes características:

a) Posición del código de barras dentro de la representación impresa: Parte inferior de la representación impresa.

b) Tamaño máximo: 2 cm de alto y 6 cm de ancho (incluye el espacio en blanco alrededor del código).

c) Zona de silencio mínimo (Quiet Zone) o ancho mínimo obligatorio en blanco alrededor del código impreso para delimitarlo: 1 mm.

d) Color de impresión: Negro.

- **Código de barras QR**

Simbología

Para la generación del código de barras se hará uso de la simbología QR Code 2005 de acuerdo a la Norma ISO/IEC 18004:2006. D3enominsad “Information technology – Automatic identification and data capture techniques – QR Code 2005 bar code symbology specification”. No debe usarse las variantes:

a) Micro QR.

Características técnicas

a) Nivel de corrección de error (Error Correction Level): nivel Q.

b) Dimensiones mínimas de los elementos del código de barras:

- Ancho mínimo de un módulo (X-Dimension): 0,0075 pulgadas (0,190 mm).
- Codificacion de caracteres UTF8

Información a consignar en el código de barras

En el código de barras se consignará la información siguiente en la medida que exista en el comprobante de pago electrónico o la nota electrónica:

a) Número de RUC del emisor electrónico.

b) Tipo de comprobante de pago electrónico

c) Numeración conformada por serie y número correlativo.

d) Sumatoria IGV, de ser el caso.

e) Importe total de la venta, cesión en uso o servicio prestado.

f) Fecha de emisión.

g) Tipo de documento del adquirente o usuario, de ser el caso.

h) Número de documento del adquirente o usuario, de ser el caso.

La información señalada en los incisos anteriores de este numeral debe consignarse con el mismo formato empleado en el comprobante de pago electrónico o la nota electrónica y se estructura de acuerdo al siguiente orden, siendo el separador de campo el carácter pipe (“|”):

RUC **|** TIPO DE DOCUMENTO **|** SERIE **|** NUMERO **|** MTO TOTAL IGV **|** MTO TOTAL DEL COMPROBANTE **|** FECHA DE EMISION **|** TIPO DE DOCUMENTO ADQUIRENTE **|** NUMERO DE DOCUMENTO ADQUIRENTE **|**

Características de la Impresión

La impresión debe cumplir las siguientes características:

e) Posición del código de barras dentro de la representación impresa: Parte inferior de la representación impresa.

f) Tamaño máximo: 6 cm de alto y 6 cm de ancho (incluye el espacio en blanco alrededor del código).

g) Zona de silencio mínimo (Quiet Zone) o ancho mínimo obligatorio en blanco alrededor del código impreso para delimitarlo: 1 mm.

h) Color de impresión: Negro.

5 Resumen de Comprobantes Impresos

Se describe en detalle la secuencia de pasos a seguir para el procedimiento de preparación del Resumen de Comprobantes Impresos

a) Condiciones de envío.
Los comprobantes de pago a ser informados son aquellos impresos o importados por imprenta autorizada y tickets o cintas emitidas por maquinas registradoras. En caso de comprobantes impresos por imprenta autorizada, deberán corresponder a rangos previamente autorizados por SUNAT

b) **Procedimiento de envío**
El envío del archivo resumen de comprobantes impresos se realizará a través de la opción correspondiente habilitada en SUNAT Operaciones en Línea, teniendo en cuenta lo siguiente:

- Paso 1: Preparar un archivo de extensión “TXT” conteniendo la información de los comprobantes, en ninguno de los casos se incluye el detalle o descripción de los ítems del comprobante.

  Las especificaciones de cada campo de este RESUMEN está descrito en el ANEXO 11 RESUMEN DE COMPROBANTES IMPRESOS.

  Luego de completar la longitud de cada campo se debe incluir un símbolo conocido como pipa o palote “|”.

