CONTRATO NÚMERO GE GUION AL GUION CINCUENTA Y DOS GUION DOS MIL VEINTICINCO (GE-AL-52-2025). En la ciudad de Guatemala, el siete de agosto de dos mil veinticinco. NOSOTROS: Por una parte, **ARNALDO ADEMAR ALVARADO CIFUENTES,** de cincuenta y tres años de edad, casado, guatemalteco, Ingeniero, de este domicilio, con Documento Personal de Identificación (DPI), Código Único de Identificación (CUI) dos mil quinientos noventa y ocho espacio sesenta y seis mil cuatrocientos treinta y uno espacio mil seiscientos uno (2598 66431 1601), extendido por el Registro Nacional de las Personas de la República de Guatemala; actúo en mi calidad de Sub Gerente del Instituto Técnico de Capacitación y Productividad "INTECAP", con cuentadancia número dos mil veintidós guion cien guion ciento uno guion diecinueve guion cero veintinueve (2022-100-101-19-029); acredito mi personería con: a) Certificación del punto Quinto del acta número treinta y seis guion dos mil dieciséis (36-2016), de la Honorable Junta Directiva del "INTECAP"; y b) Certificación del Acta de toma de posesión del cargo número ochenta y cuatro guion dos mil dieciséis (84-2016), de fecha veintiocho de octubre de dos mil dieciséis, extendida por la División de Recursos Humanos del "INTECAP", en lo sucesivo denominado "INTECAP"; y por la otra parte, **ESTUARDO JOAQUÍN OLIVARES RUIZ,** de cincuenta y nueve (59) años de edad, casado, Ingeniero en Sistemas, guatemalteco, de este domicilio, con Documento Personal de Identificación (DPI), Código Único de Identificación (CUI) dos mil ciento setenta y seis espacio cuarenta mil sesenta espacio cero ciento uno (2176 40060 0101), extendido por el Registro Nacional de las Personas de la República de Guatemala; actúo en mi calidad de Administrador Único y Representante Legal de la entidad "Red Óptima, Sociedad Anónima", inscrita en el Registro Mercantil General de la República de Guatemala, al número ciento

diecisiete mil trecientos treinta (117330) folio veintinueve (29) libro doscientos once (211) de Sociedades; propietaria de la empresa de nombre comercial "Red Optima", inscrita en el Registro Mercantil General de la República de Guatemala, al número seiscientos setenta y cinco mil cuatrocientos sesenta y cuatro (675464) folio seiscientos cuarenta y uno (641) del libro seiscientos treinta y siete (637) de Empresas Mercantiles, calidad que acredito con el acta notarial de fecha dos de junio de dos mil veintitrés, autorizada en esta ciudad por el Notario Jorge Luis Molina Del Cid, debidamente inscrita en el Registro Mercantil General de la República de Guatemala, bajo el número setecientos un mil quinientos doce (701512), folio treinta y uno (31), libro ochocientos dieciocho (818) de Auxiliares de Comercio; señalo como lugar para recibir notificaciones en la sexta (6ta) avenida uno guion treinta y seis (1-36) zona catorce (14), Plaza Los Arcos, Oficina cuatro A (4 A) de esta ciudad, en lo sucesivo seré denominado "Red Optima". Ambos comparecientes manifestamos hallarnos en el libre ejercicio de nuestros derechos civiles y que la representación que se ejercita es suficiente conforme a la Ley para la celebración del presente **CONTRATO DE COMPRAVENTA** contenido en las cláusulas siguientes:

