Intecap

CONTRATO NÚMERO GE GUION AL GUION CUARENTA Y NUEVE GUION DOS MIL VEINTICINCO (GE-AL-49-2025). En la ciudad de Guatemala, el cuatro de agosto de dos mil veinticinco. **NOSOTROS: 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, **MANGLYO EDGARDO GARCÍA ARENALES,** de cincuenta y tres (53) años de edad, casado, Ingeniero, guatemalteco, con domicilio en el departamento de Chimaltenango y de paso por esta ciudad, con Documento Personal de Identificación (DPI), Código Único de Identificación (CUI) dos mil cuatrocientos sesenta y dos espacio sesenta y seis mil setecientos ocho espacio cero cuatrocientos dieciséis (2462 66708 0416), 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 "Servicomp de Guatemala, Sociedad

Anónima", inscrita en el Registro Mercantil General de la República de Guatemala, al número cincuenta y nueve mil doscientos ochenta y cinco (59285) folio novecientos veintiocho (928) libro ciento cincuenta y dos (152) de Sociedades; propietaria de la empresa de nombre comercial "Servicomp", inscrita en el Registro Mercantil General de la República de Guatemala, al número trescientos sesenta mil cuatrocientos treinta y siete (360437) folio trescientos nueve (309) del libro trescientos veintidós (322) de Empresas Mercantiles, calidad que acredito con el acta notarial de fecha diez de diciembre de dos mil veintidós, autorizada en esta ciudad por la Notaria Marelin Andrea Gil Noguera, debidamente inscrita en el Registro Mercantil General de la República de Guatemala, bajo el número seiscientos ochenta y tres mil seiscientos cuarenta y cuatro (683644), folio trescientos (300), libro ochocientos once (811) de Auxiliares de Comercio; señalo como lugar para recibir notificaciones en la catorce (14) avenida siete guion doce (7-12) zona catorce (14), Empresarial La Villa, Bodega veintitrés (23), de esta ciudad, en lo sucesivo seré denominado "Servicomp". 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 veintiuno guion dos mil veinticinco (21-2025), cuyo objeto es la adquisición de licenciamiento de antivirus

a nivel institucional; bajo el número de operación Guatecompras veintiséis millones seiscientos cincuenta y dos mil quinientos veintiocho (NOG 26652528); Acta número SC guion cero sesenta y ocho guion dos mil veinticinco (SC-068-2025), de fecha veinticuatro de junio de dos mil veinticinco, de recepción y apertura de plicas; Acta número SC guion cero setenta y ocho guion dos mil veinticinco (SC-078-2025), de fecha dos de julio de dos mil veinticinco, de calificación y adjudicación de ofertas; cotización contenida en formulario electrónico COT guion dos mil veinticinco guion veintiséis millones seiscientos cincuenta y dos mil quinientos veintiocho guion treinta y siete millones trescientos noventa y un mil novecientos diecisiete (COT-2025-26652528-37391917), código de autenticidad seis millones trescientos sesenta y nueve mil setecientos sesenta y nueve E (6369769E), de fecha diecinueve de junio de dos mil veinticinco; oferta de "Servicomp", de fecha veinticuatro de junio de dos mil veinticinco; Acuerdo de aprobación de la adjudicación número GE guion cuatrocientos cuarenta guion dos mil veinticinco (GE-440-2025), de fecha catorce de julio de dos mil veinticinco; y Memorando número SS guion noventa guion dos mil veinticinco (SS-90-2025), de fecha dieciséis de julio de dos mil veinticinco. Se tiene por incorporada al presente contrato la documentación anteriormente citada.

SEGUNDA: OBJETO DEL CONTRATO: Adquisición de licenciamiento de antivirus a nivel institucional; para el efecto "Servicomp" vende al "INTECAP" lo siguiente: Licenciamiento de antivirus con prevención, detección y respuesta ampliada y avanzada de amenazas, marca ESET Protect Elite, dos mil (2000); se utilizará para la protección de 2000 dispositivos por un plazo de doce (12) meses. Con las siguientes características específicas: CONSOLA DE ADMINISTRACIÓN; incorpora garantía de compatibilidad extendida para sistemas operativos sesenta

y cuatro (64) bits, Microsoft Windows® diez (10), once (11) o superior, Microsoft Windows Server dos mil dieciséis (2016) o superior, Ubuntu LTS veinte (20) + , RedHat ocho (8) +, CentOS ocho (8)+,Virtual Appliance compatible con VMware vSphere/ESXi & Microsoft Hyper-V; permite importar o exportar configuraciones del producto de manera fácil, vía archivos xml livianos y transportables, se garantiza tanto para estaciones de trabajo como servidores; toda configuración del producto en general puede realizarse desde consola administrativa, puede gestionarse integralmente desde una única consola administrativa centralizada. Queda descrito que todos los productos adquiridos se administrarán desde una sola consola de administración, no importando el sistema operativo sobre el cual hayan sido implementados; la consola de administración posee soporte para equipos y/o servidores clonados sean estos físicos o virtuales, el identificador por disco o volumen de disco no constituye un problema para identificar individualmente cada equipo administrado; el servidor de administración y consola administrativa son totalmente un modelo de servicio basado en la nube, no requiere espacio físico o equipo alguno donde esta funja como nodo central para la administración de la totalidad del licenciamiento requerido; se otorga totalmente en modalidad nube, no requiere instalación alguna de componentes de administración interna, salvo sean requeridos repositorios o contenedores de actualizaciones internamente; el servidor y consola de administración proveen factibilidad de selección del centro de datos por ocupar para albergar la misma, sea la selección deseada dentro del territorio de los Estados Unidos de América y/o la Unión Europea; el servidor y consola de administración operan dentro del entorno de seguridad y disponibilidad de Microsoft Azure, dentro de localidad USA o bien dentro de territorio EU; el servidor y consola de administración ocupa

Intecap

Microsoft Azure para la seguridad física y ambiental del centro de datos donde la misma sea albergada; el centro de datos en la nube donde se albergue la consola/servidor utiliza criptografía sólida para proteger los datos de los clientes durante el transporte fuera del sitio desde el entorno de la nube (por ejemplo, en tránsito a un almacenamiento de datos de respaldo físico), garantiza la seguridad de la información contenida dentro del mismo servidor/consola de administración; la comunicación entre agente de conexión y servidor de administración en la nube, se realiza mediante puerto TCP cuatrocientos cuarenta y tres (443) ocupando medidas de seguridad de transporte cifrado TLS y no interceptable en el medio, es decir protocolo de comunicación entre agente y servidor está cifrado adicional al canal cifrado de comunicación TLS ocupado; el servidor de administración y consola posee asignada una única instancia de hardware en forma privada que no comparte base de datos y/o recursos con un tercero, de forma tal que cada instancia de acceso es totalmente diferente para cada cliente del fabricante seleccionado, de tal forma que se delimita cualquier afección en caso de acceso no autorizado a una tercera instancia dentro de la infraestructura nube del fabricante seleccionado; la consola de administración ofrece protección contra ataques de fuerza bruta, inactivando acceso a la fuente origen (IP) que ha causado afección, integra funcionalidades extendidas de seguridad por medio integración de doble factor de autenticación; el servidor de administración y la consola administrativa ofrecen una consolidada y completa administración de los productos adquiridos, en su totalidad indican el estado, configuraciones y políticas aplicadas de cada uno de los nodos internos ligados a dicha consola de administración; el servidor de administración y consola administrativa ofrecen diversos y variados roles de acceso mediante grupos de usuarios con el fin de definir niveles de acceso

a administración de los diferentes recursos que dicha consola administrativa ofrezca a los administradores TI internamente; provisionan acceso web mediante servidor de aplicaciones JAVA, facilitando navegación y uso desde la mayoría de los navegadores web disponibles al momento dentro de la institución; la consola de administración opera en su totalidad en modalidad web, integralmente está desarrollada y compilada sobre código JAVA; el servidor de administración y consola administrativa ofrecen la posibilidad de segmentación para grandes redes mediante nodos de sincronización remota; de tal forma que facilitan la administración y sincronización de los clientes remotos, dichos nodos de sincronización podrán obrar como gestores de firmas, repositorios locales de instaladores, así como receptores de políticas y estados de los clientes locales; la consola de administración es totalmente web, compatible con cualquier navegador web tanto en sistemas operativos Microsoft, GNU/Linux, Mac OS y/o cualquier otro que a conveniencia pueda ocuparse para el acceso a dicha consola de administración; la consola de administración web se garantiza para al menos los siguientes navegadores sin requerir la instalación de algún plugin y/o complemento adicional dentro del mismo navegador o bien dentro del computador ocupado para la gestión de consola administrativa: Mozilla Firefox, Microsoft Edge, Google Chrome, Safari y Opera; la consola de administración web ofrece por completo administración para todos los productos ofertados independientemente del sistema operativo donde esta implementado, de forma tal que en su totalidad y absolutamente todos los productos sean administrados desde una sola interfaz web; la consola de administración incorpora Dashboard accesibles desde cualquier navegador web y desde cualquier punto dentro o fuera de la red local; no requiere para dicha operación el uso de IIS o motor diferente al integrado

