SUSCERTE/OCJ/VENCERT/001/2022

CONVENIO DE ADHESIÓN AL SISTEMA NACIONAL DE GESTIÓN DE INCIDENTES TELEMÁTICOS (VENCERT)

Entre la **OFICINA NACIONAL DE CONTABILIDAD PÚBLICA (ONCOP),** creado a través del Artículo 126 de la Ley Orgánica de la Administración Financiera del Sector Público, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 37.029 de fecha 05 de septiembre de 2.000, representado en este acto por el ciudadano **FERNANDO YAMIR ZERPA DÍAZ**, titular de la Cédula de Identidad Nº **V- 14.700.437,** en su carácter de **JEFE DE LA OFICINA NACIONAL DE CONTABILIDAD PÚBLICA (ONCOP)**, designado mediante la Resolución N° 019 de fecha 03 de febrero del 2016, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N.º 40.842 de la misma fecha, de conformidad con lo establecido en los numerales 1 y 9 del artículo 7 del Reglamento Parcial Nº 4 de la Ley Orgánica de la Administración Financiera del Sector Público, sobre el Sistema de Contabilidad Pública, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 38.333 de fecha 12 de diciembre de 2005, y en ejercicio de la delegación otorgada mediante el artículo 1 numerales 2 de la Resolución Nº 008 de fecha 14 de marzo de 2019, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N°41.598 de la misma fecha, quien a los efectos de este Convenio se denominará **"EL ASOCIADO",** por una parte y por la otra la **SUPERINTENDENCIA DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA (SUSCERTE)**, creada bajo el Decreto con Fuerza de Ley Nº 1.204 de Mensajes de Datos y Firmas Electrónicas, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 37.148 del 28 de febrero de 2.001, representada en este acto por el ciudadano **CARLOS EDUARDO PARRA FALCÓN,** titular de la Cédula de Identidad **N° V-6.728.453**, en su carácter de Superintendente de Servicios de Certificación Electrónica, según nombramiento contenido en la Resolución Nº 031 del 03 de julio del 2.019, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 41.667 de fecha 03 julio de 2.019, suficientemente facultado para este acto de conformidad con lo dispuesto en la Resolución N° 050 de fecha 14 de agosto del 2.019, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 41.700 de fecha 22 de agosto del 2.019, quien en lo sucesivo y a los efectos de este documento se denominará "**SUSCERTE"**; quienes en su conjunto se denominarán **"LAS PARTES"**, han convenido en celebrar como en efecto celebran el presente **CONVENIO DE ADHESIÓN AL SISTEMA NACIONAL DE GESTIÓN DE INCIDENTES TELEMÁTICOS (VENCERT)**, el cual se regirá de conformidad con las cláusulas siguientes:

OBJETO DEL CONVENIO

PRIMERA: El presente Convenio tiene por objeto establecer los términos y condiciones que regirán el proceso de adhesión de **"EL ASOCIADO"** al Sistema Nacional de Gestión de Incidentes Telemáticos (VENCERT), con la finalidad que éste le preste apoyo ante incidentes telemáticos y vulnerabilidades, bajo las condiciones y obligaciones previstas durante la vigencia de este instrumento.

FINALIDAD DEL SISTEMA NACIONAL DE GESTIÓN DE INCIDENTES TELEMÁTICOS

SEGUNDA: El Sistema Nacional de Gestión de Incidentes Telemáticos (VENCERT), tiene como fin 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 que afecten la seguridad de información, en conjunto con otros entes y órganos del Poder Público Nacional. De igual forma, es el ente 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 convenio, se entenderá por:

Activos de Información: Toda información en cualquiera de sus formas y soportes, impresa, manuscrita, oral, electrónica y visual, a la cual cada institución, en atención a su función y sus intereses, le ha atribuido un valor determinado en razón de la trascendencia de dicha información. Esta definición involucra la plataforma tecnológica de la Institución.