  El registro de los comprobantes debe completarse de la siguiente forma:

  - Facturas: Se prepara la información de la factura una por línea.
  - Boletas: Se prepara la información de la boleta una por línea.
  - Notas de crédito (Relacionadas con Facturas y Boletas): Se prepara una por línea.
  - Notas de debito (Relacionadas con Facturas y Boletas): Se prepara una por línea.
  - Tickets que otorguen derecho a crédito fiscal: se preparan de uno por línea.
  - Tickets que no otorguen derecho a crédito fiscal: se prepara como resumen.

Una vez elaborado el archivo deberá ser guardado con extensión. "txt.". Para efecto del nombre del archivo deberá considerar lo indicado en el punto 6

- Paso 2: Comprimir el archivo TXT en otro de extensión "ZIP" .

- Paso 3: Cargue en archivo .ZIP, recibirá un número de constancia generada por SUNAT operaciones en Linea ("ticket")

Procedimiento de envío por correcciones

En caso se requiera corregir un envío realizado, se deberá elaborar nuevamente el archivo Resumen de Comprobantes Impresos como si se tratase del original, y se deberá seguir los pasos indicados en párrafos anteriores. Para tal efecto, el último archivo RESUMEN enviado reemplazará por completo al anterior.

Procesamiento de envíos

Los envíos son procesados secuencialmente, al momento de su recepción. De existir errores, éstos serán puestos a disposición en la opción correspondiente de SUNAT Operaciones en Linea (Opción consultas). A través de esta opción, se activará un link de descarga de archivo de errores.

Los envíos sin errores serán cargados como comprobantes de pago, notas de crédito y/o notas de débito, según corresponda, que han sido informados por contingencia.

Seguimiento de envíos

Los contribuyentes pueden hacer consultas de sus envíos utilizando la opcion correspondiente habilitada en SUNAT Operaciones en Línea, por número de constancia generada por SUNAT Operaciones en línea ("ticket") o rangos de fechas.

Estructura del Nombre del Archivo – Comprobantes Impresos

El nombre de los archivos está en función a la fecha a la que corresponde el envío. El nombre del archivo debe cumplir con el formato

"**99999999999-RF-DDMMYYYY-99"** donde:

- 99999999999 números de ruc
- RF: Caracteres identificativos del archivo "RF" textualmente representa resumen de facturas.
- DDMMYYYY: Fecha de emisión en contingencia en formato "DDMMYYYY"; ejemplo 15072014.
- 99: Numero de envío dato entre 01 al 99.

Las extensiones del archivo son .TXT y .ZIP según corresponda.

Anexo C

Aspectos técnicos - OSE

I. Constancia de Recepción – CDR

Es el documento emitido por el OSE al emisor electrónico, al comprobar informáticamente que aquello que le envió el emisor electrónico, cumple con las condiciones respectivas para considerar que se encuentre emitido un documento electrónico. La estructura es la definida en Cuadro 1, del presente anexo.

II. Mensajes de inconsistencia

Son aquellos mensajes que el Operador Servicios Electrónicos envía a los emisores electrónicos, a través de una comunicación electrónica, cuando producto de la comprobación de los documentos electrónicos, se determina que no cumplen con los aspectos esenciales definidos por SUNAT para ser considerados comprobantes de pago o documentos relacionados directa o indirectamente a éstos. Los referidos mensajes tendrán como mínimo la siguiente estructura

CAMPOS	NIVEL	CONDICIÓN	TIPO Y LONGITUD	campo
Código de la excepción	Global	M	A4	<faultstring>
Descripción de la respuesta del envío	Global	M	an..100	<detail>

III. ENVIOS A LA SUNAT

a. Sobre los envío de uno en uno

Los envíos realizados a SUNAT deberán considerar lo siguiente:

1. El archivo zip enviado deberá contener los siguientes documentos:
   - El documento electrónico XML (Generado y firmado por el Emisor electrónico o PSE según sea el caso).
   - La Constancia de Recepción – CDR OSE (Generado y firmado por el OSE).