nativamente por la solución; la consola de administración no requiere de la existencia de un Dominio de Autenticación de Usuarios para su buen funcionamiento o como condicionante de operación; sin embargo permite administrar clientes antivirus en distintos grupos de trabajo o multi-dominios ya existentes; la consola de administración web no requiere para su funcionamiento u operación sobre plataformas ASP, JSP o PHP; dicho de otra forma, la consola de administración no se basa en ninguna de las tecnologías indicadas anteriormente. La consola de administración soporta y maneja múltiples tipos de licencias del producto de seguridad, en diferentes cantidades de equipos y fechas de expiración; no requiere el uso de MMC (Microsoft Management Console) para el funcionamiento de la misma o como requisito de instalación. En términos de una correcta administración posee una configuración establecida para un determinado cliente (endpoint) pueda ser exportada en formato de fichero XML, tanto desde la Consola de administración, como desde el mismo cliente, para poder ser importada en otros clientes en caso de ser necesario; cuenta con un método para la instalación remota desatendida ya sea ocupando autenticación local o vía un directorio de autenticación, no importando si esta se realiza en dominio o en grupos de trabajo; la consola y servidor de administración no requieren System Center Configuration Manager (SCCM), CM doce (CM12), CM cero (CM0), ConfigMgr, Configuration Manager o similar para uso de consola administrativa y/o servidor de administración; el servidor central de administración (consola/servidor) es compatible a nivel de almacenamiento de registros (logs) con base de datos MySQL y SQL Server; dicha compatibilidad garantiza el funcionamiento correcto con versiones "libre de pago" de dichas bases de datos (MySQL Community Edition & MS SQL Server Express); el servidor central de administración es

compatible con SYSLOG en forma nativa, los eventos ocurridos en los clientes puedan ser interpretados por un syslog server; la consola y servidor de administración no requieren Microsoft Message Queue para instalación y/o operación; la consola/Servidor cuenta con doble factor de autenticación dos FA (2FA) para su interfaz web de administración; en forma gratuita hasta cinco operadores, así como no requiere de hardware/software que requiera pago o licenciamiento adicional; consola/servidor puede desplegar el inventario de hardware/software instalado en cada estación de trabajo o servidor donde sea desplegada la solución de seguridad; la consola permite enviar comandos o secuencias de líneas de script, particularmente dicha funcionalidad permite ejecución de al menos: Powershell, Comandos de pila CMD (bat), Cscript/ VBscript, MISEXEC scripts, entre otros; la consola/ servidor de administración permite actualizaciones automáticas para producto de seguridad tanto para las estaciones de trabajo final, así como para los servidores y sus respectivos sistemas operativos solicitados para cobertura final (Windows, Linux, MacOs). permite gestionar notificaciones automatizadas ante eventos de seguridad y/o condicionantes de coincidencia que pueda definir el administrador final de la misma; la consola/servidor faculta log auditable que registra cualquier alteración, modificación y/o eliminación de políticas, equipos, configuraciones y/o demás actividades realizadas dentro de la misma. CLIENTE ENDPOINT: integra capacidades extendidas de respuesta que involucran a su vez tecnología de múltiples capas de protección integradas en el mismo producto, dicho de otra forma, se documenta con información pública del fabricante, dicho producto funcionalmente integra al menos quince (15) capas diferentes de múltiple nivel de protección incorporada al mismo; el producto es totalmente gestionado, así como

compatible con consola de administración interna ocupada para el efecto, y se certifica compatibilidad desde el sitio del fabricante en donde se corrobora que el producto es totalmente compatible con la consola de seguridad ocupada internamente, corresponde en nombre y desarrollador del producto al mismo fabricante; ofrece binarios firmados y/o compatibles con Microsoft Azure Code Signing, no se acepta componentes obsoletos de firma cruzada no soportados por sistemas operativos Microsoft al momento; incorpora protección en tiempo real contra todo tipo de malware; incluyendo virus, gusanos, troyanos, spyware, phishing, rootkit, adware, riskware, keyloggers, ransomware y/o otros códigos maliciosos nuevos y desconocidos. Específicamente para dicho fin no depende de que el Sistema Operativo del "Endpoint/Cliente" tenga las actualizaciones y Service Pack al día; incorpora protección contra virus boot, virus macros, virus residentes en RAM, virus de acción directa, virus encriptados, virus polimórficos, virus de FAT, ransomware, y cualquier otro tipo de código malicioso en general; integra sandbox incorporado en el propio producto, con el objetivo de contener amenazas, emularlas, detectarlas y eliminarlas; dicha protección en particular es capaz de observar el comportamiento en tiempo real de cualquier binario en memoria operativa (RAM y de detectar basado en patrones de comportamiento & ML amenazas nuevas y desconocidas del tipo cero (0) Day, APT's y/o cualquier tipo de código malicioso emergente; incorpora motor de inteligencia basado en tecnología de última generación ADN proactiva y precisa, con motor propio, no de terceros fabricantes y/o colaboraciones externas ajenas al fabricante; incorpora detección de virus en archivos compactados o empaquetados, sin importar el número de niveles de compresión, en los formatos: .zip, .rar, .arj, .cab, .lzh, .tar, .gz, ace, izh, upx y/o otros; integra micro actualización de componentes, de forma

tal que permite actualizar en forma automática a una versión superior sin intervención del administrador o bien algún comando de implementación remota, permite instalar dicha actualización hasta el próximo reinicio de equipo garantizando una actualización exitosa y sin corromper algún componente del producto de seguridad; permite automáticamente actualizaciones de seguridad y estabilidad para el producto de seguridad, mismas que se distribuyen automáticamente a las versiones compatibles de forma tal que le permitan actualizar versiones afectadas por alguna vulnerabilidad y/o bien versiones de correcciones mayores que puedan afectar el rendimiento u operatividad de los equipos donde está implementada solución, dicha funcionalidad está descrita por el fabricante en su documentación y es transparente en su política de actualización de producto; el producto instalado en el computador no presenta fragmentación para su correcto funcionamiento (múltiples módulos instalados en el computador reflejados en programas instalados "Agregar/Quitar Programas" no son aceptados, exceptuando únicamente al agente de conexión); permite importar o exportar configuraciones de clientes de manera fácil, vía archivos xml livianos y transportables; incorpora capacidad de generar casos de soporte directamente desde la interfaz gráfica de la solución y simplifica cualquier requerimiento de apoyo técnico directamente desde el producto instalado en el computador o servidor protegido con la solución de seguridad; incorpora capacidad de poder enviar a los centros de soporte técnico las muestras de virus o códigos maliciosos, con la finalidad de que puedan ser analizados y/o clasificados para su contingencia inmediata directamente desde la interfaz gráfica; integra compatibilidad con tecnología Intel TDT (Intel Threat Detection Technology) basada en hardware que ayuda a reforzar detecciones en memoria operativa, permite mejorar la protección

contra el ransowmare y apoya a mantener un alto rendimiento general del sistema, figura en la documentación de fabricante y/o sitios oficiales del mismo; incorpora chequeo y control de Actualizaciones para Microsoft Windows, dicho control puede ser configurado para reportar diferentes niveles de actualización o desactivar el informe de las mismas, facilita parchar actualizaciones Microsoft en forma forzada mediante tareas automatizadas y/o bien bajo petición del administrador de la solución; toda configuración a nivel de clientes, puede realizarse desde consola administrativa y puede gestionarse integralmente desde una única consola administrativa centralizada; integra interfaz gráfica de usuario con modo oscuro incorporado, producto permite seleccionar esquema de colores claros u oscuros para dicha interfaz de usuario final; incorpora compatibilidad nativa en su interfaz gráfica con dispositivos que integren tecnología TouchScreen; incluye múltiples capas de seguridad, que operan en forma conjunta y en su defecto tienen capacidad de proteger independientemente si alguna de ellas no detecta en un momento dado el vector de compromiso; garantiza proteger al endpoint final con diferentes métodos de protección y múltiples capas de seguridad comprobables según documentación de fabricante; incluye tecnología de múltiples capas de protección livesense, dicha información es visible en cada sitio web y/o documentación del fabricante; puede comprobarse dentro de la documentación de fabricante o sitio web internacional del mismo las diferentes capas de protección embebidas al producto de seguridad ofertado, dichas capas de seguridad deberán integrar al menos las siguientes características: aprendizaje automático basado en machine learning (Deep Learning, LSTM & Neural Networks), diferentes algoritmos de clasificación ML basados en múltiples modelos de decisión (LinearSVM, Random Forest, XGboost, entre otros), inspección conductual avanzada (Deep