Seguridad de la información: Condición que resulta del establecimiento y mantenimiento de medios de protección, que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso no autorizado a la información, o que afecten la operatividad de las funciones de un sistema de computación, bajo los principios de confidencialidad, integridad, privacidad y disponibilidad de la información.

Amenaza: Todo aquello que tenga una posibilidad o probabilidad de ocurrir como causante de daño a los activos de información, se incluyen actos dirigidos, deliberados, 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).

Comunidad: Conjunto de asociados al Sistema Nacional de Gestión de Incidentes Telemáticos (VENCERT).

Confidencialidad: 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, autenticidad 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.

Informe de Evaluación de Seguridad (IES): Informe que contiene la evaluación de los sistemas de información e infraestructura tecnológica de un determinado órgano o ente, a través del manejo de vulnerabilidades e incidentes de seguridad informática, elaborado por especialistas en hacking ético. Consta de dos fases, una de Recopilación de Información y Análisis de Vulnerabilidades (RIAV), y otra de Comprobación y Análisis de Gravedad de las Vulnerabilidades Detectadas (CAGVD).

Información Confidencial: 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.

Manual de Políticas de Gestión de Incidentes: 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 materializarlos de la manera más eficiente posible.

Riesgo: Probabilidad de que una amenaza se materialice.

Servicios Proactivos: Servicios prestados por **"SUSCERTE"** a los miembros de la comunidad con el objeto de prevenir la ocurrencia de eventos de seguridad (incidentes telemáticos o vulnerabilidades detectadas).

Servicios Reactivos: 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: Condición de susceptibilidad de un recurso a ser explotado o aprovechado por agentes internos/externos no autorizados.

Inventario de la Plataforma Tecnológica de Seguridad de Información: Medios utilizados para procesar, almacenar y transmitir la información, compuesta por la arquitectura y el inventario de los activos de información que ésta contiene.

DEL RESPONSABLE DE SEGURIDAD

CUARTA: El Director, Gerente o su equivalente, de la Oficina de Tecnología de la Información de **"EL ASOCIADO",** es el responsable de la seguridad de la información de su respectivo organismo y se denominará en lo sucesivo **"EL RESPONSABLE"**, y tendrá las siguientes obligaciones:

1.**“EL RESPONSABLE”** desarrollará el instrumento normativo interno sobre seguridad informática, teniendo como marco referencial el presente convenio.

2.**“EL RESPONSABLE”** notificará a **“SUSCERTE”** acerca de los eventos de seguridad informática ocurridos en su institución, en un lapso no mayor a tres (03) días continuos.

3.**“EL RESPONSABLE”** atenderá y dará prioridad a las convocatorias realizadas por **“SUSCERTE”**, a fin de canalizar los procesos internos de mejoras continuas en los mecanismos de seguridad de información, empleados para la gestión de incidentes telemáticos ocurridos en la plataforma tecnológica de la institución.

4.**“EL RESPONSABLE”** facilitará la actualización periódica de la información de **“EL ASOCIADO”**, a saber:

(a) Ficha de la Institución (nombre, organización y datos de contacto).

(b) Inventario de la Plataforma Tecnológica de Seguridad de la Información.

5.**“EL RESPONSABLE”** identificará y notificará continuamente a **“SUSCERTE”** los riesgos y amenazas a las que está expuesta la plataforma tecnológica de su Institución, sus orígenes, recomendaciones y posibles estrategias de mitigación.

6.**“EL RESPONSABLE”** desarrollará con el apoyo de **“SUSCERTE”**, las estrategias y planes que permitan la continuidad de las operaciones de **“EL ASOCIADO”**.

7.**“EL RESPONSABLE”** clasificará los activos de información y los procesos medulares, en atención a su importancia dentro de la Institución.

8.**“EL RESPONSABLE”** realizará las evaluaciones periódicas de seguridad sobre la plataforma tecnológica, estableciendo un cronograma de mitigación para las vulnerabilidades detectadas.