2. Los tipos de documentos electrónicos deberan corresponder a:
   - Factura
   - Boleta de venta
   - Nota de crédito
   - Nota de debito
   - Resumen diario de comprobantes (boletas, notas de crédito y debito asociadas a boletas)
   - Comunicación de Baja de comprobantes
   - Comprobante de percepción

- Comprobante de retención
- Guía de Remisión
- Resumen Diario de Reversión de comprobantes de percepción y retención.

3. El Receptor SUNAT cuenta con un método personalizado para aceptar cada tipo de documento electrónico. Al respecto, los métodos de recepción definidos son los siguientes:
   - sendBill
   - sendSummary

4. Se podrán recibir XMLs con fecha futura (today + 2)

5. La firma de los documentos electrónicos XML debe corresponder al RUC del emisor o del PSE autorizado por él.

6. La firma de los CDR OSE debe corresponder al RUC del OSE seleccionado por el emisor.

b. Sobre el empaquetado y nombres de los archivos generados

b.1 Para el archivo ZIP de los tipos de documentos Factura, Boleta de venta, Nota de crédito, Nota de debito, comprobante de percepción, comprobante de retención, guía de remisión remitente y guía de remisión transportista, se deberá tener en cuenta el siguiente formato:

Posición	Nemotécnico	Descripción
01-11	RRRRRRRRRRR	RUC del emisor
12	-	Guión separador
13-14	TT	Tipo de comprobante
	01	Factura
	03	Boleta de venta
	07	Nota de crédito
	08	Nota de debito
	20	Comprobante de retencion
	40	Comprobante de percepcion
	09	Guia de Remision Remitente
	31	Guia de Remision Transportista
15	-	Guión separador
16-19	####	Serie del comprobante. Dependerá del tipo de comprobante.
20	-	Guión separador
21-28	CCCCCCCC	Número correlativo del comprobante. Este campo es variante, se espera un mínimo de 1 y máximo de 8.
29(*****)	.	Punto de extensión
30-32 (*****)	EEE	Extensión del archivo
	ZIP	Para el caso del archivo ZIP
	XML	Para el caso del documento XML

	XML (CDR OSE)	Para el caso del CDR OSE

(*****) Las posiciones pueden variar dependiendo de la longitud del correlativo.

Ejemplos:

Nombre del archivo ZIP:
20100066603-01-F001-1.zip
Nombre del archivo XML:
20100066603-01-F001-1.xml
Nombre del archivo XML (CDR OSE):
R-20100066603-01-F001-1.xml

Nombre del archivo ZIP:
20100066603-03-B001-00000001.zip
Nombre del archivo XML:
20100066603-03-B001-00000001.xml
Nombre del archivo XML (CDR OSE):
R-20100066603-03-B001-00000001.xml

Nombre del archivo ZIP:
20100066603-20-R001-00000251.zip
Nombre del archivo XML:
20100066603-20-R001-00000251.xml
Nombre del archivo XML (CDR OSE):
R-20100066603-20-R001-00000251.xml

b.2 El archivo ZIP del tipo de documento Resumen diario de comprobantes (boletas, notas de crédito y debito asociadas a boletas), Comunicación de Baja de comprobantes y Resumen de Reversión (para CRE y CPE), deberá tener el siguiente formato:

Posición	Nemotécnico	Descripción
01-11	RRRRRRRRRRR	RUC del emisor
12	-	Guión separador
13-14	TT	Tipo de Resumen
	RC	Resumen diario de Boletas
	RA	Comunicación de Bajas
	RR	Resumen de Reversion (para CRE y CPE)
15	-	Guión separador
16-23	YYYYMMDD	Fecha de generación del archivo en formato YYYYMMDD
24	-	Guión separador
25-29	CCCCC	Número correlativo del archivo. Este campo es variante, se espera un mínimo de 1 y máximo de 5.
30 (*****)	.	Punto de extensión
31-33 (*****)	EEE	Extensión del archivo

	ZIP	Para el caso del archivo ZIP
	XML	Para el caso del documento XML
	XML (CDR OSE)	Para el caso del CDR OSE

(*****) Las posiciones pueden variar dependiendo de la longitud del correlativo.