PRIMERA: BASE LEGAL: El presente contrato se suscribe con fundamento en lo que prescribe la Ley de Contrataciones del Estado, Decreto cincuenta y siete guion noventa y dos (57-92) del Congreso de la República de Guatemala y su Reglamento contenido en el Acuerdo Gubernativo ciento veintidós guion dos mil dieciséis (122-2016); Bases de Cotización número veinticuatro guion dos mil veinticinco (24-2025), cuyo objeto es la contratación del servicio de herramienta de gestión avanzada de amenazas con políticas de respuesta automatizadas en infraestructuras críticas con uso y gestión de metadata para la seguridad cibernética institucional; bajo el número

de operación Guatecompras veintiséis millones seiscientos ochenta y nueve mil trescientos cincuenta y nueve (NOG 26689359); Acta número SC guion cero setenta nueve guion dos mil veinticinco (SC-079-2025), de fecha dos de julio de dos mil veinticinco, de recepción y apertura de plicas; Acta número SC guion cero ochenta y nueve guion dos mil veinticinco (SC-089-2025), de fecha ocho de julio de dos mil veinticinco, de calificación y adjudicación de oferta; cotización contenida en formulario electrónico COT guion dos mil veinticinco guion veintiséis millones seiscientos ochenta y nueve mil trescientos cincuenta y nueve guion ochenta y ocho millones ciento noventa y seis mil seiscientos sesenta y seis (COT-2025-26689359-881966666), código de autenticidad cuatro millones novecientos cuarenta y cuatro mil setecientos ochenta y ocho C (4944788C), de fecha uno de julio de dos mil veinticinco; oferta de "Red Optima", de fecha uno de julio de dos mil veinticinco; Acuerdo de aprobación de la adjudicación número GE guion cuatrocientos cincuenta y ocho guion dos mil veinticinco (GE-458-2025), de fecha diecisiete de julio de dos mil veinticinco; y Memorando número SS guion noventa y nueve guion dos mil veinticinco (SS-99-2025), de fecha dieciocho de julio de dos mil veinticinco. Se tiene por incorporada al presente contrato la documentación anteriormente citada.

SEGUNDA: OBJETO DEL CONTRATO: Contratación del servicio de herramienta de gestión avanzada de amenazas con políticas de respuesta automatizadas en infraestructuras críticas con uso y gestión de metadata para la seguridad cibernética institucional; para el efecto "Red Optima" vende al "INTECAP" lo siguiente: **Plataforma Lumu Defender,** para la protección de dos mil (2000) dispositivos por un plazo de doce (12) meses, con las siguientes características específicas: La plataforma se basa en un sistema de seguridad que recibe todo le tráfico de la red

como mínimo, desde dispositivos Firewall, switches y servidores DNS en sistemas operativos Windows y Linux; analiza e identifica las amenazas o incidentes que ocurren en la red, incluye almacenamiento de datos por un mínimo de veinticuatro (24) meses sin costo adicional; opera como un servicio gestionado en la nube que permite la evaluación y administración continua del estado de seguridad de los activos informáticos. La solución incluye monitoreo en tiempo real de la interacción de los activos con entornos potencialmente riesgosos, mediante el uso de gestión avanzada de metadata y automatización de políticas de seguridad cibernética, lo que habilita una respuesta dinámica frente a incidentes; cuenta con la certificación SOC dos (SOC2) Tipo II, lo que confirma que el servicio implementa y mantiene controles adecuados conforme a las mejores prácticas en términos de privacidad, seguridad y confidencialidad de la información; ofrece una capacidad de integración fluida y flexible con diversos sistemas existentes en la organización, incluidos firewalls, switches y servidores DNS de múltiples fabricantes. La solución permite recolectar y procesar metadata de manera efectiva, asegurando compatibilidad universal e integración sin barreras para una gestión de seguridad centralizada y cohesionada; recolecta y analiza datos críticos para la seguridad de forma independiente a cualquier solución de seguridad preexistente. Su integración es agnóstica respecto a plataformas de firewall, switches y DNS, lo que permite una recopilación de datos homogénea y exhaustiva, sin estar limitada por la diversidad de proveedores presentes en la infraestructura; cuenta con funcionalidades avanzadas para recolectar, procesar y analizar consultas DNS dentro del ecosistema institucional, esta capacidad permite identificar y mapear la comunicación entre los activos de la red y posibles infraestructuras de amenazas externas, siendo fundamental para detectar intentos de conexión con entidades