Behavioral Inspection), protección UEFI / BIOS & Scanner UEFI Integración de protección Intel Threat Detection Technology (TDT), tecnología de protección ADN y/o Basada en Genética de Códigos Maliciosos, inteligencia de amenazas (telemetría) basada en nube, detección y bloqueo de comportamiento (HIPS), exploit Blocker a nivel host y de red, emulación por Sandboxing, exploración avanzada de memoria (memoria RAM), protección contra ataques basados en scripts, interfaz de Análisis Antimalware (AMSI), antiransomware, protección contra Phishing / Malware a nivel URL, protección contra Botnets, protección a nivel de red, control de dispositivos, protección contra ataques de fuerza bruta; tecnología integrada relacionada con Machine Learning y/o Redes Neurales de al menos veinticinco (25) años de antigüedad y desarrollo, garantizando que dichos algoritmos, modelos de clasificación y/o inteligencia de amenazas no impacten negativamente a los sistemas protegidos así como minimicen la cantidad de falsos positivos siendo estos cercanos a cero (0) o menor al cero punto cinco por ciento (0.5%) en pruebas de campo relacionadas, de similar manera el tiempo de madurez requerido para motores de inteligencia de amenazas avanzados aportando expertis provista por dicha tecnología de vanguardia permite integrar nuevos modelos de prevención, detección y respuesta incluyendo pero no limitando modelos de DeepLearning y/o IA (Inteligencia Artificial); incorpora protección a nivel Kernel, previniendo la desactivación y/o alteración por un tercero y/o código malicioso; incorpora protección a nivel Kernel, previniendo la desactivación y/o alteración por un tercero y/o código malicioso; incorpora auto-protección del núcleo y componentes de la suite de seguridad a nivel ASLR & DEP, no requiere de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"; incorpora

protección en tiempo real contra cualquier alteración al estado del kernel de la suite de seguridad, imposibilitando detenerlo o dejarlo inoperativo para protección del computador donde ha sido implementado; integra protección nativa de aprendizaje automático, la cual incluye mecanismos de simulación/detección mediante redes neurales y al menos seis algoritmos de clasificación integrados, dicho módulo de protección coadyuva en la detección de cualquier tipo de código malicioso nuevo y/o desconocido; no requiere de la instalación de cualquier modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"; integra protección nativa a nivel UEFI que permite comprobar y aplicar seguridad para el entorno previo al inicio y arranque del equipo, dicho modulo detecta componentes maliciosos en el firmware (UEFI/BIOS); no requiere de la instalación de cualquier modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"; incorpora capacidad de protección por contraseña de acceso al propio motor antivirus, a fin de que no pueda ser alterada configuración de la propia solución y/o alteración al estado de protección del computador; la instalación puede realizarse tanto localmente como remotamente desde su consola administrativa; en el término local se entiende se requiere precompilación de un paquete todo-en-uno para la instalación del producto el cual contenga las preconfiguraciones y niveles de seguridad básicos aplicables a la estación de trabajo, incorpora en un solo paso la unión y sincronización a consola administrativa; incorpora resolución automática para reinicios pendientes de actualizaciones de producto, actualizaciones de software de terceros y/o bien actualizaciones de sistema operativo, permite: posponer el reinicio a petición del usuario, reinicio forzoso del computador; definir tiempos de reinicio y/o tiempos que el usuario puede posponer el reinicio;

comunicación entre clientes administrados y servidor de administración debe realizarse mediante conexión SSL cifrada; dicha conexión es evidente y descrita en el log de estado del agente de conexión mediante cualquier navegador web para fines de validación o auditoría; el agente de conexión deberá provisionar log transaccional de referencia, así como en forma simultánea deberá mostrar su estado de conexión y descripción general de sincronizaciones a servidor administrativo; dicho log es accesible desde cualquier navegador web y en forma dinámica varía en forma automática a fin de evidenciar cualquier problema de comunicación o falla de transferencia y/o comunicación cifrada en la línea del tiempo; el agente de conexión reporta en forma precisa todo software de terceros y/o fabricante contratado ubicado en el computador que figure como instalado en el equipo donde ha sido instalado, reportando con precisión todo lo referente al hardware presente; el agente de conexión reporta en forma precisa el identificador o número de serie del equipo de cómputo en general, proporciona información sobre BIOS/UEFI instalado en el computador de forma tal que permite determinar inclusive la versión de firmware exacta de dicho componente de hardware; el agente de conexión soporta instalación de software de terceros, no delimitando e incluyendo cualquier aplicativo (EXE) que desee ejecutarse o instalarse en los computadores administrados; soporta la ejecución de comandos remotos en cada equipo donde sea desplegado, para al menos: Scripts basados en powershell (Windows); Scripts basados en Command Line (CMD - Windows); Scripts basados en Command Console (Linux): SISTEMAS OPERATIVOS COMPATIBLES: incorpora garantía de compatibilidad extendida para al menos los siguientes sistemas operativos: Microsoft Windows® once (11), diez (10), ocho punto uno (8.1), siete (7) SP uno (1), Microsoft Windows Server dos mil veintidós (2022), dos

mil diecinueve (2019), dos mil dieciséis (2016), dos mil doce R dos (2012R2), dos mil doce (2012), dos mil ocho R dos (2008R2), Mac OS diez punto doce (10.12) y/o superior, Mac OS Server, diez punto quince (10.15) o superior, RedHat, Debian, Ubuntu, Suse, Fedora & Centos así como la mayoría de distribuciones basadas en gestor de paquetes RPM y DEB con kernel Linux v tres punto diez punto cero (3.10.0) o superior, Android cinco (5) o superior; compatible con diferentes tipos de procesadores según corresponda el sistema operativo, se garantiza compatibilidad con: Sistema Operativo Windows: Intel o AMD x ochenta y seis (86) / x sesenta y cuatro (64) & ARM sesenta y cuatro (64), Sistema Operativo Mac OS: Intel sesenta y cuatro (64)-bits, Apple ARM sesenta y cuatro (64)-bits, Sistema Operativo Linux: Intel/AMD x sesenta y cuatro (64), Sistema Operativo Android: ARMv siete (7) e x ochenta y seis (86) Intel Atom. ACTUALIZACIONES DE SEGURIDAD: Las actualizaciones rutinarias de los modelos inteligentes de aprendizaje, son pequeñas e incrementales, tanto para actualizaciones rutinarias como para repositorios de distribución y/o cache local de actualizaciones. Se consideran como pequeñas e incrementales a las actualizaciones rutinarias menores a 500Kb por cada módulo de seguridad inteligente; una actualización rutinaria, capaz de actualizar modelos de detección y aprendizaje, módulos y/o componentes del sistema de seguridad, no incluyendo, pero no limitando la versión de familia del producto y/o futuras versiones del mismo; incorpora capacidad para que un cliente instalado (endpoint) pueda convertirse en repositorio de actualizaciones (mirror), con el fin de poder actualizar otros clientes desde este o poder extraer los archivos de actualización y trasladarlos manualmente a otros clientes "stand-alone"; no requiere la instalación de módulos adicionales para tales fines, no se refleja como componente adicional

en "Agregar/Quitar Programas"; posee factibilidad para actualizar de forma manual todos sus componentes y definiciones de módulos de seguridad sin ningún tipo de conectividad a red, es decir, en status "stand-alone"; las actualizaciones de distribución de firmas rutinarias (repositorios de firmas de seguridad) proveen a los clientes endpoint internos, mediante servicio HTTP/HTTPS incluido en el propio motor del producto instalado y ofrece métodos de autenticación básica o vía NTLM a fin de proteger contra el acceso de terceros a firmas de distribución local; dicha opción se integra y no está limitada y/o restringida como medio para distribución de firmas mediante motores FTP/Shares de terceros; no requiere la instalación de módulos adicionales para tales fines y no se refleja como componente adicional en "Agregar/Quitar Programas"; las actualizaciones diarias y rutinarias de los componentes del producto se realizan en tiempo real desde Internet o vía LAN Server (mirror), en forma automática y sin necesidad de intervención del usuario; se actualiza automáticamente desde una unidad extraíble que contiene los ficheros rutinarios de actualización sin intervención alguna del usuario local o bien del personal técnico; proveen un mecanismo de contención y/o mitigación de riesgos del tipo CVE incluidos o determinados para el producto, de forma tal que ante la existencia de una vulnerabilidad en el software contratado automáticamente el producto de seguridad integra un mecanismo de contención y actualización para la versión posterior estable que mitiga en caso dicha falencia de seguridad (acepta el reinicio forzoso desde la consola de administración y/o bien automatizada mediante disparadores automáticos de condiciones fijados por el administrador de producto final); HOST BASED INTRUSION PREVENTION SYSTEM: incorpora tecnología de control HIPS para estaciones de trabajo y servidores sobre plataforma Microsoft Windows, así como funcionalmente no requiere de instalación