Ejemplos:

Nombre del archivo ZIP:
20100066603-RC-20161220-1.zip
Nombre del archivo XML:
20100066603-RC-20161220-1.xml
Nombre del archivo XML (CDR OSE):
R-20100066603-RC-20161220-1.xml

Nombre del archivo ZIP:
20100066603-RA-20161220-00001.zip
Nombre del archivo XML:
20100066603-RA-20161220-00001.xml
Nombre del archivo XML (CDR OSE):
R-20100066603-RA-20161220-00001.xml

Nombre del archivo ZIP:
20100066603-RR-20161225-005.zip
Nombre del archivo XML:
20100066603-RR-20161225-005.xml
Nombre del archivo XML (CDR OSE):
R-20100066603-RR-20161225-005.xml

b.3 Por cada envío realizado por el OSE a SUNAT, se generará una Constancia de Recepción – CDR SUNAT, la cual contendrá la estructura indicada en el presente anexo.

c. Sobre los Envíos por lotes

1. El OSE podrá enviar lotes de factura, boleta de venta (siempre que se hayan enviado de manera individual), notas de crédito y débito, y documentos autorizados electrónicos, en un archivo zip, a través del servicio web que SUNAT pondrá a disposición. El método que utilizará será el sendPack.

2. SUNAT procesará de forma ASINCRONA el envío, es decir, devolverá un número de ticket con el cual el OSE deberá posteriormente consultar el estado del proceso. De haber concluido éste, el proceso devolverá adjunta una Constancia de recepción – CDR SUNAT utilizando el método getStatus.

3. El CDR – SUNAT tendrá la estructura indicada en el Cuadro 2 del presente anexo.

4. Los XML de cada lote deben considerar lo siguiente:

Los documentos deben corresponder solo a los siguientes tipos de comprobantes:

- Factura
- Boleta de venta
- Nota de crédito
- Nota de debito
- Comprobante de percepción
- Comprobante de retención
- Guía de remisión remitente
- Guía de remisión transportista

5. Los documentos electrónicos XML pueden corresponder a cualquier fecha de emisión.

6. Dentro del lote, por cada documento electrónico XML, se deber remitir el CDR OSE (Igual cantidad de documentos XML, igual cantidad de CDRs OSE).

7. Se podrá recibir lotes con XMLs con fecha futura (today + 2)

8. Los documentos deben corresponder a un mismo número de RUC del emisor.

9. La firma para los documentos electrónicos XML debe corresponder al RUC del emisor o del PSE autorizado éste.

10. La firma para los CDR OSE debe corresponder al RUC del OSE seleccionado por el emisor.

11. De detectarse XML duplicados (RUC-TT-serie-correlativo), o CDR OSE duplicados (R-RUC-TT-serie-correlativo), se rechazarán.

12. La identificación de cada lote tendrá la siguiente nomenclatura:

Posición	Nemotécnico	Descripción
01-11	RRRRRRRRRRR	RUC del emisor electrónico
12	-	Guión separador
13-14	LT	Prefijo de lote
15	-	Guión separador
16-23	YYYYMMDD	Fecha de envío del lote de comprobantes
24	-	Guión separador
25-29	CCCCC	Número correlativo del lote por día. Este campo es variante, se espera un mínimo de 1 y máximo de 5.
30 (*****)	.	Punto de extensión
31-33 (*****)	EEE	Extensión del archivo
	ZIP	Para el caso del archivo ZIP
(*****) Las posiciones pueden variar dependiendo de la longitud del correlativo. Ejemplo del nombre del lote (archivo zip):		

20100066603-LT-20160405-1.zip

Ejemplo del nombre de los documentos XML contenidos en el archivo .zip (2 comprobantes con sus 2 respectivos CDR OSE)

20100066603-01-F001-23.xml
R-20100066603-01-F001-23.xml
20100066603-03-B001-120.xml
R-20100066603-03-B001-120.xml

III.- ESQUEMA DE CONECTIVIDAD DE LOS OPERADORES DE SERVICIOS ELECTRONICOS CON SUNAT.

