Requisitos de Ciberseguridad

Los presentes Requisitos de Ciberseguridad (según dicho término se define más adelante), son de carácter obligatorio e irrenunciable y aplicarán para usted (el "**Prestador**") en relación con los servicios y/o bienes que vayan a prestar o suministrar a Infraestructura Energética Nova, S.A.B. de C.V. o cualquiera de sus subsidiarias (la "**Empresa**"), desde el momento en que firmen este documento, aun cuando a la fecha no se haya firmado un contrato o una orden de compra (indistintamente uno y otro, un "**Instrumento**").

Este documento representa los principales Requisitos de Ciberseguridad y se entenderán por incluidos con toda fuerza y validez en el Instrumento cuando aquél se firme, basado en las plantillas más recientes, incluida la ciberseguridad después de su finalización.

El Prestador que entregue el servicio y/o bien a la Empresa, acuerda maximizar la seguridad de sus personas, procesos y tecnologías a lo largo de la vigencia del Instrumento, de conformidad con los requisitos aquí establecidos y todas las leyes aplicables (conjuntamente, los "**Requisitos de Ciberseguridad**"). La Empresa se reserva el derecho de validar la efectividad de los Requisitos de Ciberseguridad y el Prestador deberá proporcionar evidencia de una validación independiente por parte de terceros, a solicitud de la Empresa. La Empresa podrá modificar los Requisitos de Ciberseguridad mediante notificación por escrito al Prestador durante la vigencia del Instrumento, en común acuerdo se definirán plazos razonables para cumplir con los cambios a los requisitos. El término "**Producto**", como se usa en este documento, significa cualquier servicio, hardware o *software* proporcionado por el Prestador a la Empresa en términos del Instrumento.

Las operaciones de los productos y servicios entregados a la Empresa se refieren a todos los activos, procesos y sistemas (incluidos los sistemas de información), los datos y metadatos (incluidos los datos del Cliente), el personal y los sitios, utilizados o procesados por el Prestador de vez en cuando en el cumplimiento de este acuerdo.

Este documento describe los requisitos de ciberseguridad genéricos para los servicios o productos entregados.

1.0 Marco de ciberseguridad. El Prestador deberá tener un marco maduro para abordar un enfoque seguro por diseño, defensa en profundidad para diseñar, construir, mantener y retirar Productos y / o Servicios (el "**Marco de Ciberseguridad**"). El Marco de Ciberseguridad se establecerá en el sentido de la serie ISO 2700x / IEC 62443 / Cloud Security Alliance / NIST 800 - xx e incluirá, entre otros: políticas, estándares y procesos de seguridad de la información, y la gobernanza interna necesaria para proteger adecuadamente la confidencialidad, integridad y disponibilidad del Contenido, Producto y/o Servicio frente al panorama actual de amenazas generales y específicas del Prestador. El Prestador incluirá la Ciberseguridad por diseño y por defecto en su Producto y/o Servicio y en todos los Sistemas de Información relacionados, de acuerdo con las Buenas Prácticas de Seguridad establecidas en los marcos de control enunciados en este párrafo ("**seguridad por diseño**" y "**seguridad por defecto**"). Esto incluye el ciclo de vida completo del Producto y / o Servicio (consulte IEC 62443-4-1), así como todos los sistemas de información relacionados (consulte ISO 2700x) necesarios para su entrega.