de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas". Incorpora HIPS con capacidades avanzadas de protección, capaz de realizar las siguientes acciones básicas requeridas: bloquear archivos y/o aplicaciones para ejecución, permitir ejecutar archivos y/o aplicaciones basadas en rutas de acceso y/o ficheros en particular, bloquear archivos y/o carpetas contra escritura y/o acceso, permitir escritura y/o acceso para archivos y/o carpetas y bloquear escritura y/o modificación a llaves del registro de sistema; incorpora tecnología avanzada que permite prevenir la explotación de vulnerabilidades en las aplicaciones más comunes; principalmente pero no limitado control de explotación para navegadores web, PDF, clientes de correo electrónico, aplicaciones MS Office & Java; incorpora motor de inspección avanzada en memoria operativa que protege contra el malware moderno que ocupa técnicas de cifrado y/o ofuscación; incorpora protección avanzada contra la deshabilitación y/o modificación del propio motor de protección antivirus por parte de terceros y/o algún código malicioso, dicha función se refleja en el componente HIPS del producto ofertado; incorpora protección especializada contra ataques del tipo ransomware, visible dentro del apartado de configuración del producto final; específicamente el módulo especializado para la prevención del ransomware detecta y bloquea procesos cuyo comportamiento encuadra con la conducta del ransomware en general. FIREWALL & NETWORK INTRUSION DETECTION AND PREVENTION SYSTEM, integra protección contra ataques de fuerza bruta, de forma tal que un IP detectado como atacante es enlistado en una lista negra por un periodo de tiempo considerable y definido directamente por el fabricante de solución de seguridad; incorpora firewall/cortafuegos avanzado integrado directamente a la solución de seguridad, el mismo ofrece protección de doble vía

capaz de filtrar bidireccionalmente el tráfico de red ya sea este entrante o saliente, no requiere de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"; El firewall/cortafuegos es totalmente administrable desde solución local o desde consola administrativa, y posee modo de solución rápida a problemas comunes guiados intuitivamente desde la propia interfaz del producto. El Firewall/Cortafuegos incorporado posee facilidad para la definición de redes de confianza mediante parámetros de detección que faculten identificar si en realidad dispositivo protegido se encuentra en una red "segura" o bien se requiere un modo superior de protección en una red nueva y desconocida; incorpora IDS & IPS (Intrusion Detection System and Intrusion Prevention System) de host para la prevención de acceso no autorizado al computador a nivel de capa de red, no requiere de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"; incorpora protección anti "BOTNETS", que faculta a la solución bloquear el acceso y comunicación a una red botnet y alerta al usuario de dicha acción y anomalía detectada; no requiere de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"; incorpora Control de Vulnerabilidades a nivel de capa de red, el cual inspecciona y protege a los protocolos más ampliamente utilizados SMB, RPC y RDP; evitando con dicho fin la propagación del malware, ataques de red dirigidos y la explotación de vulnerabilidades para las que un parche de seguridad aún no está disponible o ha sido desplegado, no requiere de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"; integra capacidad de listas negras para la prevención de acceso por parte de actores

maliciosos hacia equipos publicados sobre el internet o con acceso a segmentos públicos del internet, otorga capacidades extendidas de red que permiten delimitar el acceso de un tercero al equipo protegido si este está intentando acceso al recurso desde una IP pública comprometida y en lista negra del fabricante del producto de seguridad; integra capacidad extendida para el bloqueo de al menos: recursos administrativos de sistema (IPC$, C$, entre otros)Impresores y recursos compartidos; versiones obsoletas o inseguras de SMB / RPC, ejecución de binarios dados desde recursos SMB, ejecución de binarios dados desde recursos SMB fuera de la zona de confianza o bien desde redes externas a la red declarada como segura; conexiones SMB no seguras o sin seguridad extendida habitada, servicio del Registro Remoto, servicio del Local Security Authority, servicio del Service Control Manager, tráfico NetBios / SSDP, el cortafuegos incorporado es capaz de prevenir escaneo de puertos sea sobre protocolo TPC o UDP, y detecta tráfico malicioso del tipo ARP o posesión de los paquetes ARP como tal, posee la capacidad de definir tiempos de bloqueo establecidos para tráfico detectado como anómalo o malicioso, por defecto al menos permite fijar diez minutos (10min) de bloqueo al host origen (malicioso o atacante). FILTRADO DE RED Y/O PROTOCOLOS DE COMUNICACIÓN, incorpora la capacidad de filtrado de protocolos, para todo el tráfico de red; teniendo opción de analizar todo tipo de comunicación saliente/entrante. No requiere de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"; incorpora escaneo y limpieza de paquetes en tráfico HTTP, FTP, SMTP y POP3 tanto en los servidores como en las computadoras personales. incorpora filtrado e inspección de protocolos seguros (HTTPS, SMPTS, POP3S, FTPS, entre otros), es capaz de filtrar cualquier comunicación de

red segura, y no requiere de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control"; integra protección en los navegadores instalados dentro del equipo protegido, permite adoptar un enfoque de confianza cero en el mismo considerando todo lo que sea navegado en cualquier navegador sea considerado como riesgoso o no conocido; integra protección en los navegadores instalados dentro del equipo protegido, de forma tal que permite evitar técnicas de man-in-middle y faculta proveer características extendidas de protección, garantizando al menos lo siguiente relacionado al propio navegador: protección de memoria; protección del teclado, protección del portapapeles, protección de memoria y análisis de Script del Navegador; Incorpore capacidad de excluir aplicaciones, direcciones IP y/o rangos de direcciones del filtrado de protocolos e inspección al tráfico de red; incorpora capacidad de analizar todo el tráfico de red o bien indicar puertos y/o aplicaciones en particular a inspeccionar a nivel de filtrado de protocolos; incorpora filtrado básico para listas URL y/o IP de acceso; se puede controlar efectivamente accesos a los listados estáticos definidos, ya sean sobre comunicación en texto plano (HTTP) o sobre protocolos seguros (HTTPS); no requiere de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"; incorpora plugin para el filtrado, análisis y detección antimalware en los clientes de correo electrónico Microsoft Outlook, Windows Mail & Windows Live Mail; no requiere de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control"; incorpora tecnología avanzada que integra capas de seguridad previa al host a fin de prevenir la explotación de vulnerabilidades a nivel de red desde host remotos o locales, protege el endpoint final contra vulnerabilidades conocidas que puedan

afectar a nivel de red aun así no exista parche local instalado en el equipo que desea protegerse, no requiere de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control"; garantiza la inspección de tráfico SSL para al menos los navegadores web instalados en el computador, posee capacidad de análisis para el tráfico https y/o comunicaciones asociadas al mismo. WEB FILTERING & ANTISPAM, integra capacidad de Filtrado Web basado en categorías, con la posibilidad de definir políticas basadas en grupos de usuario y/o usuarios (tanto a nivel AD como también mediante autenticación local), no requiere de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control"; integra capacidad de Filtrado Web mediante grupos de categorías, haciendo factible el agrupamiento de múltiples y diferentes categorías de inspección URL para una misma regla de navegación; faculta permitir y/o denegar el acceso a URL estáticos mediante reglas configuradas en el Filtrado Web; provee posibilidad de agrupamiento en políticas de filtrado URL, siendo factible sumar diferencialmente los accesos y/o denegaciones a fin de aplicar una política final de maquina o grupo de usuarios; integra capacidad para la generación de logs y sincronización de los mismos a consola corporativa, de acuerdo a cada una de las acciones tomadas en concordancia con la regla URL definida ya sea bloqueo o permisión según sea el caso; dicho log contiene toda la información detallada desde el URL bloqueado/permitido hasta el usuario/equipo detectado así como hora/fecha y descripción integra del evento; no requiere de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control"; integra capacidad Filtrado Web sobre sitios URL que ocupen protocolo seguro (HTTPS), no requiere de instalación y/o módulo reflejado en componentes de

programa en "Agregar quitar Programas -> Panel de Control"; toda regla y/o política para el control URL, puede ser fijada por horarios, días de la semana en particular y/o por usuarios en especifico; garantiza protección URL anti phishing para el acceso web y/o mensajes recibidos mediante correo electrónico en cualquiera de las aplicaciones requeridas como compatibles (Microsoft Outlook, Windows Mail & Windows Live Mail); incorpora solución antispam y posee filtrado para protocolo SMTP, POP3 & IMAP en forma transparente e integrada al producto sin requerir instalación de módulos y/o agentes en el computador, no requiere instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control"; incorpora plugin para el filtrado, análisis y clasificación antispam en los clientes de correo electrónico Microsoft Outlook, Windows Mail & Windows Live Mail; no requiere de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control". provee capacidad de generar listas blancas/negras para el filtrado del correo electrónico en la estación de trabajo final y en los clientes de correo electrónico indiciados como compatibles, dicha acción se puede realizar desde el propio producto y/o consola de administración, permite definir dominios y/o direcciones en cada uno de estos apartados; Provee capacidad de protección antimalware, anti phishing y anti spam para todo lo referido con protección email sobre las aplicaciones requeridas como compatibles (Microsoft Outlook, Windows Mail & Windows Live Mail). DEVICE CONTROL, incorpora capacidades de "Device Control" administrables ya sea localmente o en forma remota desde su consola administrativa, no requiere de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control"; incorpora capacidades de "Device Control" avanzadas, con el fin de delimitar, denegar o

