

Abog. Hildamar Fernández
INFRE: 79769
Asesora Legal

SUSCERTE/AL/VenCERT/003/2010

CONVENIO DE ADHESIÓN AL

SISTEMA NACIONAL DE GESTIÓN DE INCIDENTES TELEMÁTICOS (VenCERT)

Entre la República Bolivariana de Venezuela, por órgano del Ministerio del Poder Popular para Ciencia, Tecnología e Industrias Intermedias, con competencias en materia de telecomunicaciones e informática, de conformidad con el Decreto N° 6.607 de fecha 12 de mayo de 2009, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 39.178 de fecha 14 de mayo de 2009; a través de la **SUPERINTENDENCIA DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA**, quien a los efectos de este documento se denominará "**SUSCERTE**", representada en este acto, por la ciudadana **NIURKA HERNÁNDEZ GONZÁLEZ**, titular de la cédula de identidad N° **V-10.484.661**, actuando en su carácter de Superintendente, designada mediante Resolución N° 030 de fecha 08 de enero de 2008, emanada del Ministerio del Poder Popular para las Telecomunicaciones y la Informática, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 38.856 de fecha 23 de enero de 2008, suficientemente facultada para este acto de acuerdo con lo establecido en la Resolución N° 033 de fecha 14 de febrero de 2008 del referido Ministerio, y publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 38.872 de fecha 18 de febrero de 2008, así como en la Resolución N° 058 de fecha 10 de junio de 2008, emanada del Ministerio del Poder Popular para Ciencia, Tecnología e Industrias Intermedias, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 39.200, de fecha 15 de junio de 2009, mediante la cual se le asignan competencias inherentes al desarrollo, implantación, ejecución y seguimiento del Sistema Nacional de Gestión de Incidentes Telemáticos (VenCERT), por una parte; y por la otra, la **OFICINA NACIONAL DE CONTABILIDAD PÚBLICA**, creada a través de la Ley Orgánica de la Administración Financiera del Sector Público, publicada la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.029 de fecha 05 de septiembre de 2000 y a los mismos efectos de este documento se denominará "**EL ASOCIADO**"; representado en este acto por el ciudadano **LORENZO MULET MOLINA**, venezolano, titular de la Cédula de Identidad N° **V-6.501.589**, actuando previa autorización del ciudadano Ministro según Punto de Cuenta N° 012 (ONCOP) de fecha 16/06/2010, en su carácter de Jefe de la Oficina Nacional de Contabilidad Pública, designado mediante Resolución N° 1.983, de fecha 21 de enero de 2008, emanada del Ministerio del Poder Popular para las Finanzas (actualmente Ministerio del Poder Popular de Planificación y Finanzas), publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 38.854, de fecha 21 de enero de 2008; los cuales conjuntamente se denominan "**LAS PARTES**", han convenido en celebrar como en efecto se



SIN ELEGIO
SIN MIS

celebra el presente CONTRATO DE ADHESIÓN al Sistema Nacional de Gestión de Incidentes Telemáticos (VenCERT), el cual se regirá de conformidad con las cláusulas siguientes:

OBJETO DEL CONTRATO

PRIMERA: El presente contrato tendrá por objeto establecer los términos y condiciones que regirán en el proceso de incorporación de “**EL ASOCIADO**” al Sistema Nacional de Gestión de Incidentes Telemáticos (VenCERT), el cual tiene como fin la prestación de los servicios de respuesta ante incidentes telemáticos y vulnerabilidades, bajo las condiciones y obligaciones previstas en el presente instrumento.