2.0 Controles de Acceso. El Prestador proporcionará controles de acceso, autorización y responsabilidad basados en roles dentro de su producto, que cumplan con las pautas y requisitos establecidos en los Requisitos de Ciberseguridad. Los controles deben ser apropiados para las

políticas de la Empresa. Además, el producto proporcionará roles separados para los usuarios, administradores, desarrolladores y personal de soporte del día a día, y que el acceso proporcionará acceso sólo al personal autorizado que haya recibido la capacitación adecuada sobre responsabilidades administrativas, procesos y procedimientos de seguridad. El control del acceso deberá proporcionar el acceso mínimo requerido para cada rol y denegará el acceso a usuarios no autorizados de acuerdo con la vigencia del servicio y verificados por el usuario solicitante del servicio. Los productos alojados por el Prestador, si los hubiere, incluirán controles para proteger las cuentas de servicio y las cuentas genéricas, con la finalidad de evitar su modificación o uso no autorizado. Las contraseñas de las cuentas de servicio y las genéricas deben cambiarse al menos cada tres meses. El Prestador verificará y divulgará todos los métodos conocidos para acceder a los productos, y no accederá ni permitirá que otros accedan a los productos sin el consentimiento previo de la Empresa (aparte de los productos alojados, e incluso en esos casos, solamente el Prestador podrá acceder a los productos alojados). El Prestador también garantiza que los administradores del entorno de producción de los productos alojados utilizarán autenticación de dos factores al proporcionar soporte administrativo remoto para el entorno. Antes de que el Servicio esté listo, el Prestador deberá proporcionar a la Empresa el concepto de función de autorización y autenticación detallada general actual (incluida la cantidad aproximada de personas autorizadas por función), que garantiza un acceso restringido a los datos y procesos basados en los principios de "privilegio mínimo", "necesidad de saber" y "segregación de funciones". El entorno del Prestador ofrecerá una autenticación de dos factores para cuentas privilegiadas para interfaces de gestión. Para los usuarios de la Empresa, el Prestador deberá admitir una solución de autenticación que permita una autenticación sólida para usuarios / cuentas basada en las opciones de autenticación de la Empresa. Para el intercambio de Contenido entre la infraestructura de La Empresa y la infraestructura del Prestador, el Prestador deberá proporcionar una autenticación basada en certificados desde y hacia el entorno del Producto y / o Servicio. De lo contrario, ambas Partes acordarán cualquier otra forma de autenticación.

3.0 Arquitectura Compartida. El Prestador acepta identificar las partes en donde los recursos compartidos son utilizados dentro de su arquitectura por otros clientes y los controles de seguridad implementados para proteger los datos de la Empresa del acceso de usuarios no autorizados y de terceros. Si el Instrumento contempla un entorno dedicado, entonces dicho entorno no contendrá recursos compartidos, incluyendo, entre otros, todos los componentes, sistemas e infraestructura.

4.0 Respuesta a Incidentes y Notificación de Incumplimiento. El Prestador acuerda que cualquier incumplimiento, violación de datos o cualquier otro incidente de ciberseguridad, interno o externo, que pueda comprometer múltiples fuentes de datos o afectar los servicios de la Empresa, deberá notificar e informar oportunamente a [nombre del administrador del contrato por la Empresa] y soc.noc@ienova.com.mx al teléfono 800 626 6026 dentro de las 24 horas de conocimiento de la infracción, deberá cooperar plenamente para proporcionar toda la información relacionada, seguido de un plan de remediación, dentro de las 72 horas de remediación, y 2 semanas hábiles desde la notificación inicial para completar la investigación completa entregando un reporte ejecutivo y otro detallado del incidente, especificando la información que fue comprometida, estuvo expuesta o con riesgos asociados, así como un resumen del reporte forense. En caso de no cumplir con estos plazos la Empresa se reserva el derecho de suspender el servicio e iniciar la desconexión de la infraestructura del Prestador con la de La Empresa en caso de existir para mitigar cualquier compromiso y/o riesgo de Ciberseguridad que pueda ser trasladado a la Empresa.