hostiles y tomar medidas proactivas para interrumpir y prevenir ataques cibernéticos; está diseñada para realizar la recolección de datos sin depender de hardware adicional ni requerir el uso de puertos espejo en la infraestructura de red existente. Esta capacidad permite una implementación eficiente, ágil y compatible con la arquitectura actual, evitando interrupciones operativas y costos asociados a equipos especializados; cuenta con la capacidad de acceder y extraer datos de los buzones de spam de Office trescientos sesenta y cinco (365), permite el análisis detallado de intentos de ataque, esta funcionalidad incluye la identificación de las fuentes y metodologías utilizadas, lo que contribuye a una estrategia de defensa mas informada, proactiva y alineada con la inteligencia de amenazas; es una solución robusta y flexible con capacidad de integrarse con dispositivos remotos que operan bajo sistemas operativos Windows, MacOs, y otros, permite recolectar, procesar y analizar metadata de red generados por estas plataformas, proporciona una visión comprensiva y unificada del panorama de seguridad en entornos operativos heterogéneos; posee capacidades integrales para la recopilación, procesamiento y análisis de metada de red en dispositivos que operan bajo el sistema operativo Linux, garantiza visibilidad completa sobre la actividad de red generada por estos sistemas; recopila, procesa y analizar metadata de red proveniente del protocolo DNS en servidores Windows, incluyendo compatibilidad con Windows Server dos mil doce (2012) como mínimo. Esto garantiza su operatividad con infraestructuras existentes que aún utilizan versiones anteriores del sistema operativo; Basa su proceso de recolección de datos para la medición de compromiso exclusivamente en metadata, sin depender de la captura o análisis de paquetes de datos. Esta aproximación permite una implementación no intrusiva, eficiente y enfocada en la visibilidad estratégica de amenazas; ofrece una API

abierta para la ingestión de metadatos, permitiendo a la organización integrar esta funcionalidad de manera flexible y adaptarla a sus objetivos específicos y necesidades particulares dentro de su entorno de seguridad; al ejecutar un proceso de evaluación continua del compromiso (CEC) utiliza técnicas avanzadas de análisis y correlación de metadata para medir con precisión la exposición y actividad maliciosa en la red. Este sistema detecta indicadores de compromiso en tiempo real, ofreciendo monitoreo constante y un diagnóstico profundo de la postura de seguridad cibernética de la organización; dispone de capacidades de análisis en tiempo real para evaluar y monitorear el estado de compromiso de los activos informáticos. La solución incorpora técnicas avanzadas de procesamiento de eventos en tiempo real, detección de anomalías y algoritmos inteligentes de análisis de comportamiento, permitiendo identificar desviaciones de patrones normales que indican vulneraciones de seguridad; incorpora un sistema sofisticado de clasificación de amenazas que, tras la detección de compromisos, categoriza automáticamente el tipo de amenaza, la solución identifica malware, comandos y controles (C&C) phishing y otros vectores de ataque emergentes, utilizando tecnologías basadas en inteligencia artificial y aprendizaje automático para mantener actualizado el espectro de amenazas reconocidas; cuenta con una infraestructura de almacenamiento de datos que permite la retención de registros históricos por un período mínimo de dos (2) años, sin requerir recursos de aprovisionamiento externos ni ampliaciones de capacidad posteriores a la implementación inicial; cuenta con funcionalidades avanzadas de análisis retrospectivo, que permiten inspeccionar y correlacionar datos históricos frente a nuevos vectores de ataque. La solución incluye la capacidad de aplicar de forma retroactiva Indicadores de Compromiso (IoCs) recientemente identificados sobres