9.**“EL RESPONSABLE”** implementará formalmente las recomendaciones formuladas por **“SUSCERTE”**, en cuanto a los procedimientos a ser aplicados dentro de su Institución en materia de seguridad informática.

10.**“EL RESPONSABLE”** seleccionará, instalará y mantendrá las mejores prácticas en las herramientas de seguridad informática apropiadas para su plataforma tecnológica, considerando para ello, los estándares internacionales y las recomendaciones formuladas por **“SUSCERTE”**.

DE LA ATENCIÓN A LOS INCIDENTES TELEMÁTICOS

QUINTA: “EL RESPONSABLE” está obligado a suministrar a **“SUSCERTE”,** toda la información del incidente que sea detectado por sus especialistas o notificado por **“SUSCERTE”**, para su posterior análisis y detección de la causa, dentro de las cuarenta y

ocho (48) horas siguientes a la detección o notificación. Para la solicitud y envío de cualquier información se dará prioridad a los medios electrónicos. Cualquier negligencia o retraso en el suministro de la información por parte de **"EL RESPONSABLE",** así como cualquier obstaculización en la investigación que **"SUSCERTE"** o las autoridades competentes desplieguen para identificar las causas de un incidente, será reportado mediante informe a la máxima autoridad del órgano para que tome las acciones administrativas que se requieran, sin perjuicio de la notificación que se haga al órgano de investigación penal correspondiente, en caso de presumirse la comisión de un hecho punible.

PARÁGRAFO ÚNICO: Una vez que **"EL RESPONSABLE"** suministre la información requerida por **"SUSCERTE"** para el análisis del incidente, ésta procederá a informar las recomendaciones necesarias para ser implementadas por el órgano en un plazo de quince (15) días continuos siguientes a la recepción del informe de recomendaciones.

DE LAS EVALUACIONES DE SEGURIDAD

SEXTA: "SUSCERTE" evaluará, por lo menos una (01) vez al año, los sistemas de información e infraestructura tecnológica de los órganos con los cuales tenga suscrito **CONVENIO DE ADHESIÓN AL SISTEMA NACIONAL DE GESTIÓN DE INCIDENTES TELEMÁTICOS (VENCERT)**, y de cualquier otro órgano que contemple dentro de su planificación, emitiendo con posterioridad a la evaluación, el correspondiente **Informe de Evaluación de Seguridad (IES).**

SÉPTIMA: "El RESPONSABLE" deberá, una vez recibido el Informe de Evaluación de Seguridad (IES) de su respectivo órgano elaborado por **"SUSCERTE"**, realizar todas las correcciones sobre las vulnerabilidades detectadas, en un lapso de treinta (30) días continuos contados a partir de la fecha de recepción. "**SUSCERTE"** realizará el seguimiento correspondiente para la implementación de estas correcciones y prestará la asesoría necesaria para que las mismas se realicen con éxito.

SÉPTIMA: "El RESPONSABLE" deberá, realizar todas las correcciones sobre las vulnerabilidades detectadas, en un lapso de treinta (30) días continuos contados a partir de la de recepción del Informe de Evaluación de Seguridad (IES) de su respectivo órgano elaborado por **"SUSCERTE"**, y éste realizará el seguimiento correspondiente para la implementación de estas correcciones y prestará la asesoría necesaria para que las mismas se realicen con éxito.

DE LA OBLIGATORIEDAD DE ACATAR LAS RECOMENDACIONES EN MATERIA DE SEGURIDAD INFORMÁTICA

OCTAVA: Las recomendaciones señaladas en el parágrafo único de la cláusula quinta, así como las correcciones especificadas en la cláusula séptima del presente Convenio, son de obligatorio acatamiento por parte de **"EL RESPONSABLE".** Si transcurridos los lapsos señalados para el cumplimiento de aquellas, **"EL RESPONSABLE"** no ha implementado las recomendaciones y/o correcciones en su organismo, sin haber causas para ello,