5.0 Cifrado. Cuando el Instrumento estipule el cifrado, o si la Empresa determina que el cifrado es aceptable para evitar la divulgación no autorizada de información de la Empresa, a fin de proteger

la información confidencial de la Empresa, los productos del Prestador usarán controles criptográficos que satisfacen los requisitos de FIPS 197 de tal manera que datos e información confidencial se vuelven inaccesibles por un usuario no autorizado, considerando el uso de algoritmos de inscripción avanzada (AES). Cuando el producto del Prestador utilice claves de cifrado, el producto del Prestador no almacenará las claves de cifrado codificadas dentro del código fuente. Las claves de cifrado se almacenarán y protegerán por separado del producto mientras están en tránsito y en reposo, y serán revocables para su reimplementación y mantenimiento. El contenido se cifrará en tránsito, incluido, entre otros, el contenido transmitido por terreno público y en reposo. Los certificados criptográficos de la Empresa se utilizarán para las interfaces de usuario, cuando corresponda. Todos los certificados, claves y herramientas criptográficas solo se utilizarán para el propósito previsto y se protegerán contra el acceso, la modificación, la pérdida y la divulgación no autorizados. El Prestador utilizará un sistema seguro de gestión de claves (KMS) para almacenar y archivar las claves de forma segura.

6.0 Contraseña y Estándares de Inicio de Sesión. Los productos del Prestador proporcionarán una identificación única (identificable individualmente) para las cuentas de usuarios. Cuando no se pueda alcanzar la responsabilidad individual para el acceso a sistemas sensibles, se deberá de emplear la autenticación multifactorial. Los productos del Prestador proporcionarán una complejidad de contraseña que cumpla con los siguientes parámetros: las cuentas de los usuarios requerirán de un mínimo de 8 caracteres, una combinación de letras mayúsculas y minúsculas, números y caracteres especiales, las contraseñas tendrán no más de 90 días de antigüedad y se mantendrá el historial de 10 contraseñas anteriores. Las cuentas de los administradores requerirán un mínimo de 10 caracteres, una combinación de letras mayúsculas y minúsculas, números y caracteres especiales, tendrán no más de 90 días de antigüedad y se mantendrá el historial de 10 contraseñas anteriores. Las credenciales de inicio de sesión y las contraseñas estarán protegidas por un cifrado de transporte que cumpla con los requisitos mínimos de cifrado de la Sección 5.0.

7.0 Seguridad de Datos. El Prestador certifica que su producto proporciona la seguridad necesaria para cumplir con todas las leyes de protección de datos personales de la localidad, entorno de alojamiento e infraestructura donde se ubique el producto o servicio, así como los requisitos reglamentarios aplicables para el almacenamiento, procesamiento y transmisión de datos. Esto incluye específicamente, pero no se limita a, todas las leyes y reglamentos que requieren protecciones específicas para la información de identificación personal, tarjetas de crédito y la información financiera, y los registros de auditoría. El Prestador conviene en que permitirá la validación por parte de la Empresa o por terceros contratados por ella para verificar el cumplimiento de todos los requisitos legales y reglamentarios.

8.0 Registro y Detalles de Errores. El Prestador acepta registrar todo el uso de productos y aplicaciones, el acceso, el uso indebido y los suficientes mensajes de error detallados para monitorear y analizar el uso de los productos, y retendrá toda la información durante un mínimo de noventa (90) días a partir de la fecha de registro. El Prestador además acepta que el producto incluya una pista de auditoría, entradas de registro con sello de tiempo e identificación de registro única con atribución. La Empresa tiene el derecho de solicitar registros en cualquier momento y sin costo para la Empresa.

9.0 Soporte Operativo. El Prestador realizará verificaciones de datos de seguridad social, análisis de drogas e historial crediticio para el personal que respalda los productos alojados (si corresponde) antes de comenzar a trabajar con la Empresa y de manera continua, sin costo para la Empresa. La

Empresa se reserva el derecho de solicitar esta documentación para ratificar el cumplimiento de estas verificaciones por parte del Prestador.