los registros almacenados, lo que permite evaluar la exposición previa a amenazas emergentes y comprender la cronología y propagación potencial de infecciones dentro de la red institucional; está fundamentada en un marco sofisticado de análisis de metadatos que incluye un sistema de correlación que interactúa con mas de ochenta (80) fuentes de ciber inteligencia, garantizando una amplia cobertura en la identificación de amenazas, el uso de modelos de aprendizaje automático supervisados y algoritmos de inteligencia artificial para la detección y validación precisa de patrones de actividad maliciosa, la aplicación de técnicas de machine learning no supervisadas, que permiten descubrir nuevas amenazas y comportamientos anómalos sin requerir etiquetado previo de datos; está diseñada con una arquitectura abierta y modular que permite la integración de fuentes adicionales de ciberinteligencia, alineándose con la estrategia de "Bring your own threat intelligence" (BYOT). Esta capacidad habilita la incorporación y procesamiento dinámico de inteligencia sobre amenazas generada internamente o adquirida de terceros, enriqueciendo la base de datos de amenazas y mejorando la precisión del sistema de detección; identifica y cataloga indicadores de compromiso (IoCs) y hashes de archivos maliciosos asociados con cada incidente de seguridad detectado. Asimismo, proporciona una interfaz directa y segura desde la cual los usuarios pueden acceder y descargar estos IoCs y hashes, facilitando investigaciones detalladas y permitiendo una respuesta rápida y eficaz ante incidentes; incluye capacidades avanzadas de enriquecimiento contextual para cada incidente de compromiso detectado. La solución integra referencias internas y externas que facilitan la comprensión completa de la naturaleza y el alcance del compromiso, lo cual es esencial para una evaluación precisa de la amenaza para apoyar decisiones informadas durante la respuesta a incidentes; ofrece una

plataforma flexible que permite la clasificación y agrupación de los activos de información según criterios definidos por el usuario. La solución soporta la creación de segmentos personalizados de activos, facilitando una gestión diferenciada y específica basada en necesidades de seguridad, tipo de datos manejados u otros parámetros relevantes para la organización; permite la asignación dinámica de niveles de relevancia a los activos de información de la institución. Esta funcionalidad es altamente configurable, lo que permite a los administradores de seguridad establecer ya justar la importancia de los activos según su criticidad, exposición al riesgo o valor estratégico, facilitando así la priorización efectiva de acciones de protección y respuesta; proporciona la frecuencia de compromiso, por día de la semana y hora del día. Además, muestra la distribución de los ataques según los grupos previamente configurados (como usuario remoto, oficina central o IoT) e incluye características relacionadas con cada compromiso y los playbooks correspondientes para cada tipo de ataque detectado. Asimismo, ofrece una interfaz para la gestión de incidentes, abiertos, cerrados y silenciados, que permite registrar y dar seguimiento a las acciones tomadas en respuesta a cada incidente; proporción información detallada sobre la bandeja de spam analizada, incluyendo como mínimo el volumen de correos inspeccionados, los destinatarios que reciben más spam y correos maliciosos, las tendencias de ataque, los días y horas de mayor recepción de correos maliciosos y la correlación entre los mensajes recibidos y los contactos reales realizados con infraestructura comprometida; permite la creación de nuevos usuarios con roles específicos dentro de la institución, incluyendo los roles de Administrador y solo Lectura. Esto facilita una gestión adecuada de accesos y privilegios conforme a las políticas internas de seguridad; permite la supervisión de los colectores desplegados en la red. La plataforma proporciona visibilidad del