permitir dispositivos portátiles y/o medios extraíbles tales como: dispositivos de almacenamiento USB, dispositivos ópticos cd/dvd, impresoras usb, dispositivos de almacenamiento firewire, dispositivos bluetooth, tarjetas lectoras de memoria, dispositivos de imagen, modems, puertos lpt/com, dispositivos portátiles (móviles); incorpora funciones avanzadas para el control de dispositivos siendo posible aplicar reglas con el fin de delimitar, denegar o permitir de acuerdo a las siguientes condiciones del dispositivo periférico conectado: marca; modelo y serie; incorpora funciones avanzadas para el control dispositivos siendo capaz de asignar políticas de acuerdo a grupos de trabajo local o grupos dinámicos mediante un Directorio Activo; provee extensión de operación por usuario local y/o usuarios de un Directorio Activo; incorpora funciones avanzadas para el control de dispositivos mediante grupos de "dispositivos", se puede asignar reglas y/o directrices mediante grupos pre-establecidos de dispositivos con el fin de facilitar administración, así como el control adecuado de los dispositivos conectados a las estaciones de trabajo; toda regla y/o política para el control de dispositivos, puede ser fijada por horarios, días de la semana en particular y/o por usuarios en específico. CLOUD SANDBOXING, incorpora tecnología de detección en tiempo real basada en la nube, con el fin de prevenir ataques cero day (0Day) y/o campañas de propagación de malware lanzadas globalmente; dicho alcance está garantizado para correo electrónico, así como todo tipo de tráfico de red, tanto para reputación de archivos, así como vínculos URL; la integración de tecnología "Cloud Protection" no requiere de instalación de módulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"; la tecnología basada en la nube y en tiempo real, permite al usuario operador del endpoint verificar la reputación de los procesos activos y de los archivos

directamente desde la interfaz del programa o desde el menú contextual; incorpora tecnología en la nube para la detección de código nuevo y emergente, posibilitando detección del código malicioso y/o vínculo URL inclusive previo al lanzamiento de firmas antivirus de detección estándar; incorpora tecnología "Antiphishing", que previene al usuario de los intentos de adquirir contraseñas, datos bancarios y/o otra información sensible por parte de los sitios web falsos, haciéndose pasar por los legítimos; funcionalmente no requiere de instalación de módulos adicionales para tales fines, no refleja como componente adicional en "Agregar/Quitar Programas"; la tecnología de protección basada en la nube se basa en telemetría de datos integrada para al menos un billón de computadores globalmente, dicho de otra forma, garantiza la capacidad de integración para al menos la cantidad de endpoints descritos con la finalidad de aportar capacidad extendida de telemetría de datos y DeepLearning de última generación; incorpora tecnología de protección basada en la nube las siguientes capas de detección avanzada de amenazas: desempaquetado y análisis avanzado; detección de aprendizaje automático avanzado, motor de detección experimental y análisis exhaustivo del comportamiento; integra capacidad para al menos seleccionar los siguientes niveles de análisis para la validación del resultado aportado por la tecnología basada en la nube: malicioso, altamente sospechoso, sospechoso y limpio; tecnología de protección basada en la nube que otorga capacidad de protección zero-trust con la finalidad de impedir ejecución inmediata de ficheros descargados desde el internet, trasmitidos mediante dispositivos periféricos y/o transportados mediante carpetas de red, dicho de otra manera, garantiza dicha tecnología confirme la inocuidad de los mismos previo al uso y/o ejecución de dichos ficheros; tecnología de protección basada en la nube que otorga capacidad de definir tiempo

máximo de espera para la validación del resultado obtenido por la emulación sandboxing realizada por el mismo, permite establecer tiempo máximo que un fichero deberá ser retrasado para el acceso y/o ejecución del mismo dentro del computador; tecnología de protección basada en la nube que otorga visibilidad de cada fichero enviado a la misma, así como en forma precisa indica el veredicto obtenido mediante la emulación sandboxing cloud, de igual manera en caso de ser detectado un objeto malicioso permite obtener visibilidad del resultado de emulación del mismo, siendo capaz de identificar el mecanismo y razón por la cual fue detectado como malicioso; tecnología de protección basada en la nube que soporta sistemas operativos del tipo Windows, Linux & MacOS de forma tal que la misma puede ser habilitada con una simple tarea de configuración desde la consola/servidor central de administración sin requerir o valerse de software adicional instalado en el computador; tecnología de protección basada en la nube que provee automáticamente protección a todos los dispositivos ligados al licenciamiento adquirido de forma tal que ante una nueva y desconocida detección realizada por dicho componente en cualesquiera de los dispositivos protegidos permite proveer protección automática al resto de los mismos sin necesidad o intervención manual alguna de los operadores de la solución, constituyendo una capa de defensa automática identificada como Detection and Response dentro del framework de seguridad Gartner Adaptive Security Architecture (ASA). CIFRADO DE DISCO, El Agente de conexión es capaz de validar el estado de cifrado del computador, permite identificar con facilidad cualquier equipo no cifrado o asegurado correctamente mediante cifrado asimétrico AES de al menos doscientos cincuenta y seis (256) bits; ofrece capacidad de cifrado de disco duro completo con tecnología privativa para sistemas operativos del tipo Windows, no

se acepta gestión de Bitlocker o similar; permite cifrar automáticamente desde la consola de administración, es capaz de cifrar cualquier dispositivo gestionado desde la misma y nativamente sea soportado para los sistemas operativos requeridos como compatibles; ofrece capacidad de cifrado de disco duro completo para Mac OS, para dicho efecto deberá garantizarse total compatibilidad File Vault; se garantiza compatibilidad de cifrado de disco con los siguientes sistemas operativos: Windows diez (10) y Windows once (11), y Mac OS v diez punto catorce (v10.14) al catorce punto cero (14.0); soporta en forma explícita modo UEFI del disco duro, con la finalidad de otorgar mayor seguridad en el arranque y manejo del dispositivo; permite crear y gestionar políticas para la configuración del cifrado de disco, siendo capaz de otorgar diversas funcionalidades integradas al producto; permite desactivar pre-boot login de forma tal que no solicite una contraseña de acceso al dispositivo cifrado; permite uso de TPM para el cifrado de disco sobre estaciones de trabajo que ejecuten sistema operativo Windows; otorga compatibilidad con discos que habiliten funcionalidad OPAL sobre estaciones de trabajo que ejecuten sistema operativo Windows; garantiza lo siguiente para la gestión de usuarios y contraseñas: definir complejidad de contraseña, de forma tal que requiera obligatoriamente el uso de caracteres especiales, mayúsculas, minúsculas y/o números, limitar intentos de contraseña incorrecta, así como permitir establecer el máximo número de intentos fallidos previo a bloqueo temporal del acceso a disco cifrado, definir caducidad de contraseña y permitir establecer una antigüedad máxima permitida para la misma, permitir ocupar contraseñas (códigos) de recuperación desde la consola central de protección y permitir definir el número máximo códigos de recuperación por estación de trabajo; permite fijar contraseñas de recuperación en caso de un olvido accidental de

contraseña de cifrado y/o bien algún bloqueo asociado a la misma, este mecanismo de recuperación es posible tanto para estaciones Windows y Mac OS; otorga un mecanismo de descifrado forzado desde un medio extraíble y/o bien secuencia de comandos aplicable según corresponda y según sea el caso para estaciones de trabajo Windows o Mac OS; permite descifrar desde la consola de administración cualquier dispositivo previamente cifrado con la solución, sea una estación Windows o Mac OS. PROTECCIÓN NATIVA PARA MICROSOFT EXCHANGE SERVER, integra protección para la capa de transporte del correo electrónico provisionado por Servidor Microsoft Exchange en forma totalmente transparente, dicha funcionalidad ser realiza tanto para el correo saliente como el correo entrante sin requerir la instalación y/o modulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control"; integra protección Antimalware, Antispam, Anti-Phishing & Análisis mediante cloud sandboxing para todo correo electrónico enviado y/o recibido mediante Servidor Microsoft Exchange, no requiere de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control"; integra protección antimalware para la base de datos embebida a Microsoft Exchange, de forma tal protege cada buzón de usuario e inclusive realizar análisis retrospectivo para los buzones de correo electrónico que pudiesen haber recibido código malicioso previo a la instalación de dicha solución de seguridad; no requiere de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control"; integra protección antimalware integrada directamente a la base de datos ocupada por Microsoft Exchange, protege del envió/recepción de código malicioso inclusive cuando se ocupa portal web provisionado por Microsoft Exchange (OWA); no requiere de instalación y/o módulo reflejado en componentes