10.0 Vulnerabilidades y Defectos. El Prestador acepta mantener un proceso de seguimiento de vulnerabilidades y defectos que identifique y remedie los posibles defectos, además de clasificarlos por su impacto en la seguridad de los productos del Prestador y los componentes y paquetes de *software* que lo respaldan, sin costo para la Empresa. Se debe notificar a la Empresa respecto a vulnerabilidades críticas o defectos especificando tiempos de remediación o mitigación de forma periódica acordada con el administrador de contrato de forma semestral. El Prestador conviene también en que, a expensas del Prestador, probará y remediará todas las vulnerabilidades de *software,* estas pueden ser identificados por ejercicios de escaneos de vulnerabilidades de El Prestador o estar divulgadas públicamente en la Base de datos de vulnerabilidad nacional (http://nvd.nist.gov/) y por Open Web Application Security Project (www.owasp.org) dentro de los treinta (30) días posteriores a su publicación. En general, esto evitará que el producto sea fácilmente susceptible a secuencias de comandos entre sitios, inyección, SQL, desbordamientos de búfer, validación de entrada y otros ciberataques similares. El Prestador garantiza además que el producto no contendrá ningún código que pueda facilitar el acceso inesperado o no aprobado o interrupciones del producto, incluidos, entre otros: virus informáticos, gusanos, bombas de tiempo, puertas traseras, caballos de Troya, huevos de pascua y cualesquiera otras formas de código malicioso, y acepta proporcionar documentación que detalle dichos procesos a solicitud de la Empresa y sin costo para la Empresa. La Empresa se reserva el derecho de solicitar esta documentación para ratificar el cumplimiento de estas verificaciones por parte del Prestador.

11.0 Evaluaciones y Pruebas de Seguridad. El Prestador acuerda que contratará a un tercero independiente, que será acordado por el Prestador y la Empresa, a expensas del Prestador, para probar el producto en busca de vulnerabilidades y riesgos de ciberseguridad a través de una prueba de seguridad detallada anualmente, o el Prestador podrá optar por certificarse bajo un estándar industrial aceptado. Estándar, que será aprobado por la Empresa. Si el Prestador elige una prueba de seguridad anual, dicha prueba incluirá todos los controles de seguridad que respaldan el producto, su entorno de alojamiento de producción y la infraestructura de soporte operativo. El Prestador requerirá que dicho tercero proporcione un informe que detalle los resultados de la prueba y el Prestador deberá proporcionar a la Empresa una copia de dicho informe dentro de los treinta (30) días posteriores a la prueba. En el caso de que dicho informe muestre vulnerabilidades en el producto, el Prestador deberá proporcionar de inmediato a la Empresa un plan de remediación propuesto y un cronograma para su finalización, todo sin costo para la Empresa. Todas las vulnerabilidades, defectos o errores del producto revelados al Prestador serán corregidos y remediados por el Prestador, a expensas del Prestador, dentro de los treinta (30) días a partir de la fecha de dicho informe. La Empresa se reserva el derecho de solicitar esta documentación para ratificar el cumplimiento de estas verificaciones por parte del Prestador, esta documentación incluye evidencia de las pruebas, certificaciones de cumplimiento vigentes, entre otros.

12.0 El Prestador debe mantener en todo momento apego a las políticas de Ciberseguridad de la Empresa y sus subsidiarias, y seguir los lineamientos establecidos.

13.0 Estándares y certificaciones de la industria. El Prestador proporcionará su Producto y / o Servicio de acuerdo con las Buenas Prácticas de Seguridad y, en particular, deberá cumplir y/o estar certificado en el alcance del Producto y / o Servicio proporcionado de acuerdo con los siguientes estándares, políticas y estándares técnicos de la industria en su versión más reciente: *ISO / IEC*