La conectividad entre los OSE y SUNAT se realizará a través de internet y estará restringido a las direcciones IP que indique cada OSE.

El OSE debe contar con conexión a los siguientes dominios:

- e-ose1 y e-ose2
- e-descargaose1 y e-descargaose2
- e-betaose1 y e-betaose2

Es responsabilidad del OSE el balanceo entre ambos dominios.

CUADRO 1
Constancia de Recepción OSE – CDR OSE

N°	DATO	CONDICIÓN INFORMÁTICA	TIPO Y LONGITUD (2)	FORMATO	Tag XML	Validación
1	Número de versión de UBL	M	an..10	=2.1	/ApplicationResponse/cbc:UBLVersionID	Valor fijo: "2.1"
2	Número de versión del CDR OSE	M	an..10	=1.0	/ApplicationResponse/cbc:CustomizationID	Valor fijo: "1.0"
3	Número de autorización del comprobante (UUID)	M	an..36		/ApplicationResponse/cbc:ID	Validar estructura: 8-4-4-4-12 (hexadecimal)
4	Fecha de recepción del comprobante por OSE	M	an..10	YYYY-MM-DD	/ApplicationResponse/cbc:IssueDate	
5	Hora de recepción del comprobante por OSE	M	an..12	hh:mm:ss.sssss	/ApplicationResponse/cbc:IssueTime	Debe ser menor o igual al momento de recepción SUNAT
6	Fecha de comprobación del comprobante (OSE)	M	an..10	YYYY-MM-DD	/ApplicationResponse/cbc:ResponseDate	
7	Hora de comprobación del comprobante (OSE)	M	an..12	hh:mm:ss.sssss	/ApplicationResponse/cbc:ResponseTime	Debe ser mayor a la fecha de recepción OSE
8	Número de documento de identificación del que envía el CPE (emisor o PSE)	M	an..15		/ApplicationResponse/cac:SenderParty/cac:PartyLegalEntity/cbc:CompanyID	Debe corresponder al RUC del que envía el CPE al OSE Si el RUC es de un PSE, éste debe estar autorizado por el emisor (vinculado) a la fecha de comprobación
9	Tipo de documento de identidad del que envía el CPE (emisor o PSE)	M	n1	Catálogo 06	/ApplicationResponse/cac:SenderParty/cac:PartyLegalEntity/cbc:CompanyID/@schemeID	Valor fijo; "6"
		M			/ApplicationResponse/cac:SenderParty/cac:PartyLegalEntity/cbc:CompanyID/@schemeAgencyName	Valor fijo: "PE:SUNAT"
		M			/ApplicationResponse/cac:SenderParty/cac:PartyLegalEntity/cbc:CompanyID/@schemeURI	Valor fijo: "urn:pe:gob:sunat:cpe:see:gem:catalogos:catalogo6"
10	Número de documento de identificación del OSE	M	an..11		/ApplicationResponse/cac:ReceiverParty/cac:PartyLegalEntity/cbc:CompanyID	El certificado digital con el que se firma el CDR OSE, debe corresponder a este RUC.