de programa en "Agregar quitar Programas -> Panel de Control"; integra funcionalmente protección a nivel de transporte para Microsoft Exchange, puede realizar lo siguiente: filtrar correos electrónicos basado en el tipo de documento adjunto (identificador por tipo de ficheros), filtrar correos electrónicos basado en el contenido del adjunto (identificador de ficheros por tipo y uso), filtrar correos electrónicos basado en el contenido del cuerpo del mensaje (body message), puede identificar características, texto o similar contenido en el mismo, filtrar correos electrónicos por tipo de extensión (filtrado de extensiones permitidas), filtrar correos electrónicos por tamaño del mensaje; filtrar correos electrónicos que hayan sido enviados a múltiples usuarios (cadenas de mensaje), delimitar cadenas de mensajes o bien identificar y bloquear por medio de contadores cualquier tipo de correo electrónico que encuadre en identificación de cadenas de mensajes (dirigido en forma específica una cantidad de usuarios por definir y totalmente variable, ej: diez (10), treinta (30), treinta y tres (33) destinatarios en un solo mensaje); incorpora solución antispam a nivel endpoint y posee filtrado para protocolos SMTP, POP3 & IMAP en forma transparente e integrada al producto sin requerir instalación de módulos y/o agentes en el computador. PROTECCIÓN DE LA NUBE PARA MICROSOFT TRESCIENTOS SESENTA Y CINCO (365) & GOOGLE WORKSPACE, incorpora un motor de inspección multicapa basado en la nube que otorga protección contra las diferentes amenazas modernas que ocupan técnicas de cifrado y/o ofuscación, permite proteger e integrarse nativamente con plataformas Office trescientos sesenta y cinco (365) mediante servicio SaaS integrado directamente al tenant de Microsoft trescientos sesenta y cinco (365) y/o integrarse con Google Workspace para protección de Google Drive y Google Mail; el nivel de alcance y protección en la nube se garantiza e integra

en forma fácil y precisa con las plataformas: Microsoft OneDrive for Business, Microsoft Exchange Online Microsoft Sharepoint Online, Microsoft Teams, Google Workspace (Google Mail & Google Drive); otorga compatibilidad de protección para al menos los planes Microsoft trescientos sesenta y cinco (365): Planes de Microsoft trescientos sesenta y cinco (365) Education, Microsoft trescientos sesenta y cinco A tres (365A3), Microsoft trescientos sesenta y cinco A cinco (365A5), Planes de Exchange Online, Exchange Online Plan uno (1), Exchange Online Plan dos (2), Microsoft trescientos sesenta y cinco (365) Business Standard, Planes de OneDrive, OneDrive for Business Plan uno (1), OneDrive for Business Plan dos (2), Microsoft trescientos sesenta y cinco (365) Business Basic, Microsoft trescientos sesenta y cinco (365), Business Standard; cubre la totalidad de usuarios solicitados para protección en la nube para las aplicaciones en la nube para Microsoft trescientos sesenta y cinco (365) & Google Workspace, garantiza la inspección de todo correo electrónico y/o fichero almacenado sobre Microsoft OneDrive for Business & Sharepoint Online y/o bien Google Mail & Google Drive; incorpora tecnología de detección en tiempo real basada en la nube, con el fin de prevenir ataques cero Day (0Day) y/o campañas de propagación de malware lanzadas globalmente; dicho alcance se garantiza para correo electrónico, así como todo tipo de tráfico de red, tanto para reputación de archivos, así como vínculos URL; integra tecnología "Cloud Protection que se integra mediante API Cloud ofertada mediante modelo Software-as-a-Service (SaaS); incorpora tecnología sandboxing basada en la nube que integra al menos tres (3) modelos de aprendizaje deep-learning (Deep Machine Learning) y al menos seis (6) modelos de clasificación para cada modelo Deep Machine Learning aplicado; garantiza protección integrada mediante API cloud para cualquier tipo de fichero

mediante análisis cloud sandboxing, automáticamente y sin intervención alguna del usuario clasifica, detecta y/o elimina cualquier código malicioso nuevo o desconocido; incorpora tecnología en la nube para la detección de código nuevo y emergente, posibilitando detección del código malicioso y/o vínculo URL inclusive previo al lanzamiento de firmas antivirus de detección estándar; incorpora tecnología "Antiphishing", previene al usuario de los intentos de adquirir contraseñas, datos bancarios y/o otra información sensible por parte de los sitios web falsos, haciéndose pasar por los legítimos; provee una auditoria detallada de las acciones ejecutadas para tratamiento antispam, antivirus y/o phishing, sin importar ni delimitar acciones tomadas para Microsoft OneDrive for Business & Microsoft Sharepoint Online así como para Google Drive & Google Mail; integra protección para la capa de transporte del correo electrónico provisionado por Servidor Microsoft Exchange Online (Office trescientos sesenta y cinco (365) & Google Workspace (Gmail) en forma totalmente transparente, dicha funcionalidad se realiza tanto para el correo saliente como el correo entrante sin requerir la instalación y/o modulo reflejada en cualquier computador interno a la red y visible desde componentes de programa en "Agregar quitar Programas -> Panel de Control"; integra protección Antimalware, Antispam, Anti-Phishing & Análisis mediante cloud sandboxing para todo correo electrónico enviado y/o recibido mediante Servidor Microsoft Exchange Online y/o Google Mail; provee capacidad de generar listas blancas/negras para el filtrado del correo electrónico en la estación de trabajo final y en los clientes de correo electrónico indicados como compatibles; se puede realizar desde el propio producto y/o consola de administración y permite definir dominios y/o direcciones en cada uno de estos apartados; provisiona cuarentena centralizada para archivos de Exchange Online,

OneDrive, Teams, Sitios de SharePoint, Google Drive y/o Google Mail, misma que deberá provisionar al menos treinta (30) días de retención garantizada; provisiona administración de cuarentena sencilla para los mensajes de correo electrónico, de los archivos adjuntos, así como de los archivos de Exchange Online, OneDrive, Teams, Sitios de SharePoint, Google Drive y/o Google Mail. VULNERABILITY & PACH MANAGEMENT, garantiza gestión de vulnerabilidades y parcheo de aplicaciones para al menos los siguientes sistemas operativos: Microsoft Windows diez (10), once (11), Microsoft Windows Server dos mil doce (2012) R dos (2), dos mil dieciséis (2016), dos mil diecinueve (2019) y dos mil veintidós (2022); garantiza gestión de vulnerabilidades y parcheo de aplicaciones en cada estación y/o servidor donde sea requerido, para dicho efecto no requiere la instalación de ningún componente adicional en el computador o bien de complementos o plugin adicionales para dicha gestión, en otras palabras, la gestión de parches y vulnerabilidades está integrada en el propio producto de seguridad ofertado; permite visualizar a nivel de vulnerabilidades todo lo relacionado con el riesgo de aplicaciones y sus consideraciones descriptivas, de forma tal que garantiza otorgar visibilidad de lo siguiente: nombre de la aplicación, versión de la aplicación, fabricante de la aplicación, puntuación de riesgo cero a cien (0 – 100), CVE de Referencia, Categoría de Vulnerabilidad (Aplicación o Sistema Operativo) e Información detallada por equipo, por grupo de equipos y/o por totalidad de equipos; proporciona un listado público de aplicaciones cubiertas por el gestor de vulnerabilidades y parcheo de aplicaciones, el mismo puede ser visible desde un sitio web propio del fabricante de solución; provisiona un gestor de parcheo para cobertura de las vulnerabilidades descubiertas internamente, sean estas de aplicaciones o de sistema operativo según corresponda cobertura para cada uno