27001 o equivalente. Previa solicitud, el Prestador deberá enviar su certificado y/o dictámenes, incluidas las declaraciones de aplicabilidad a IEnova, así como todas las certificaciones del Prestador aplicables y disponibles adicionales u otra evidencia de las capacidades solicitadas en el contexto de la Ciberseguridad (por ejemplo, ISO / IEC 27018, BSI C5, Cloud Security Alliance, IEC 62443-4-1, PCI-DSS, HIPAA). Para evitar que las certificaciones de ciberseguridad relevantes del Prestador caduquen durante la vigencia del Acuerdo, el Prestador acuerda volver a certificarse continuamente para cualquier sistema relevante utilizado en la provisión del Producto y / o Servicio antes de la expiración de cualquier certificación existente. El Prestador deberá informar a la Empresa inmediatamente si alguno de los certificados relevantes pierde su validez. El Prestador también deberá cumplir con todas las leyes y regulaciones aplicables relacionadas con el Producto y / o Servicio.

14.0 Derecho a Informar. La Empresa y el Prestador tienen el derecho de informar a las organizaciones de informes de vulnerabilidad pública en Territorio Nacional sobre cualquier defecto o condición de configuración que resulte en vulnerabilidades a la información manejada por la entrega, la entrega misma u otro hardware, software o sistemas que pondrían en riesgo a la Empresa y/o a los intereses de la Empresa.

15.0 Destrucción de información y datos. El Prestador acuerda que de acuerdo con el cronograma de registros de la Empresa o en acuerdo con el administrador del contrato se establecerá el período de retención de datos aplicable en el Instrumento, sobre los datos que ya no son necesarios o, a solicitud de la Empresa, el Prestador destruirá los datos de una manera que los hará completamente inutilizables e irrecuperables, y proporcionarán a la Empresa un certificado de destrucción, a solicitud de la Empresa. El Prestador deberá devolver o destruir los datos tras la rescisión o vencimiento del contrato revoque todo el acceso a información y datos propiedad de IEnova. El Prestador deberá certificar que los datos que posee propiedad de IEnova han sido eliminados o destruidos.

16.0 Documentación Formal. El Prestador acepta proporcionar documentación formal al usuario de la Empresa de los servicios contratados para el uso, mantenimiento e implementación segura del producto del Prestador. La documentación del producto se actualizará dentro de los treinta (30) días posteriores a la actualización, parche o cambio similar del producto. La documentación del producto incluirá, entre otras cosas, un inventario de todos los componentes, una lista de todas las cuentas del sistema (es decir, genéricas y / o predeterminadas), configuraciones, controles de ciberseguridad y dependencias. El Prestador deberá divulgar por escrito todos los métodos conocidos para administrar el producto, incluidos, entre otros, las cuentas de usuarios no documentados y todos los comandos, configuraciones y operaciones utilizados para administrar el producto.

17.0 Conexión de red. En caso de que se requiera una conexión entre la Empresa y la red del El Prestador, el Prestador deberá proporcionar una solución de red privada virtual o se utilizará la solución de Acceso para Socios Comerciales, es decir, otros proveedores de servicio) de la Empresa.

18.0 Informes de aseguramiento. A solicitud de la Empresa, pero no más de una vez al año, el Prestador deberá proporcionar el informe de auditoría, atestiguamientos SSAE-16 SOC2 Tipo II actual (e IEC 62443 si corresponde) y otras pruebas / evidencias similares (por ejemplo, informes de auditoría externa) de un Marco de ciberseguridad. El Prestador deberá gestionar las deficiencias identificadas en las evaluaciones / auditorías de acuerdo con los métodos y medidas para las auditorías definidas en el Acuerdo. Si la corrección de los hallazgos de la auditoría no se ha definido en el Acuerdo, el

Prestador deberá remediar las deficiencias informadas en función de su gravedad declarada en los informes de auditoría (excepto cuando el Prestador y la Empresa hayan acordado una priorización de corrección diferente), en un tiempo razonable y sin costo para la Empresa. Después de proporcionar los hallazgos de la auditoría, el Prestador deberá proporcionar un plan de trabajo oportuna que describa el programa de remediación y actualizaciones de estado periódicas sobre el progreso del plan de trabajo y una declaración de cumplimiento después de la finalización del plan de trabajo.