FINALIDAD DEL SISTEMA NACIONAL DE GESTIÓN DE INCIDENTES TELEMÁTICOS

SEGUNDA: El Sistema Nacional de Gestión de Incidentes Telemáticos (VenCERT), tiene por finalidad, entre otros, la articulación de esfuerzos en la gestión de emergencias telemáticas y reportes de vulnerabilidades sobre Infraestructuras Críticas de la Nación, posibilitando la detección oportuna de nuevos patrones de ataque y el análisis de los sistemas comprometidos, a fin de manejar información pertinente que permita el establecimiento de estrategias de respuestas ante incidentes de seguridad de información, en conjunto con otros entes y órganos del Poder Público Nacional, y a su vez ser responsable de proponer y procurar la implementación de recomendaciones, normas, estándares y procedimientos, para la seguridad de los sistemas telemáticos de la Administración Pública y su ambiente operativo, basados en los principios internacionalmente aceptados en esta materia; combinando esfuerzos con la comunidad Internet y elevando la conciencia ciudadana sobre temas de seguridad informática.

DEFINICIONES

TERCERA: A todos los efectos derivados del presente contrato, se entenderá por:

Activos de Información: Se considera como tal a la información en cualquiera de sus formas y soportes; vale decir, impresa, manuscrita, oral, electrónica y visual a la cual cada Institución, en atención a sus intereses le ha atribuido un valor determinado en función a la trascendencia de dicha información. Esta definición involucra la Plataforma Tecnológica de la Institución.

Amenaza: Todo aquello que tenga una posibilidad o probabilidad de ocurrir, como causante de daño, incluyen actos dirigidos, deliberados y sucesos no dirigidos, aleatorios o impredecibles.

Asociados: Toda entidad de carácter público o privado que se adhiere a las condiciones establecidas por SUSCERTE, relacionadas con la ejecución del Sistema Nacional de Gestión de Incidentes Telemáticos (VenCERT).



SIN ELETTO

Comunidad: Conjunto de Asociados al Sistema Nacional de Gestión de Incidentes Telemáticos (VenCERT).

Confidencialidad: Es el compromiso de discreción, que “LAS PARTES” exigen a sus empleados, contratados, terceros y/o relacionados, sobre los conocimientos, procedimientos y documentos que comprenden los activos de información de su propiedad o bajo su custodia.

Eventos de Seguridad Informática: Hechos u ocurrencias observables o medibles en la Plataforma Tecnológica.

Gestión de Incidentes Telemáticos: Proceso que involucra la asignación de prioridad, tipificación y recursos para el manejo y resolución oportuna de incidentes telemáticos que afecten la confidencialidad, integridad y disponibilidad de los activos de información de la comunidad atendida.

Incidente Telemático: Evento imprevisto, o comportamiento anómalo que afecte la integridad, confidencialidad y/o disponibilidad de los activos de información de la Institución.

Información Confidencial: Es toda información oral o escrita intercambiada entre “LAS PARTES” vinculada con la gestión de incidentes o vulnerabilidades, la cual será mantenida y protegida bajo estrictos controles. “LAS PARTES” acuerdan que no usarán, venderán, intercambiarán, publicarán, suministrarán o divulgarán la información confidencial incluyendo las copias fotostáticas, reproducciones, o información reproducida por medios electrónicos, a cualquier persona, sin la previa autorización por escrito, de conformidad con lo explícitamente estipulado en este Contrato de Adhesión.

Infraestructuras Críticas de la Nación: para los efectos del presente contrato, se entienden como las instalaciones, sistemas y redes, así como servicios y equipos físicos y de tecnología de la información cuya inhabilitación o destrucción tendría un impacto negativo sobre la población, la salud pública, la seguridad económica, el medio ambiente, la gobernabilidad o el eficaz funcionamiento del Estado y necesarios entre otros para la operación de Energía, el Petróleo, Telecomunicaciones, Industrias ligeras y comercio, distribución de agua y gestión de aguas residuales, sistemas de tráfico aéreo, Sistema Financiero, Sanitarios Públicos, y en general todo aquel que el Estado en ejercicio de sus funciones así lo determine.

Inventario de la Plataforma Tecnológica de Seguridad de Información: entendida esta



como todos aquellos medios utilizados para procesar, almacenar y transmitir la información, compuesta por la arquitectura y el inventario de los activos de información que esta contiene.