						Debe corresponder a un OSE registrado en el padrón. Debe estar vinculado al Emisor del comprobante, a la fecha de comprobación.
11	Tipo de documento de identidad del OSE	M	n1	Catálogo 06	/ApplicationResponse/cac:ReceiverParty/cac:PartyLegalEntity/cbc:CompanyID/@schemeID	Valor fijo: "6"
		M			/ApplicationResponse/cac:ReceiverParty/cac:PartyLegalEntity/cbc:CompanyID/@schemeAgencyName	Valor fijo: "PE:SUNAT"
		M			/ApplicationResponse/cac:ReceiverParty/cac:PartyLegalEntity/cbc:CompanyID/@schemeURI	Valor fijo: "urn:pe:gob:sunat:cpe:see:gem:catalogos:catalogo6"
12	Código de Respuesta	M	n1		/ApplicationResponse/cac:DocumentResponse/cac:Response/cbc:ResponseCode	Valor fijo: "0", indica que el documento electrónico fue aceptado
		M			/ApplicationResponse/cac:DocumentResponse/cac:Response/cbc:ResponseCode/@listAgencyName	Valor fijo: "PE:SUNAT"
13	Descripción de la Respuesta	M	an..250		/ApplicationResponse/cac:DocumentResponse/cac:Response/cbc:Description	No debe ser nulo
14	Código de observación	C	n4		/ApplicationResponse/cac:DocumentResponse/cac:Response/cac:Status/cbc:StatusReasonCode	
		C			/ApplicationResponse/cac:DocumentResponse/cac:Response/cac:Status/cbc:StatusReasonCode/@listURI	Valor fijo: "urn:pe:gob:sunat:cpe:see:gem:codigos:codigoretorno"
15	Descripción de la observación	C	an..250		/ApplicationResponse/cac:DocumentResponse/cac:Response/cac:Status/cbc:StatusReason	
16	Serie y número del comprobante	M	an..13	####-########	/ApplicationResponse/cac:DocumentResponse/cac:DocumentReference/cbc:ID	Debe corresponder con el CPE
17	Fecha de emisión del comprobante	M	an..10	YYYY-MM-DD	/ApplicationResponse/cac:DocumentResponse/cac:DocumentReference/cbc:IssueDate	
18	Hora de emisión del comprobante	M	an..12	hh:mm:ss.ssss	/ApplicationResponse/cac:DocumentResponse/cac:DocumentReference/cbc:IssueTime	
19	Tipo de comprobante	M	n2	Catálogo 01	/ApplicationResponse/cac:DocumentResponse/cac:DocumentReference/cbc:DocumentTypeCode	
20	Hash del comprobante	M			/ApplicationResponse/cac:DocumentResponse/cac:DocumentReference/cac:Attachment/cac:ExternalReference/cbc:DocumentHash	

21	Número de documento de identificación del emisor	M	an..15		/ApplicationResponse/cac:DocumentResponse/cac:IssuerParty/cac:PartyLegalEntity/cbc:CompanyID	
22	Tipo de documento de identidad del emisor	M	n1	Catálogo 06	/ApplicationResponse/cac:DocumentResponse/cac:IssuerParty/cac:PartyLegalEntity/cbc:CompanyID/@schemeID	
23	Número de documento de identificación del receptor	M	an..15		/ApplicationResponse/cac:DocumentResponse/cac:RecipientParty/cac:PartyLegalEntity/cbc:CompanyID	
24	Tipo de documento de identidad del receptor	M	n1	Catálogo 06	/ApplicationResponse/cac:DocumentResponse/cac:RecipientParty/cac:PartyLegalEntity/cbc:CompanyID/@schemeID	