19.0 Registro y monitoreo. El Prestador deberá registrar y monitorear los eventos relevantes para la seguridad, incluidos, entre otros, interfaces, cambios en la autorización, autenticación de cuentas de cualquier tipo y cambios en el servicio de registro en sí, preferiblemente con el respaldo de soluciones de seguridad de última generación. El seguimiento se realizará independientemente de la prestación del Servicio, es decir, sin acceso al Contenido. El Prestador intervendrá inmediatamente en caso de comportamiento sospechoso y realizará investigaciones forenses posteriores. El Prestador almacenará dichos registros para eventos relacionados con la seguridad de forma centralizada, fuera del entorno del Producto y / o Servicio, con un tiempo de retención de al menos 90 días. Se aplicarán los derechos de auditoría contractuales de la Empresa.

20.0 Prohibición de poner en peligro las funcionalidades. El Prestador no incluirá ninguna funcionalidad (por ejemplo, "puerta trasera") en su hardware y software aplicable al Producto y / o Servicio entregado a la Empresa que ponga en peligro la integridad, confidencialidad y disponibilidad del hardware, software, contenido que sean contrarios a los intereses de la Empresa en lo que respecta a la confidencialidad y el cumplimiento de la seguridad. Dicha funcionalidad que pone en peligro incluye (i) la descarga no deseada de Contenido, (ii) la manipulación o cambios no deseados del Contenido o la lógica del proceso, (iii) la alimentación no deseada de Contenido o (iv) la mejora no deseada de la funcionalidad.

21.0 Obligación de notificación. El Prestador solo tendrá derecho a cambiar o adaptar el Producto y / o Servicio siempre que se proporcione al menos el mismo nivel de Buenas Prácticas de Seguridad que se solicite y acuerde entre las Partes. El Prestador deberá informar a la Empresa antes de cualquier cambio relevante relacionado con el Producto y / o Servicio que pueda afectar negativamente el cumplimiento del Prestador con los Requisitos de Ciberseguridad como se establece en este documento. En tal caso, se aplicarán los derechos de la Empresa establecidos en el Instrumento. El Prestador deberá contar con un proceso efectivo, documentado y revisado periódicamente para informar a la Empresa de inmediato en caso de cualquier circunstancia (p. Ej., Desastre) que afecte materialmente al Producto y / o Servicio, incluidos los modos de comunicación y las interfaces.

22.0 Evaluación de requisitos de ciberseguridad. Para el Servicio que se proporciona en virtud del Instrumento, si la Empresa lo solicita, el Prestador entregará una Evaluación de Requisitos de Ciberseguridad que describa las medidas tomadas para cumplir con los requisitos de ciberseguridad solicitados por la Empresa, que se basa en los requisitos del Instrumento y que reflejará los niveles de seguridad de la oferta correspondiente o posteriores solicitudes de cambio. El Prestador entregará dicha evaluación preferiblemente como parte de cualquier oferta de Producto y / o Servicio, pero a más tardar [30] días después de la firma del Instrumento y antes de que el Producto y / o Servicio esté listo y antes de cualquier cambio de Producto y / o Servicio si no se acuerda lo contrario con la Empresa. Dicha evaluación deberá ser implementada y cumplida por el Prestador antes de que el Servicio esté listo, si no se acuerda mutuamente lo contrario, y estará sujeta a la aprobación previa de la Empresa. Sobre la base de la evaluación de la evaluación, ambas Partes definirán mutuamente