Manual de Políticas de Gestión de Incidentes: Es el compendio de pasos y mejores prácticas en el área de Gestión de Incidentes, que funciona como marco de referencia al personal encargado de ejecutar esta tarea, a fin de efectuarla de la manera más eficiente posible.

Riesgo: Es la probabilidad de que una amenaza se materialice.

Servicios Proactivos: Son aquellos servicios prestados a los miembros de la Comunidad con el objeto de prevenir la ocurrencia de eventos de seguridad (incidentes telemáticos o vulnerabilidades detectadas).

Servicios Reactivos: Son aquellos servicios prestados por “SUSCERTE” con posterioridad a la ocurrencia de eventos de seguridad (Incidentes telemáticos o vulnerabilidades detectadas), a los Asociados o a cualquier persona de carácter público o privado que así lo requiera.

Vulnerabilidad: Es la condición de susceptibilidad de un recurso a ser explotado o aprovechado por agentes internos/externos no autorizados.

DEL RESPONSABLE DE SEGURIDAD

CUARTA: “EL ASOCIADO” designará a un “RESPONSABLE DE SEGURIDAD”, y lo notificará por escrito a “SUSCERTE”; en un lapso no mayor de TRES (03) días hábiles, una vez suscrito el presente contrato; el “RESPONSABLE DE SEGURIDAD” tendrá entre otras, las siguientes funciones:

1. Notificar a “SUSCERTE” acerca de los eventos de seguridad informática ocurridos en su Institución.
2. Participar en las convocatorias realizadas por “SUSCERTE”, a fin de canalizar los procesos internos de mejora continua en los mecanismos de seguridad de información, empleados para la gestión de incidentes telemáticos ocurridos en la plataforma tecnológica de la Institución.
3. Facilitar la actualización periódica de la información de “EL ASOCIADO”, a saber:
 - 3.1. Ficha de la Institución (nombre, organización y datos de contacto).
 - 3.2. Inventario de la Plataforma Tecnológica de Seguridad de Información.
4. Identificar y notificar los riesgos y amenazas a las que está expuesta la plataforma tecnológica de su Institución, sus orígenes, recomendaciones y posibles estrategias de



SIN EFECTO

mitigación.

5. Desarrollar con el apoyo de "SUSCERTE", las estrategias y planes que permitan la continuidad de las operaciones de "EL ASOCIADO".
6. Clasificar los activos de información y los procesos medulares, en atención a su importancia dentro de la Institución.
7. Realizar evaluaciones periódicas de seguridad sobre la plataforma tecnológica, estableciendo un cronograma de mitigación para las vulnerabilidades detectadas.
8. Implementar formalmente las mejores prácticas, así como las recomendaciones formuladas por "SUSCERTE", en cuanto a los procedimientos a ser aplicados dentro de su Institución en materia de seguridad informática.
9. Seleccionar, instalar y mantener las herramientas de seguridad informática apropiadas para su plataforma tecnológica, considerando para ello las mejores prácticas, estándares internacionales y las recomendaciones formuladas por "SUSCERTE".

OBLIGACIONES DE "SUSCERTE"

QUINTA: "SUSCERTE" se compromete a prestar a "EL ASOCIADO", los servicios reactivos y proactivos que se indican a continuación:

SERVICIOS REACTIVOS: Comprenden los siguientes:

Manejo de Incidentes

- Atender de manera oportuna el o los incidentes que ocurran en la plataforma tecnológica del ente u órgano o las vulnerabilidades detectadas, a fin de facilitar el acceso a los activos de la información objeto de ataque, con la mayor celeridad posible.
- Prestar apoyo técnico ante incidentes telemáticos, a fin de determinar las posibles causas que los originaron.
- Administrar el registro de los incidentes donde se haya brindado alguna clase de apoyo a "EL ASOCIADO".
- Analizar e investigar la extensión del incidente y calificar la prioridad del mismo.
- Enviar informes sobre incidentes a los Equipos de Respuesta asociados al VenCERT.
- Asistir a "EL ASOCIADO", en la elaboración de avisos dirigidos a los usuarios o a los medios de comunicación.
- Coordinar con la Comunidad y entidades externas a la misma, bien sean nacionales o internacionales, la respuesta ante incidentes telemáticos o vulnerabilidades detectadas.
- Atender Incidentes in situ, según la gravedad de los mismos y de acuerdo a las necesidades de "EL ASOCIADO".



SIN EFECTO

Manejo de Vulnerabilidades

- Recibir y analizar información sobre las vulnerabilidades en los Sistemas de Información de los Asociados a la Comunidad.
- Hacer las debidas recomendaciones ante las vulnerabilidades identificadas y analizadas.
- Coordinar las respuestas ante vulnerabilidades.
- Prestar asesoría orientada a la resolución de vulnerabilidades detectadas.
- Identificar y analizar “en línea” las vulnerabilidades de los Sistemas de Información de la Comunidad expuestos en Internet o ubicados en redes internas, de acuerdo a la solicitud de los Asociados.

SERVICIOS PROACTIVOS: Comprenden los siguientes:

- Publicar alertas y avisos, a fin de prevenir posibles ataques o identificar nuevas vulnerabilidades.
- Activar el sistema de alerta temprana de incidentes, a través del establecimiento de una red de sensores y análisis de registros de actividad anónimos, que permitan analizar la información de manera centralizada para facilitar la toma de decisiones.
- Ejecutar programas de formación y capacitación continua a su personal interno, así como a los miembros de la Comunidad, con el objeto de fortalecer los mecanismos de seguridad de la información.
- Brindar asesoramiento sobre las mejoras pertinentes, en relación con la infraestructura de los sistemas de información de “EL ASOCIADO”.
- Notificar inmediatamente a “EL ASOCIADO” sobre cualquier incumplimiento distinto de las obligaciones de confidencialidad, para que éste último proceda a resolverlo en el plazo de setenta y dos (72) horas contadas a partir de la notificación.

OBLIGACIONES DE “EL ASOCIADO”

SEXTA: Serán obligaciones de “EL ASOCIADO”:

1. Cumplir y hacer cumplir a cabalidad todas y cada una de las cláusulas estipuladas en el presente contrato.
2. Suscribir Acuerdos de Confidencialidad con su personal interno y terceros, conforme a lo dispuesto en las cláusulas Novena y Décima del presente contrato.
3. Designar a la persona que actuará como “RESPONSABLE DE SEGURIDAD” ante “SUSCERTE” y a su suplente en caso de ausencia, conforme a lo dispuesto en la Cláusula Cuarta; así como notificar de inmediato a “SUSCERTE” sobre cualquier cambio que ocurriese sobre la persona que ejerza tales funciones.
4. Facilitar a “SUSCERTE” toda la información que sea requerida, a fin de gestionar



SIN EFECTO

cualquier incidente o vulnerabilidad encontrada.

5. Usar la información recibida por “SUSCERTE” clasificada según la normativa legal o sublegal aplicable, exclusivamente para los fines a los que deba ser destinada.
6. Actuar conforme a los estándares, códigos éticos y manuales de mejores prácticas internacionalmente aceptados.
7. Facilitar un listado de proveedores y prestadores de servicios técnicos, así como un inventario de los equipos informáticos empleados en materia de seguridad de la información, e informar periódicamente sobre cualquier cambio vinculado a éstos.
8. Formular denuncias ante los órganos competentes, cuando el incidente telemático del que ha sido objeto, sea calificado como un hecho punible.
9. Disponer de un Manual de Políticas de Gestión de Incidentes, conforme a los parámetros mínimos exigidos por “SUSCERTE”; o en su defecto adoptar el suministrado por ésta.