"**SUSCERTE"** procederá a ratificar a **"EL RESPONSABLE"** las recomendaciones o correcciones formuladas, dándole un plazo de cinco (05) días hábiles para su ejecución. Si vencido el nuevo plazo otorgado, **"EL RESPONSABLE"** no ha implementado las recomendaciones o correcciones indicadas por **"SUSCERTE",** ésta procederá a remitir un **Informe de Cierre con Vulnerabilidades (ICV)**, a la máxima autoridad del órgano y a la Comisión Nacional de las Tecnologías de Información (CONATI), en caso de violación de normas instruccionales en materia de seguridad informática, a efectos de iniciar el procedimiento administrativo sancionatorio correspondiente.

OBLIGACIONES DE "SUSCERTE"

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

1. SERVICIOS REACTIVOS:

(a) Manejo de Incidentes

- Atender de manera oportuna el o los incidentes que ocurran en la plataforma tecnológica del 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 originen.
- Llevar un 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 a 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"**.

b) 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 con "**EL ASOCIADO"** las respuestas de las vulnerabilidades.
- Ofrecer 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.

2. SERVICIOS PROACTIVOS:

- 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.
- Brindar asesoría sobre las mejoras pertinentes en relación con la infraestructura de los sistemas de información de **"EL ASOCIADO"**.

•Notificar inmediatamente a **"EL ASOCIADO"**, cualquier hecho que vulnere el objeto del presente Convenio o presuma incumplimiento del mismo por parte de **"EL ASOCIADO",** para que éste último proceda a resolverlo en el plazo de tres (03) días continuos, contados a partir de la notificación.

OBLIGACIONES DE "EL ASOCIADO"

DÉCIMA: Serán obligaciones de **"EL ASOCIADO":**
1. Cumplir y hacer cumplir todas y cada una de las cláusulas estipuladas en el presente convenio.
2. Suscribir acuerdos de confidencialidad con su personal interno y terceros, conforme a lo dispuesto en las cláusulas décima tercera y décima cuarta del presente convenio.
3. Facilitar a **"SUSCERTE"** toda la información que sea requerida, a fin de gestionar cualquier incidente o vulnerabilidad encontrada.
4. Usar la información suministrada por **"SUSCERTE",** clasificada según la normativa legal o sublegal aplicable, exclusivamente para los fines a los que deba ser destinada.

5. Actuar conforme a los estándares, códigos éticos y manuales de buenas prácticas internacionalmente aceptados o recomendados por **"SUSCERTE".**
6. 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.
7. Formular denuncias ante los órganos competentes, cuando el incidente telemático del que ha sido objeto, constituya presumiblemente un hecho punible.
8. 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.
9. Coadyuvar con **"SUSCERTE"** en la comprobación periódica que ésta haga sobre los niveles de seguridad de sus plataformas tecnológicas, con el fin de poder realizar acciones preventivas ante futuros ataques.

DEL TRATAMIENTO DE LA INFORMACIÓN

DÉCIMA PRIMERA: Toda información que se genere con ocasión al cumplimiento del presente Convenio se considera de carácter confidencial. **"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 al objeto del presente Convenio, para ello deberán darle la protección debida, conforme a la normativa legal o sublegal aplicable. "**LAS PARTES"** acuerdan que no usarán, venderán, intercambiarán, publicarán, suministrarán o divulgarán la información confidencial, incluyendo copias fotostática, reproducciones o información reproducida por medios electrónicos, a cualquier persona, sin la previa autorización por escrito de la otra parte, sin perjuicio del deber de informar a las máximas autoridades jerárquicas de los órganos, así como de las autoridades competentes cuando se presuma la comisión de un hecho punible.