estado de los colectores, del servicio de la aplicación, del uso de recursos del colector y ofrece gráficas que muestran, en el tiempo, la cantidad de información recolectada por cada colector de metadatos; cuenta con un portal web que proporciona estadísticas detalladas sobre los indicadores de compromiso (IoCs) facilitando la visualización, análisis y gestión de la actividad maliciosa detectada en la red; incluye un portal web compatible y completamente funcional en los navegadores más utilizados incluyendo Google Chrome, Mozilla Firefox, Internet Explorer y Safari. Esta compatibilidad garantiza accesibilidad universal, facilitando la gestión y el monitoreo de la seguridad desde distintos dispositivos y ubicaciones, optimizando la experiencia del administrador en diversos entornos operativos; permite filtrar la información por rangos de tiempo predefinidos (como hoy, ayer, últimos siete días) o por períodos personalizados. Además, permite filtrar datos relacionados con incidentes basados en criterios como tipo de incidente, numero de endpoints, numero de contactos y fecha de creación. Asimismo, la solución permite agrupar los activos de información según las necesidades de la institución sin restricciones, facilitando una gestión personalizada y eficiente; muestra el tiempo promedio de respuesta de la institución ante un incidente, así como la cantidad promedio de incidentes registrados diariamente. Esta información permite evaluar la eficiencia operativa y fortalecer los procesos de respuesta ante eventos de seguridad; provee información que evidencia la eficiencia operativa alcanzada por la institución en el procesamiento de indicadores de Compromiso (IoCs), incluyendo métricas de ahorro operacional expresadas en horas de trabajo de los analistas de seguridad. Esto permite cuantificar el impacto positivo de la automatización y priorización inteligente en los procesos de detección y respuesta; Analiza cada incidente utilizando una matriz de conocimiento basada en tácticas y técnicas

adversarias observadas en el mundo real, alineadas con el marco MITRE ATT&CK. Esta capacidad permite contextualizar las amenazas detectadas y facilita una respuesta más precisas y orientada a las metodologías utilizadas por los atacantes; incluye un análisis global de las tácticas y técnicas maliciosas utilizadas por los atacantes en la institución, basado en la matriz MITRE ATT&CK y sustentado en las incidencias reportadas por la plataforma, esta funcionalidad proporciona una mapa de calor que permite visualizar como los atacantes intentan acceder a la red, brindando la visibilidad necesaria para ajustar el stack de ciberseguridad y mejorar la eficiencia y eficacia de las defensas; es capaz de responder automáticamente a compromisos detectados mediante su conexión a la infraestructura de defensa a través de API. Esta capacidad permite ajustar dinámicamente las políticas de bloqueo pertinentes, fortaleciendo la respuesta automatizada frente a amenazas; incorpora integración nativa para funciones de bloqueo automático con proveedores reconocidos por e lsector como Palo Alto Networks, Fortinet, Check Point, Cisco, entre otros. Esta capacidad permite una respuesta inmediata y eficaz ante compromisos integrándose directamente con las plataformas de defensa ya existentes en la infraestructura de la organización; muestra que elementos de STack de seguridad, a través de procesos de integración, recibieron la información de los indicadores de Compromiso (loCs) vinculados con un incidente y respondieron automáticamente para mitigar la amenaza, basándose en la información entregada por la solución. Esto proporciona visibilidad sobre la efectividad de la automatización y la coordinación entre herramientas de seguridad; muestra en tiempo real la cantidad de indicadores de compromiso (loCs) activos, clasificados como mínimo en dominios, URLs, hashes y direcciones IP. Esta funcionalidad proporciona visibilidad inmediata sobre las amenazas vigentes en el entorno institucional;