DEL TRATAMIENTO A LA INFORMACIÓN

SÉPTIMA: “LAS PARTES” se comprometen a usar la información intercambiada entre sí o puesta a disposición bien sea que se trate de información propia o de terceros, única y exclusivamente a los fines de dar cumplimiento con el objeto del presente contrato, para ello deberán protegerla conforme a la normativa legal o sublegal aplicable.

TITULARIDAD DE LA INFORMACIÓN/ LICENCIA Y DERECHOS RELACIONADOS

OCTAVA: Toda la Información intercambiada u obtenida por “LAS PARTES” en virtud del presente Contrato de Adhesión, seguirá siendo propiedad de quien la suministra; y se respetarán los derechos de titularidad que existieran sobre la misma, en caso de no ser propiedad de quien la suministra; en consecuencia, ninguna de “LAS PARTES” adquirirá, directa o indirectamente derechos sobre la información que recibe en razón del objeto del presente instrumento.

DE LA CONFIDENCIALIDAD

NOVENA: “EL ASOCIADO” se compromete a suscribir Acuerdos de Confidencialidad con su personal interno al cual le sean asignadas funciones en materia de Seguridad de la Información, con la prohibición expresa de reproducir, divulgar, transferir, distribuir, transmitir o publicar, toda información (oral o escrita en cualquier formato o contenida en cualquier dispositivo), vinculada con la gestión de incidentes o vulnerabilidades y que requiera protección dentro y fuera de la Institución, conforme a las condiciones establecidas en la normativa legal y sublegal aplicable.

DE LA CONFIDENCIALIDAD ANTE TERCEROS

DÉCIMA: “EL ASOCIADO” se compromete a suscribir convenios de confidencialidad con



terceros distintos de la comunidad, que presten servicios vinculados con las actividades relativas a la gestión de incidentes o vulnerabilidades. Dichos convenios serán conforme a los parámetros establecidos por “SUSCERTE”.

DEBER DE NOTIFICACION

DÉCIMA PRIMERA: “LAS PARTES” deberán notificarse de inmediato y de forma detallada, si cualquiera de ellas está en conocimiento de que alguno de sus representantes, filiales, oficiales, directores o empleados (o cualquier otra persona que haya recibido la información confidencial directa o indirectamente) ha divulgado, usado, o cuando existan indicios de que la información confidencial se verá comprometida, contraviniendo las condiciones establecidas en el presente instrumento.

RESPONSABILIDADES DERIVADAS DEL INCUMPLIMIENTO SOBRE CONFIDENCIALIDAD

DÉCIMA SEGUNDA: Cualquier incumplimiento a las disposiciones establecidas en el presente Contrato relativas a las obligaciones sobre confidencialidad a la que tenga acceso, podrá constituir un ilícito de naturaleza penal, conforme a lo establecido en la Ley Especial Contra los Delitos Informáticos y demás leyes relacionadas con la violación a la intimidad, reserva e interceptación de comunicaciones, sabotaje, utilización indebida de información privilegiada; sujetándose en consecuencia a las sanciones que prevén dichas disposiciones. Asimismo podrá dar lugar a responsabilidad civil, administrativa y disciplinaria según sea el caso, de conformidad con el ordenamiento jurídico vigente.

DE LA REVELACIÓN AUTORIZADA DE INFORMACIÓN

DÉCIMA TERCERA: “EL ASOCIADO” podrá divulgar la Información Técnica recibida de “SUSCERTE”, a sus filiales, empleados, agentes autorizados e instituciones gubernamentales, únicamente en la medida en que tales entidades estén relacionadas o sean afectadas por la ocurrencia de incidentes o potencialmente afectadas por causa de vulnerabilidades detectadas, siempre y cuando se notifique previamente por escrito a “SUSCERTE”, y exista un acuerdo de confidencialidad suscrito entre “EL ASOCIADO” y la persona a quien se le suministre dicha información.