medidas adicionales como se indica en el capítulo “Medidas adicionales de ciberseguridad”, documentadas en un plan de hitos y que el Prestador implementará sin costo para la Empresa. La Empresa entiende que el nivel de protección proporcionado como se describe en la Evaluación de Requisitos de Ciberseguridad por parte del Prestador está sujeto al progreso y desarrollo técnico. En ese sentido, el Prestador tendrá derecho a implementar protecciones alternativas adecuadas que estén de acuerdo, pero continuará brindando al menos el mismo nivel de seguridad que se solicita en la evaluación respectiva. Otros cambios a la Evaluación de requisitos de seguridad cibernética estarán sujetos a la aprobación previa de la Empresa. El Prestador informará a la Empresa sobre las actualizaciones de la Evaluación de Requisitos de Ciberseguridad a su debido tiempo y proporcionará información y explicaciones adicionales (ya sea por escrito o en un taller acordado entre ambas Partes) con respecto a dichos Requisitos de Ciberseguridad si la Empresa lo solicita. Los cambios periódicos dentro de los Requisitos de Ciberseguridad solicitados por la Empresa serán revisados e implementados por el Prestador en la Evaluación de Requisitos de Ciberseguridad en la medida que sea relevante para el Producto y / o Servicio a su debido tiempo después de la publicación de los Requisitos de Ciberseguridad actualizados. Dichos cambios en la Evaluación de requisitos de seguridad cibernética estarán sujetos a la aprobación de la Empresa.

23.0 Copia de seguridad y recuperación de datos. El Prestador deberá utilizar soluciones de respaldo y recuperación adecuadas y otras medidas para cumplir con el Objetivo de tiempo de recuperación (RTO – Recovery Time Objective) de [veinticuatro (24) horas] y el Objetivo de Punto de Recuperación (RPO – Recovery Time Objective) de [ocho (8) / horas] en caso de desastre y (si corresponde) con los niveles de servicio de emergencia según definidos en el Instrumento o en los Anexos relacionados. Las copias de seguridad se almacenarán de forma segura fuera del entorno del Producto y / o Servicio. El Prestador creará, implementará y mantendrá actualizado un (i) respaldo y recuperación de datos y un (ii) plan de recuperación de desastres de Tecnologías de Información de acuerdo con los requisitos comerciales identificados que periódicamente, al menos una vez al año o después de cambios importantes, serán ejecutado. Se proporcionará evidencia de dicha prueba a la Empresa cuando la solicite. Para evitar dudas y si es necesario, se definirá y acordará un concepto de archivo por separado.

24.0 Disponibilidad del servicio. El Prestador deberá monitorear continuamente la disponibilidad del Servicio. Si se producen dos interrupciones en un período de dos horas, todo el período desde el comienzo de la primera interrupción hasta el final de la segunda interrupción se considerará tiempo de inactividad. El Prestador garantiza una disponibilidad mínima del servicio del [99.999]%.

25.0 Sanciones y penalizaciones. La Empresa se reserva la decisión de desvincular infraestructura, servicios, recursos humanos involucrados de las actividades y proyectos vigentes y futuros. La Empresa se reserva la decisión de penalizar, a través de limitar el pago de un mes de costo del servicio o lo proporcional según corresponda durante el primer incidente, en el caso de una segunda reincidencia, la Empresa podrá rescindir el Instrumento.

26.0 Conflictos. Nada de lo contenido en este documento se interpretará que limita en forma alguna las obligaciones del Prestador contenidas en otras partes del Instrumento, incluidos, entre otros, los términos y condiciones contenidos en el cuerpo principal del mismo. En caso de conflicto entre el Instrumento y este documento, únicamente en relación con todo lo relacionado con la Ciberseguridad, este documento prevalecerá.

Apartado 1 – Requisitos de ciberseguridad para Prestadores de servicio en la nube

En adición y complemente a los requisitos de ciberseguridad expuestos previamente, el Prestador deberá cumplir los siguientes lineamientos si ofrece servicios o productos en la nube.