permite la implantación mediante la instalación de un colector pasivo dentro de la institución, sin requerir hardware específico, además, es compatible como mínimo con plataformas de virtualización como VirtualBox, Hyper-V, Oracle y VMware, lo que facilita una implementación flexible y adaptable a la infraestructura existente; permite la mitigación automática de amenazas sin requerir la instalación de un componente en los endpoints de la institución, esto se logra mediante integraciones con la infraestructura de red y seguridad existente, lo que permite una respuesta eficaz sin intervención directa en los dispositivos finales; puede ingerir metadatos para la medición remota del compromiso del dispositivo. Esta funcionalidad permite evaluar el nivel de compromiso de equipos remotos, garantizando visibilidad y control sin necesidad de intervención directa o local; realiza la mitigación utilizando los componentes de seguridad ya existentes en la institución. La solución se integra con la infraestructura vigente para orquestar respuestas automáticas, optimizando recursos y evitando la necesidad de implementar nuevas herramientas; figura en el informe "Network Analysis and Visibility" de Forrester en la categoría de líderes o posición equivalente, lo que respalda su reconocimiento en la industria como una solución destacada en análisis y visibilidad de red; por un precio total de setecientos cincuenta y ocho mil setecientos sesenta quetzales (Q758,760.00). La contratación de la plataforma, garantía y el soporte técnico, además de las especificaciones descritas, deben cumplir con las indicadas en la oferta de "Red Óptima".

TERCERA: VALOR DEL CONTRATO Y FORMA DE PAGO: El monto a que asciende la contratación de la plataforma, la garantía y el soporte técnico, del presente contrato es de **SETECIENTOS CINCUENTA Y OCHO MIL SETECIENTOS SESENTA QUETZALES (Q758,760.00);** valor que incluye el Impuesto al Valor Agregado (IVA); para los efectos de pago, "Red Optima" debe

presentar la factura electrónica en línea-FEL-, emitida por el proveedor a través de su agencia virtual del Portal de la Superintendencia de Administración Tributaria y copia del acta de recepción en la que conste que las licencias han sido recibidas de conformidad por el "INTECAP". Dicho pago se hará con cargo a la partida presupuestaria número dos mil veinticinco guion once millones doscientos mil treinta y cuatro guion cero cero cero guion cero cero guion once guion cero cero guion cero cero cero cero guion cero cero uno guion cero cero cero guion cero ciento uno guion ciento cincuenta y ocho (2025-11200034-000-00-11-00-000-001-000-0101-158), de Administración Institucional, Informática y/o en la que en el futuro corresponda.

CUARTA: LUGAR, FORMA Y PLAZO DE ENTREGA: "Red Optima" se compromete a entregar el documento que contenga la información del servicio de la plataforma en Bodega General, en el Centro de Capacitación Guatemala uno (1), ubicado en la catorce (14) calle treinta y uno guion treinta (31-30), Colonia Ciudad de Plata II, zona siete (7) **de esta ciudad, en un plazo de cinco (5) días hábiles,** computados a partir del día siguiente de que el "INTECAP" le notifique por escrito, la aprobación del presente contrato.

QUINTA: SEGURO DE CAUCIÓN: a) DE CUMPLIMIENTO: "Red Optima" se obliga a prestar a favor y a entera satisfacción del "INTECAP" previa aprobación del presente contrato un seguro de caución de cumplimiento equivalente al diez por ciento (10%) del valor total del contrato, con una institución aseguradora debidamente autorizada para operar en Guatemala y de reconocida capacidad y solvencia financiera, en tanto dicho seguro no esté aceptado por el "INTECAP", éste no podrá hacerle ningún pago a "Red Optima". En caso de incumplimiento del presente contrato por parte de "Red Optima", el "INTECAP" dará audiencia por diez (10) días a la institución aseguradora, para que se manifieste al respecto, vencido

el plazo si no hay oposición manifiesta de la aseguradora, sin más trámite se ordenará el requerimiento respectivo y la institución aseguradora, deberá efectuar el pago dentro del plazo de treinta (30) días contados a partir de la fecha del requerimiento, circunstancia que se hará constar en la póliza. El seguro deberá mantenerse vigente hasta que el "INTECAP" compruebe que "Red Optima" ha cumplido con las condiciones del contrato, extendiendo la constancia respectiva para la cancelación.