de los sistemas operativos requeridos al efecto; provisiona opciones de parcheo automatizado, permite definir estrategia de parcheo y actualización internamente, sean totales o bien delimitadas para determinadas aplicaciones que se consideren como seguras para actualización automatizada, en general solución permite diferentes estrategias de actualización según sea necesario por cada sistema involucrado internamente; provisiona actualizaciones automáticas para sistemas operativos indicados como requeridos, permite definir actualizar sea todas las actualizaciones necesarias o bien definir solo actualizaciones críticas de seguridad aplicables al sistema; permite definir horarios de inspección de versión de vulnerabilidades de aplicaciones y/o sistema operativo, permite definir rangos horarios aplicables donde solución puede corroborar actualizaciones pendientes sean del sistema operativo y/o aplicaciones instaladas soportadas por el gestor de vulnerabilidades; permite definir tiempos de reinicio si en caso la actualización de aplicación o de sistema operativo requiere realizarlo, dicha acción dimensiona posibilitar al usuario de cancelar un reinicio y/o bien forzarlo a realizarlo en determinado momento; toda gestión de parcheo de aplicaciones y sistema operativo, se garantiza independientemente si la solución deja de funcionar en un momento determinado, no se aceptan virtual patching (parches virtuales) o contenedores de CVE, la solución deseada debe ser identificada como gestor de actualizaciones y parcheo para aplicaciones y/o extensible para los sistemas operativos indicados como compatibles. DETECCIÓN Y RESPUESTA AMPLIADA GUION XDR, integra módulo de detección y respuesta ampliada (XDR), dicho complemento de seguridad puede registrar toda actividad realizada en el computador sea realizada por binarios (ejecutables o librerías dinámicas), scripts powershell, cscript , archivo de lotes o similares, permite determinar causa raíz de

un incidente de seguridad así como permita mitigar y responder correctamente al mismo; incorpora capacidades extendidas para mitigar riesgos que no puedan ser identificados con facilidad mediante una solución del tipo NextGen (NGAV) o similares; incorpora sofisticada detección y respuesta que permita identificar comportamientos anómalos en las estaciones de trabajo final y/o servidores de producción; no depende de alguna consola ubicada en la nube o fuera de las instalaciones de la dependencia, toda funcionalidad requerida es del tipo local y permite en cualquier línea del tiempo inspeccionar, monitorizar o evaluar registros auditables recopilados por la herramienta de Detección y Respuesta solicitada; extiende las capacidades de detección para permitir detectar y/o responder ante: detección de las amenazas persistentes, detención de los ataques sin archivos, bloqueo de las amenazas cero (0) day; protección del ransomware; neutralización de los ataques patrocinados por el estado; bloqueo hash SHA guion uno (-1); aislamiento de equipos de red Funcionalmente deberá ser capaz de indicar con precisión cualquier script ejecutado mediante powershell, dicha funcionalidad deberá proporcionar evidencia total de la línea de comandos ejecutada (strings del script y/o código fuente del mismo); proporciona una detección única basada en el comportamiento y en la reputación de archivos, dicha reputación de ficheros debe estar al día y en constante evaluación mediante telemetría global, misma que permite en tiempo real evaluar la reputación del fichero, proceso o script analizado; permite configurar la sensibilidad de las reglas de detección para diferentes grupos de computadoras o usuarios, así como permite eliminar fácilmente las falsas alarmas que pudiese causar alguna regla de detección manual incorporada por el equipo de seguridad de la información; permite combinar criterios como nombre de archivo, ruta, hash, path, línea de comandos y/o firmante de aplicación, con la

finalidad de hacer coincidir disparadores con precisión para las condiciones de activación de las alertas; permite ubicar con facilidad cualquier comportamiento sospechoso inclusive para eventos pasados, mismo que esta representado por cualquier regla de detección nueva agregada; permite al menos históricos de tres meses consecutivos, mismos que pueden ser evaluados dinámicamente ya sea mediante reglas de detección nuevas y/o reputación de ficheros obtenidos por indicadores de amenazas de terceros (IOC's) o mediante telemetría global del fabricante; permite ubicar cualquier indicador de compromiso de forma tal que permita determinar si una amenaza ya existía antes de la emisión de alerta para alguna regla estática configurada; incluye reglas de detección integradas, y permite crear propias reglas para responder a los incidentes detectados; permite bloquear, detener o eliminar cualquier fichero o proceso mediante reglas de acción automatizadas y/o bien mediante intervención manual de algún operador de seguridad a cargo de solución de seguridad XDR, dicha funcionalidad es extendida para ejecutar la misma acción sobre todos los computadores en forma simultánea; permite mayor visibilidad de lo ocurrido en cada computador respecto a ficheros, scripts y/o procesos en general; proporciona visibilidad total de lo ocurrido, siendo capaz de identificar el origen de una afección en particular, misma visibilidad es total y no solo representada en una imagen estática, posibilitando de dicha manera descubrir la naturaleza del origen y causa de afección. SOLUCIÓN DOS FA (2FA) & MFA. La consola/servidor provisiona doble factor de autenticación dos FA (2FA) para su interfaz web de administración; proporciona logs auditables que integran los registros siguientes: provisionamiento de usuarios, intentos fallidos de autenticación, autenticaciones satisfactorias, cambios en los estados del dos FA (2FA) (Ejemplo bloqueo de usuario, desbloqueo, otros), self-enrollment activity,

mensajes OTPs enviados, mensajes de Error, acciones realizadas dentro de la Consola Web, proporciona capacidad de generación de reportes basados en los logs auditables requeridos como indispensables para el correcto funcionamiento y seguridad interna; incluye un paquete de SMS similar o igual a la cantidad total del licenciamiento adquirido (puestos de usuario); permite la compra de paquetes SMS sin afectar la vigencia o expiración del licenciamiento adquirido, ante necesidad de paquetes SMS permite adquirir paquetes/buzones de mensajes de texto para el provisionamiento de usuarios y OTP vía SMS; soporta tanto usuarios nativos de dominio, así como usuarios locales en modalidad standalone; provisiona autenticación RADIUS, dicha solución provisiona y soporta peticiones de autenticación que requieren verificar autenticación para los códigos/contraseñas de un solo uso; ofrece compatibilidad nativa con las redes privadas virtuales (VPN), permitiendo integrar la solución de Doble Factor de Autenticación para el acceso de dichas redes privadas virtuales (VPN); posee compatibilidad de integración a nivel de acceso VPN para los siguientes fabricantes Barracuda, Cisco ASA, Citrix, Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F cinco (F5) FirePass, Fortinet, Juniper, Palo Alto & SonicWall; ofrece de forma nativa integración con Microsoft Remote Desktop Protocol (RDP), garantiza el acceso seguro integrando la misma solución de doble factor de autenticación sin necesidad de instalar cualquier complemento adicional en el equipo donde sea instalada; ofrece integración con Microsoft Desktop Windows Login (Sesión de usuario local), garantiza el acceso seguro integrando la misma solución de doble factor de autenticación sin necesidad de instalar cualquier complemento adicional en el equipo; ofrece compatibilidad para protección del Microsoft Desktop Windows Login (Sesión del usuario local), para al menos los siguientes sistemas operativos:

Windows diez (10), once (11), Windows ocho (8), ocho punto uno (8.1) Windows siete SP uno (7SP1); integra mecanismo de recuperación Master Recovery Key cuando se integre protección para el Microsoft Desktop Windows Login (Sesión del usuario local), ante un fallo de comunicación con el servidor de autenticación central sea posible recuperar el acceso al computador protegido. soporta integración para al menos las siguientes plataformas Microsoft: Remote Desktop (RDP), Remote Desktop Web Access, Remote Web Access, Windows Desktop Login, Outlook Web Access, Exchange Control Panel y Exchange Administrator Centre, Microsoft Dynamics CRM, Microsoft Sharepoint Server Remote Desktop Gateway RADIUS, Microsoft ADFS tres diagonal cuatro (¾), soporta integración con Office trescientos sesenta y cinco (365), Google Cloud y cualquier otro servicio cloud compatible con ADFS tres diagonal cuatro (3/4); soporta compatibilidad RADIUS para integrar mecanismo de doble factor de autenticación mediante Pluggable Authentication Module (PAM) para al menos los siguientes sistemas operativos: Mac OS, Linux, UNIX, Cualquier otro compatible con mecanismo de autenticación PAM; soporta mecanismo de integración para SAML dos punto cero (2.0) mediante Identity Provider (IdP); provisiona servicio web del tipo API REST-based codificada en formato de respuesta JSON; provisona servicio web del tipo API para al menos las siguientes funciones: provisionamiento de usuarios, bloqueo/desbloqueo de usuarios, provisionamiento de mensajes SMS; proporciona mecanismos de lista blanca para facilitar a los administradores exclusiones IP desde las cuales no se requiere el doble factor de autenticación como protección de acceso; proporciona kit SDK de desarrollo que facilita la integración de terceras aplicaciones que por su arquitectura no es posible integrar mediante API o bien mediante cualquiera de los complementos solicitados; todo