1. El Prestador proporcionará anualmente sin costo adicional a la Empresa una copia de un informe SOC 1 y SOC 2 - Tipo II de la SSAE SSAE 1 y SOC 2 Statement on Standards for Attestation Engagements 16 (SASE 16) (y cuando corresponda cualquier categoría sucesora de informes de auditoría, colectivamente "**Informe SOC**") que cubra los controles internos sobre los informes financieros asociados con los servicios prestados y las instalaciones de alojamiento. El Informe SOC incluirá, sin limitación, controles para la gestión de datos basados en cinco "principios de servicio de confianza": seguridad, disponibilidad, integridad del procesamiento, confidencialidad y privacidad. El Informe SOC cubrirá un período de 12 meses según lo definido por la Empresa y será realizado anualmente por el proveedor de servicios elegido por el Prestador. El Prestador proporcionará los últimos informes disponibles, o informe que cubre un período solicitado, a la Empresa dentro de los 30 días posteriores a la solicitud. Si algún Informe SOC está sujeto a calificación o revela deficiencias materiales en los controles y procedimientos internos relacionados con las operaciones, servicios y productos, el Prestador desarrollará y presentará a la Empresa un plan para curar y corregir dichas deficiencias (el "**Plan de Remediación**") dentro de los 10 días hábiles posteriores a la finalización del Informe SOC e iniciar la implementación del Plan de Remediación con prontitud después de la aprobación del Plan de Remediación por parte de la Empresa, o dentro de otro plazo acordado por las Partes.

2. Si los productos o servicios entregados por el Prestador contienen software, firmware o chipsets:
   a. El Prestador implementará las normas, procesos y métodos adecuados para prevenir, identificar, evaluar y reparar cualquier vulnerabilidad, código malicioso e incidentes de seguridad en productos y servicios que sean consistentes con las buenas prácticas y estándares de la industria de ciberseguridad;
   b. El Prestador continuará apoyando y proporcionando servicios para reparar, actualizar y mantener productos y servicios, incluida la provisión de parches a la Empresa para remediar vulnerabilidades durante la vida útil razonable de los productos y servicios;
   c. El Prestador proporcionará a la Empresa una lista de materiales que identifique todos los componentes de software de terceros contenidos en los productos. El software de terceros estará actualizado en el momento de la entrega a la Empresa;
   d. El Prestador otorgará a la Empresa el derecho, sin embargo, La Empresa no estará obligado, a probar o haber probado productos en busca de código malicioso y vulnerabilidades en cualquier momento, y apoyará adecuadamente a La Empresa en estos ejercicios;
   e. El Prestador proporcionará a la Empresa un contacto para todos los problemas relacionados con la seguridad de la información (disponible durante el horario comercial).

3. El Prestador informará inmediatamente a la Empresa de todos los incidentes de seguridad de la información relevantes ocurridos o sospechosos y vulnerabilidades descubiertas en cualquier operación, servicio y producto proporcionados por el Prestador, en la medida en que la Empresa se vea afectado materialmente o exista la probabilidad de que se vea afectado materialmente.

4. El Prestador adoptará las medidas apropiadas para lograr que sus proveedores estén obligados, en un plazo razonable, a obligaciones similares a las disposiciones de esta sección.

5. Si el Prestador desarrolla el producto/software exclusivamente para la Empresa, el Prestador proporcionará a la Empresa toda la documentación relacionada y el código fuente y legible y el código objeto de software desarrollado o convertido para la Empresa.

6. La Empresa tiene derecho a auditar anualmente al Prestador sin causa y, además, si la Empresa tiene una sospecha justificada de que el Prestador no cumple plenamente con dichas disposiciones, en cada caso previa notificación razonable. La auditoría contempla los servicios contratados bajo el Instrumento. En caso de incumplimientos será necesario que El Prestador presente al administrador del contrato un plan de mitigación con plazos establecidos. La Empresa se reserva el derecho de rescindir el Instrumento por incumplimientos.

EN TESTIMONIO DE LO ANTERIOR, el Prestador firma de conformidad el día [_____] de [_____] de [_____].

[•]

_____

[•]

Representante Legal