SEXTA: SOPORTE TÉCNICO: "Red Optima", ofrece soporte técnico integral durante todo el proceso de despliegue de la solución incluyendo provisión de licencias, infraestructura en la nube y servicios asociados. Este soporte garantiza una implementación sin contratiempos y sin costos adicionales fuera del contrato inicial, cubriendo todas las etapas desde la instalación hasta la operación completa y asegurando el cumplimiento de los requisitos técnicos y funcionales específicos. Cuenta con un centro de atención SOC/CiberSOC que posee certificaciones de seguridad basadas en estándares reconocidos, incluyendo ISO veintisiete mil (ISO 27000), que garantiza la privacidad y la capacidad adecuada para el manejo seguro de la información; ofrece un servicio de soporte a través de un centro de servicio o mesa de ayuda con las siguientes características: disponibilidad veinticuatro por siete (24x7) tanto de manera remota como presencial, atención de solicitudes vía telefónica correo electrónico y portal web, soporte con solicitudes ilimitadas para los usuarios, en caso de fuerza mayor, escalamiento directo con el fabricante para resolución remota con disponibilidad veinticuatro por siete (24x7), este modelo asegura una atención continua y efectiva frente a incidentes y solicitudes; garantiza la implementación de actualizaciones menores y parches de seguridad considerados críticos durante el periodo de garantía. Estos parches se aplican en

un máximo de cuarenta y ocho (48) horas tras su liberación. Además la solución recibe actualizaciones periódicas para mejorar su funcionalidad y rendimiento, asegurando la continuidad y seguridad operativa; ofrece un nivel de servicio con una disponibilidad igual o superior al noventa y nueve punto cinco por ciento (99.5%), esto garantiza una operación continua y confiable para la protección y monitoreo de la infraestructura de seguridad; el incumplimiento de los compromisos aquí contraídos será motivo para requerirle por la vía correspondiente el cumplimento de estas obligaciones.

SÉPTIMA: INDUCCIÓN: "Red Optima" proporciona transferencia de conocimientos para un mínimo de seis (6) personas del Departamento de Informática, la capacitación abarca temas de funcionamiento, configuración y administración de la solución, con una duración de ocho horas por persona, en los días, horarios y lugares establecidos por el Departamento de informática. Además, en caso de requerirse transferencia adicional por cambios o ajustes en la solución, esta será proporcionada sin costo adicional.

OCTAVA: PROHIBICIONES: "Red Optima" tiene la prohibición expresa de ceder, enajenar, traspasar o disponer de cualquier forma, total o parcialmente los derechos provenientes del presente contrato, bajo pena de nulidad de lo pactado.

NOVENA: DECLARACIÓN JURADA: Yo, **ESTUARDO JOAQUÍN OLIVARES RUIZ,** declaro bajo juramento que ni yo en lo personal ni mi representada nos encontramos comprendidos en las limitaciones contenidas en el Artículo ochenta (80) de la Ley de Contrataciones del Estado; así como no somos deudores morosos del Estado ni de las entidades a que se refiere el Artículo uno (1) de la referida Ley.

DÉCIMA: CLÁUSULA RELATIVA AL COHECHO: Yo, **ESTUARDO JOAQUÍN OLIVARES RUIZ,** manifiesto que conozco las penas relativas al delito de cohecho,

así como las disposiciones contenidas en el Capítulo III del Título XIII del Decreto 17-73 del Congreso de la República de Guatemala, Código Penal. Adicionalmente, conozco las normas jurídicas que facultan a la Autoridad Superior del "INTECAP" para aplicar las sanciones administrativas que pudieren corresponderme, incluyendo la inhabilitación en el Sistema de Información de Contrataciones y Adquisiciones del Estado denominado GUATECOMPRAS.

DÉCIMA PRIMERA: CASO FORTUITO O FUERZA MAYOR: Si surgiere un caso fortuito o de fuerza mayor que impidiera a cualquiera de las partes cumplir con sus obligaciones contractuales, convienen en dar aviso a la otra parte por escrito dentro del plazo de cinco (5) días de ocurrido el hecho, acompañando las pruebas pertinentes para que si estuviere justificada la causa no se aplique la sanción.