INFORMACIÓN NO SUJETA A CONFIDENCIALIDAD

DÉCIMA CUARTA: No constituirá información confidencial aquella información que “LAS PARTES” demuestren fehacientemente que:

1. Sea del dominio público.
2. Cuando al momento de su divulgación, era conocida por “LAS PARTES” y no estaba sujeta a ninguna obligación de confidencialidad o restricción de uso, y que la misma no había sido obtenida directa o indirectamente de “LAS PARTES”.

J/19

RESERVA LEGAL
VISTO
8/11
SUSCERTE

SIN EFFETTO

3. Luego de ser suministrada por alguna de "LAS PARTES", ésta sea publicada o se haga del dominio público sin ningún acto u omisión de "LAS PARTES", o de las personas a quienes haya suministrado dicha información.
4. Si "LAS PARTES" transmiten información sin clasificación de seguridad o restricciones de uso, conforme a la normativa legal o sublegal aplicable.
5. Haya sido divulgada en el marco de aplicación de una norma legal o sublegal, o bien mediante orden judicial.

DE LOS PROCEDIMIENTOS DE CONTROL DE LA INFORMACIÓN

DÉCIMA QUINTA: "LAS PARTES" adoptarán y mantendrán controles para el resguardo de toda la Información Confidencial que reciban, en virtud de lo cual se comprometen a:

1. Mantener una lista de todas las personas a quienes se les divulga Información de carácter Confidencial, directa o indirectamente, incluyendo sin limitación, a los empleados, funcionarios, directores, asesores, agentes y representantes de "EL ASOCIADO" y sus Filiales, que tengan acceso a esa Información.
2. Garantizar en todo momento que la Información Confidencial se mantenga en un lugar seguro y que esté protegida adecuadamente contra robo, daño, pérdida o acceso no autorizado, a través de la normativa legal y sublegal aplicable.

DE LA DEVOLUCIÓN DE LA INFORMACIÓN CONFIDENCIAL

DÉCIMA SEXTA: Al vencimiento o terminación del presente contrato, "LAS PARTES" procederán a devolver o destruir según sea el caso, todo el material en original y copia contentivo de Información Confidencial, que haya sido facilitada o aquella generada como resultado de dicha información; de igual modo procederán a borrar toda Información Confidencial de cualquier computador, equipo o dispositivo que la contenga, excepto aquella retenida en los sistemas computarizados de respaldo, conforme a la normativa legal y sublegal aplicable; todo ello previa solicitud por escrito, en cuyo caso deberá ser devuelta dentro de los quince (15) días siguientes a la recepción de la notificación.

MODIFICACIÓN DE LAS CONDICIONES DEL CONTRATO

DÉCIMA SÉPTIMA: Toda modificación que se produzca con ocasión del funcionamiento del VenCERT y las novedades que se vayan incorporando, relacionadas con la prestación concreta de determinados servicios, se harán por pacto expreso.

DE LA VIGENCIA

DÉCIMA OCTAVA: El presente Contrato de Adhesión tendrá una vigencia de **TRES (3) AÑOS** contados a partir de su suscripción, pudiendo ser renovado automáticamente por períodos iguales, salvo que "LAS PARTES" decidan de mutuo acuerdo, rescindirlo anticipadamente mediante notificación escrita que justifique los motivos de dicha decisión.

ASESORIA LEGAL
19/11/2011
SUSCERTE

SIN EFECTO

DE LA TERMINACIÓN ANTICIPADA DEL CONTRATO

DÉCIMA NOVENA: Cualquiera de “LAS PARTES” puede rescindir el presente Contrato, si demuestra que la otra parte infringió cualquier garantía, disposición u obligación del presente instrumento, distinta de las obligaciones referidas a la Información Confidencial, y no subsanó el incumplimiento, en el plazo de quince (15) días contados a partir de la notificación que de la infracción haya recibido por escrito la parte infractora.