CUADRO 2
Constancia de Recepción SUNAT – CDR SUNAT

N°	CAMPOS	NIVEL	CONDICIÓN	TIPO Y LONGITUD	FORMATO	Tag XML	OBSERVACIONES
1	Versión del UBL	Global	M	an..10		/ApplicationResponse/cbc:UBLVersionID	
2	Versión de la estructura del documento	Global	M	an..10		/ApplicationResponse/cbc:CustomizationID	
3	Firma Digital (Firma electrónica)	Global	M	an..3000		/ApplicationResponse/ds:Signature	
4	Número identificador del proceso de recepción	Global	M	n19	YYYY#########	/ApplicationResponse/cbc:ID	
5	Fecha de comprobación OSE	Global	M	an..10	YYYY-MM-DD	/ApplicationResponse/cbc:IssueDate	Formato Date del XML
6	Hora de comprobación OSE	Global	M	an..11	hh:mm:ss	/ApplicationResponse/cbc:IssueTime	
7	Fecha de generación CDR SUNAT	Global	M	an..10	YYYY-MM-DD	/ApplicationResponse/cbc:ResponseDate	Formato Date del XML
8	Hora de generación CDR SUNAT	Global	M	an..11	hh:mm:ss	/ApplicationResponse/cbc:ResponseTime	
9	Código y descripción de observaciones	Global	M	an..250		/ApplicationResponse/cbc:Note	Solo en caso de existir observaciones
10	Número de RUC del Emisor	Global	M	an..15		/ApplicationResponse/cac:SenderParty/cac:PartyIdentification/cbc:ID	
11	Número de RUC del Receptor	Global	M	an..15		/ApplicationResponse/cac:ReceiverParty/cac:PartyIdentification/cbc:ID	
12	Serie y número del comprobante	Global	M	an..13		/ApplicationResponse/cac:DocumentResponse/cac:Response/cbc:ReferenceID	Formato de acuerdo al tipo de documento procesado
13	Código de respuesta del envío	Global	M	n1		/ApplicationResponse/cac:DocumentResponse/cac:Response/cbc:ResponseCode	Siempre será “0”
14	Descripción de la respuesta del envío	Global	M	an..100		/ApplicationResponse/cac:DocumentResponse/cac:Response/cbc:Description	

Anexo D

Carta Fianza

I. Carta Fianza – Requisito para la inscripción en el Registro OSE

La carta fianza debe cumplir con lo siguiente:

a) Ser emitida a favor de la SUNAT, por alguna empresa del sistema financiero o del sistema de seguros, autorizada por la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS) a emitir cartas fianza.

b) Constar en ella que en caso de ejecución, la empresa que la extendió debe emitir y entregar un cheque girado a la orden de SUNAT/BANCO DE LA NACIÓN.

c) Ser irrevocable, solidaria, incondicional, de ejecución inmediata, fiel cumplimiento y sin beneficio de excusión.

d) Emitirse por un monto equivalente a 28 UIT, e indicar expresamente que ese monto garantiza el pago de la deuda tributaria y administrativa generada por una o más multas impuestas al amparo de la presente resolución, por el incumplimiento de las obligaciones que adquiere el sujeto. La UIT a considerar es la vigente al momento de la emisión de la carta fianza.

e) Ser ejecutable a solo requerimiento de la SUNAT.

f) Tener una vigencia mínima de doce meses.

g) En caso la empresa que emitió la carta fianza, fuese intervenida y declarada en disolución conforme a la Ley General del Sistema Financiero y del Sistema de Seguros Orgánica de la Superintendencia de Banca y Seguros - SBS, aprobada por la Ley Nº 26702 y normas modificatorias, el sujeto deberá presentar una nueva carta fianza, considerando las características definidas en los literales precedentes y hasta la fecha en que se emita la resolución que resuelva la solicitud de inscripción la Registro OSE.

II. Renovación o sustitución de la carta fianza

La carta fianza debe renovarse o sustituirse, considerando, en lo pertinente, lo indicado en los literales a) al f) del numeral anterior; con la finalidad de mantener vigente la garantía en tanto el sujeto tenga la calidad de OSE. La referida renovación o sustitución debe realizarse dentro de un plazo máximo de cuarenta y cinco (45) días calendarios anteriores a la fecha de vencimiento de ésta.

En caso la empresa que emitió la carta fianza, fuese intervenida y declarada en disolución conforme a la Ley General del Sistema Financiero y del Sistema de Seguros Orgánica de la Superintendencia de Banca y Seguros - SBS, aprobada por la Ley Nº 26702 y normas modificatorias, el OSE deberá presentar una nueva carta fianza, dentro de los quince (15) días hábiles contados a partir del día siguiente de publicada la resolución de la SBS mediante la cual se declara la disolución de la empresa del sistema financiero o de la empresa del sistema de seguros.