DÉCIMA SEGUNDA: TERMINACIÓN DEL CONTRATO: El presente contrato se dará por terminado cuando ocurran cualesquiera de las circunstancias siguientes: a) Por vencimiento del plazo siempre que no se haya acordado prórroga alguna; b) Por rescisión unilateral del INTECAP, al determinarse atraso en la entrega de las licencias; con base a la fecha establecida y fijada en el presente contrato, sin perjuicio de aplicar las multas que correspondan de conformidad con los Artículos ochenta y cinco (85) y ochenta y seis (86) de la Ley de Contrataciones del Estado; c) Por rescisión acordada de mutuo acuerdo; y d) Por casos fortuitos o de fuerza mayor que hagan innecesario el contrato o que afecten su cumplimiento.

DÉCIMA TERCERA: CONTROVERSIAS: Los otorgantes convenimos expresamente en que toda controversia, diferencia o reclamación que surgiere como consecuencia del presente contrato, serán resueltas directamente con carácter conciliatorio, pero si no fuera posible llegar a un acuerdo, la cuestión o

cuestiones a dilucidarse, se someterán a la jurisdicción del Tribunal de lo Contencioso-Administrativo.

DÉCIMA CUARTA: SANCIONES: a) Retraso en la entrega: El retraso de "Red Optima" en la entrega de las licencias por causa imputable a él, se sancionará con el pago de una multa por cada día de atraso, del valor que represente la parte afectada, conforme al artículo ochenta y cinco (85) de la Ley de Contrataciones del Estado y los porcentajes establecidos en el Reglamento de la Ley de Contrataciones del Estado; b) Variación en calidad o cantidad: Si, "Red Optima" contraviniendo total o parcialmente el contrato, perjudicare al "INTECAP", variando la calidad o cantidad del objeto del mismo, será sancionado con una multa del cien por ciento (100%) del valor que represente la parte afectada de la negociación, de conformidad con el artículo ochenta y seis (86) de la Ley de Contrataciones del Estado. El "INTECAP" por cualquiera de los conceptos indicados en los literales anteriores, podrá hacer la deducción correspondiente del saldo que hubiere a favor del contratista o hacer efectivo el seguro respectivo.

DÉCIMA QUINTA: RECEPCIÓN Y LIQUIDACIÓN: "Red Optima" al disponer de las licencias de la plataforma y estar lista para la entrega de las mismas, deberá hacerlo del conocimiento de la Gerencia del "INTECAP", por escrito, quien nombrará la comisión receptora y liquidadora que fundamentándose en el contrato, bases y oferta, verificará cantidad, calidad y demás especificaciones y recibirá las licencias descritas en la cláusula segunda del presente contrato, diligencia en la cual deberá estar presente un representante de "Red Optima", en caso contrario, se entenderá que acepta el contenido de las actas que se faccionen, de las cuales se enviará copia certificada a donde corresponde, para los efectos que procedan; la liquidación

deberá practicarse dentro de los noventa (90) días subsiguientes a la recepción de las licencias.

DÉCIMA SEXTA: APROBACIÓN: Para que el presente contrato surta sus efectos legales y obligue a las partes a su cumplimiento, es indispensable que sea aprobado de conformidad con la Ley.

DÉCIMA SÉPTIMA: ACEPTACIÓN: Los otorgantes en los términos y condiciones estipuladas aceptamos el presente contrato, el que, leído íntegramente, por ambas partes y enterados de su contenido, validez y efectos legales, lo ratificamos, aceptamos y firmamos en nueve (9) hojas de papel membretado del "INTECAP".

Ing. Arnaldo Ademar Alvarado Cifuentes
Sub Gerente

Intecap
Subgerencia

Ing. Estuardo Joaquín Olivares Ruiz
Administrador Único y Representante Legal

RED ÓPTIMA, S.A.