DE LAS RESOLUCIONES

VIGÉSIMA: “LAS PARTES” podrán resolver de pleno derecho el presente Contrato de común acuerdo cuando existan razones suficientes que lo justifiquen, notificando a la otra parte por lo menos con treinta (30) días de antelación a la resolución del mismo.

DEL CASO FORTUITO O FUERZA MAYOR

VIGÉSIMA PRIMERA: Las disposiciones establecidas en el presente contrato relativas a la confidencialidad de la información, se mantendrán vigentes aún estando en presencia de un caso fortuito o fuerza mayor, tales como: guerra, actos de Estado, insurrección, conmoción civil, disturbios, movilizaciones, huelgas, bloqueos, desastres naturales, etc.); por lo que “LAS PARTES” no quedarán relevadas de su compromiso de confidencialidad a que se obligan en los casos antes citados.

NOTIFICACIONES

VIGÉSIMA SEGUNDA: Cualquier notificación y/o solicitud que deba o pueda realizarse entre “LAS PARTES” con motivo del presente contrato, se hará por cualquier medio que permita dejar constancia del contenido de la comunicación y de su recepción (por escrito o correo firmado electrónicamente). En caso de notificaciones por escrito, “LAS PARTES” fijan las direcciones siguientes:

- **“SUSCERTE”:** Avenida Andrés Bello, Sector Guaicaipuro, Torre Fondo Común, piso 13, Municipio Libertador, Caracas -Venezuela.
Teléfonos: (0212) 578.56.72 / 578.56.74
Correo Electrónico: superintendencia@suscerte.gob.ve
Dirección de Internet: <http://www.suscerte.gob.ve>
- **“EL ASOCIADO”:** Oficina Nacional de Contabilidad Pública (ONCOP), Avenida Urdaneta, Esquina Carmelitas, Edificio Norte del Ministerio del Poder Popular de Planificación y Finanzas, Mezzanina, Municipio Libertador, Caracas-Venezuela.
Teléfonos: (0212) 802.49.03/ 802.49.43
Correo Electrónico: lmulet@mppef.gob.ve
Dirección de Internet: <http://www.oncop.gob.ve>



SIN EFECTO

SOLUCIÓN DE CONFLICTOS

VIGÉSIMA TERCERA: Las controversias relativas sobre las obligaciones distintas de Confidencialidad que guarden relación con el presente Acuerdo o derive de su interpretación, aplicación, ejecución o cumplimiento del mismo, serán resueltas de manera amistosa por **“LAS PARTES”**, quienes se obligan a realizar sus mejores esfuerzos para solventarlas dentro de un lapso de **QUINCE (15) DÍAS HÁBILES**, contados a partir de la formulación del reclamo; siempre y cuando la naturaleza de la controversia lo permita. Así mismo, **“LAS PARTES”**, dentro de las discusiones amistosas, podrán acordar consultar a expertos técnicos para que emitan opinión sobre aspectos relacionados con la diferencia ocurrida, en cuyo caso, no serán vinculantes para **“LAS PARTES”** las conclusiones y/o recomendaciones emitidas por los expertos

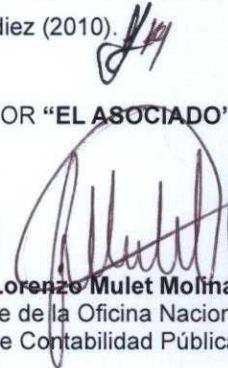
Se hacen cuatro (4) ejemplares de un mismo tenor y a un sólo efecto. En Caracas, a los veinticinco (25) días del mes de noviembre del año dos mil diez (2010).

POR **“SUSCERTE”**,



Niurka Hernández González
Superintendente

POR **“EL ASOCIADO”**,



Lorenzo Mulet Molina
Jefe de la Oficina Nacional de Contabilidad Pública



ASESORIA LEGAL
VIS
SUSCERTE
11/11



SIN EFECTO