token (código dos FA (2FA) deberá poseer al menos seis (6) dígitos, así como deberá permitir que los mismos sean basados en uso o en disponibilidad de tiempo; ofrece flexibilidad para la toma de decisión respecto al método por usuario para la generación del token único de acceso, siendo posible al menos mediante lo siguiente: aplicación instalada en el smartphone (SoftToken Mobile Application), hardware token, mensaje de texto vía sms, correo electrónico y terceras integraciones; ofrece compatibilidad al menos para los siguientes mecanismos de autenticación: mobile application, push authentication FIDO dos (FIDO2) (y FIDO U dos F (FIDOU2F), hard token, sms / terceras integraciones de entrega; en la modalida hard token es compatible con dispositivos hardware del tipo HMAC (HOTP) compatibles con OATH; puede instalarse en dispositivos del tipo Android & IOS; en su modalidad "Mobile Application / SofToken para iOS & Android" ofrece protección mediante PIN así como autenticación biométrica mediante huella dactilar; en su modalidad "Mobile Application / SofToken para iOS & Android" ofrece capacidad de copia del token generado, facilitando la copia/pegado sobre terceras aplicaciones instaladas en el smartphone; en su modalidad "Mobile Application / SofToken para iOS" deberá ofrecer protección biométrica basada en reconocimiento facial. COBERTURA DE LICENCIAMIENTO, posee garantía y cobertura sobre los sistemas operativos indicados como requeridos (endpoints & servidores, incluyendo servidor de administración de la solución), un solo y único lote de licenciamiento involucra a todos los sistemas indicados; ocupa una única clave de activación, llave o similar para todos los productos contratados e indicados como compatiblemente requeridos; puede ser administrado por una única consola de administración, todos los productos adquiridos para los sistemas operativos indicados como compatibles pueden administrarse integralmente desde

una única consola validada e implementada en la red interna corporativa; incluye múltiples capas de seguridad, que operan en forma conjunta y en su defecto tienen capacidad de proteger independientemente si alguna de ellas no detecta en un momento dado el vector de compromiso; garantiza proteger al endpoint final con diferentes métodos de protección y múltiples capas de seguridad comprobables; incluye múltiples capas de seguridad para los diversos componentes ofertados, garantiza en caso para la tecnología de telemetría de datos, cloudsandboxing, protección email y/o protección para Office trescientos sesenta y cinco (365) +GoogleWorkspace según corresponda; la instalación puede realizarse tanto localmente como remotamente desde su consola administrativa; en el término local se entiende se requiere precompilación de un paquete todo-en-uno para la instalación del producto el cual contenga las preconfiguraciones y niveles de seguridad básicos aplicables a la estación de trabajo, así mismo incorpora en un solo paso la unión y sincronización a consola administrativa; incluye medias de instalación originales provistas por el fabricante, evidenciables mediante certificado de originalidad provisto por el fabricante y entregado con las mismas; el fabricante posee oficinas de representación y/o comercialización dentro de territorio nacional, y figura registros de dominios de internet www locales con la finalidad de transparentar contacto y/o referencia de presencia local, y posee números locales de contacto directo con dicho fabricante: el fabricante posee al menos diez (10) centros de Research and Development (R&D) alrededor del mundo, dentro de los cuales al menos uno (1) está dentro de territorio latinoamericano; posee certificación ISO/IEC veintisiete mil uno dos puntos dos mil trece (27001:2013) vigente tanto para su sede central (HQ) así como para la gestión y el desarrollo de los productos; posee certificación ISO nueve mil uno dos

punto dos mil quince (9001:2015) vigente tanto para su sede central (HQ) así como para la gestión y el desarrollo de los productos ; posee al menos treinta (30) años de experiencia en el desarrollo de productos de seguridad y productos relacionados, posee una política de fin de ciclo definida (EOL) visible en su documentación y/o sitios web específicos que permite con total transparencia delimitar productos y versiones que pueden ocuparse dentro del licenciamiento; por el precio unitario de trescientos siete quetzales con noventa y cinco centavos (Q307.95) y precio total de seiscientos quince mil novecientos quetzales (Q615,900.00), el licenciamiento de antivirus, además de las especificaciones descritas, deben cumplir con las indicadas en la oferta de Servicomp.

TERCERA: VALOR DEL CONTRATO Y FORMA DE PAGO: El monto a que asciende la compra de las licencias detalladas, en la cláusula segunda del presente contrato es de **SEISCIENTOS QUINCE MIL NOVECIENTOS QUETZALES (Q615,900.00);** valor que incluye el Impuesto al Valor Agregado (IVA); para los efectos de pago, "Servicomp" 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 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 y/o en la que en el futuro corresponda.

CUARTA: LUGAR, FORMA Y PLAZO DE ENTREGA: "Servicomp" se compromete a entregar a INTECAP el acuerdo de licenciamiento de antivirus que debe ser emitido por el fabricante/propietario del software o casa matriz, identificado con un número único, que describa la relación de la suscripción entre el fabricante/ propietario y el INTECAP, incluyendo el contenido y vigencia de doce (12) meses de la suscripción adquirida, contados a partir de la activación del licenciamiento. El documento que contenga la información de la herramienta, deberá ser entregado en la Bodega General, 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 un (1) día hábil, computados a partir del día siguiente de que el "INTECAP" le notifique por escrito, la aprobación del presente contrato.

QUINTA: SEGUROS DE CAUCIÓN: a) DE CUMPLIMIENTO: "Servicomp" 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 "Servicomp". En caso de incumplimiento del presente contrato por parte de "Servicomp", 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 "Servicomp" ha cumplido con las condiciones del contrato, extendiendo la constancia respectiva para la cancelación; y b) DE CALIDAD Y FUNCIONAMIENTO: "Servicomp" como requisito previo para la recepción de las licencias objeto del presente contrato deberá otorgar un seguro de calidad y funcionamiento por el equivalente al quince por ciento (15%) del valor total del presente contrato, con el cual garantiza la calidad de las licencias, comprometiéndose a reparar las fallas o desperfectos que le sean imputables. Este seguro es por el plazo de dieciocho (18) meses, computados a partir de la recepción de las mismas.

SEXTA: GARANTÍA: "Servicomp" por su parte ofrece una garantía de doce (12) meses para el licenciamiento adjudicado; tiempo durante el cual se compromete a reparar o sustituirlo si fuera necesario, el cual se computa a partir de la activación de los mismos.

SÉPTIMA: SOPORTE TÉCNICO: "Servicomp", garantiza que proveerá de cincuenta (50) horas de soporte técnico por el plazo de un (1) año. El licenciamiento cuenta con soporte del fabricante ESET durante un (1) año, el tipo de soporte es veinticuatro horas al día los siete días de la semana, los trescientos sesenta y cinco días del año, dicho soporte puede ser por medio de correo electrónico o por medio telefónico. Los servicios ofrecidos son: soporte técnico general que incluye asistencia en la instalación y configuración de productos ESET, resolución de problemas técnicos relacionados con el software, actualizaciones y parches de seguridad, consultoría sobre mejores prácticas y optimización del uso de los productos y soporte especializado, que incluye el soporte para la aplicación, asistencia en la integración de productos ESET con otros sistemas y plataformas, capacitación y formación para usuarios y administradores. Los tiempos de

resolución según la categoría de incidentes se clasifican en incidentes críticos, que afecta la operación y requieren atención inmediata, tiempo de respuesta quince minutos de resolución, cuatro horas; incidentes importantes, problemas que afectan a la productividad, pero no detienen la operación, tiempo de respuesta treinta minutos y tiempo de resolución ocho horas; e incidentes menores, problemas que tienen un impatcto limitado en la operación, tiempo de respuesta una hora y tiempo de resolución, veinticuatro horas. De las solicitudes del servicio, se atenderán solicitudes de información, consultas generales sobre el uso de los productos, con tiempo de respuesta de dos horas y tiempo de resolución de cuarenta y ocho horas; y solicitudes de configuración, asistencia en la configuración de productos, con tiempo de respuesta de dos horas y tiempo de resolución de veinticuatro horas. Tipos de escalonamiento de casos, escalonamiento interno, nivel uno, soporte básico proporcionado por técnicos de primera línea; nivel dos, soporte avanzado proporcionado por especialistas en productos de ESET; nivel tres, soporte experto proporcionado por ingenieros con experiencia en resolución de problemas complejos; y escalonamiento externo. El incumplimiento de los compromisos aquí contraídos será motivo para hacer efectivo el seguro de caución de calidad y funcionamiento o para requerirle por la vía correspondiente el cumplimento de estas obligaciones.

OCTAVA: PROHIBICIONES: "Servicomp" 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, **MANGLYO EDGARDO GARCÍA ARENALES,** 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, **MANGLYO EDGARDO GARCÍA ARENALES,** 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 "Servicomp" en la entrega de las licencias 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, "Servicomp" 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: "Servicomp" al disponer de las licencias 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 "Servicomp", 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 veintitrés (23) hojas de papel membretado del "INTECAP".

Ing. Arnaldo Ademar Alvarado Cifuentes
Sub Gerente

Intecap
Subgerencia

Manglyo Edgardo García Arenales
Administrador Único y Representante Legal

SERVICOMP DE GUATEMALA, S. A.
14 Avenida 7-12 Zona 14
Empresarial La Villa Bodega No. 23
Guatemala, Guatemala
PBX: 2326-9191
Ing. Manglyo Edgardo García Arenales
Representante Legal