TITULARIDAD DE LA INFORMACIÓN/ LICENCIA Y DERECHOS RELACIONADOS

DÉCIMA SEGUNDA: Toda la información intercambiada u obtenida por **"LAS PARTES"** en

virtud del presente Convenio de Adhesión, seguirá siendo propiedad de quien la suministre, y se respetarán los derechos de titularidad que existieren sobre la misma en caso de no ser propiedad de quien la suministre; 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

DÉCIMA TERCERA: "EL ASOCIADO" deberá 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 CUARTA: "EL ASOCIADO" deberá suscribir convenios de confidencialidad con terceros, 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 NOTIFICACIÓN

DÉCIMA QUINTA: "LAS PARTES" deberán notificarse de inmediato y de forma detallada, cuando estén 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 existieren indicios de divulgación o uso, de la información confidencial o de que ésta estuviere comprometida, contraviniendo las condiciones establecidas en el presente instrumento.

DE LA REVELACIÓN AUTORIZADA DE INFORMACIÓN

DÉCIMA SEXTA: "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 por medio electrónico previamente a **"SUSCERTE"** y/o 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 SÉPTIMA: No constituirá información confidencial aquella 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"**.
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, 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 OCTAVA: "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",** entes adscritos 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 NOVENA: Al vencimiento o terminación del presente convenio, **"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 hábiles siguientes a la recepción de la notificación.

DEL CASO FORTUITO O FUERZA MAYOR

VIGÉSIMA: Las disposiciones establecidas en el presente Convenio relativas a la confidencialidad de la información, se mantendrán vigentes aún estando en presencia de un caso fortuito o fuerza mayor, tales como: guerra, insurrección, conmoción civil, golpe de estado, 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.

DE LA VIGENCIA

VIGÉSIMA PRIMERA: El presente Convenio de Adhesión tendrá vigencia de **dos (02) años** a partir de su suscripción.

NOTIFICACIONES

VIGÉSIMA SEGUNDA: Cualquier notificación y/o solicitud que deba o pueda realizarse entre **"LAS PARTES"** con motivo del presente Convenio, 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 / 74
Correo Electrónico: incidentes@vencert.gob.ve

-"EL ASOCIADO": Av. Urdaneta, Esquina de Carmelitas, Edificio Norte del Ministerio del Poder Popular de Economía, Finanzas y Comercio Exterior, Mezzanina, Municipio Libertador del Distrito Capital.
Teléfonos: (0212) 802.49.19/ 39
Correo electrónico: despachoncop@mppbf.gob.ve

SOLUCIÓN DE CONFLICTOS

VIGÉSIMA TERCERA: Las controversias relativas a la confidencialidad de la información, o cualquier otro aspecto que guarde relación con el presente Convenio, o que se derive de su interpretación, aplicación, ejecución o cumplimiento, 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.

Se hacen dos (02) ejemplares de un mismo tenor y a un sólo efecto en Caracas, a los veintitrés (23) días del mes de marzo de 2.022.

Por "EL ASOCIADO"

Fernando Yamir Zerpa Diaz
Firmado digitalmente por Fernando Yamir Zerpa Diaz
Fecha: 2022.03.23 14:19:24 -04'00'

FERNANDO ZERPA DIAZ
Jefe de la Oficina Nacional de Contabilidad Pública
Resolución Nº 019, publicada en la G.O.R.B.V. Nº 40.842 de fecha 03 de febrero de 2016; y la Resolución N° 008, publicada en la G.O.R.B.V. N° 41.598 de fecha 14 de marzo de 2019.

Por "SUSCERTE"

Carlos Eduardo Parra Falcon
Firmado Por: Carlos Eduardo Parra Falcon
Fecha: 23-03-2022 18:26:22
Razón: Convenio
Ubicación: Despacho del Superintendente
Contacto: cparra@suscerte.gob.ve
SOFE Escritorio FIIIDT-CSICE

CARLOS EDUARDO PARRA FALCÓN
Superintendente de Servicios de Certificación Electrónica
Resolución N.º 031 del 03 de julio de 2.019, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 41.667 de la misma fecha, y facultado para este acto por Resolución N° 050 de fecha 14 de agosto de 2.019, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 41.700 en fecha 22 de agosto de 2.019.