

CONTRATO NÚMERO GE GUION AL GUION SESENTA Y TRES GUION DOS MIL VEINTIDÓS (GE-AL-63-2022). En la ciudad de Guatemala, el dieciocho de octubre de dos mil veintidós. NOSOTROS: **ARNALDO ADEMAR ALVARADO CIFUENTES**, de cincuenta años de edad, casado, guatemalteco, Ingeniero Industrial, 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 I uno guion treinta y seis (11-36), acreditó 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"; y por la otra parte, **DOUGLAS GAMALIEL SOLARES LARIOS**, de treinta y cuatro años de edad, casado, guatemalteco, Administrador, de este domicilio, con Documento Personal de Identificación (DPI), Código Único de Identificación (CUI) dos mil quinientos cuarenta y tres espacio trece mil seiscientos noventa y ocho espacio cero ciento uno (2543 13698 0101), extendido por el Registro Nacional de las Personas de la República de Guatemala, actúo en mi calidad de Presidente del Consejo de Administración y Representante Legal de la entidad "ELECTRÓNICA COMUNICACIONES Y SERVICIOS, SOCIEDAD ANÓNIMA", inscrita en el Registro Mercantil General de la República de Guatemala al número quince mil ochocientos ochenta y tres (15883), folio ciento trece (113)

*[Handwritten signature]*  
5751457

*[Handwritten signature]*

*[Handwritten signature]*

1565



libro setenta y siete (77) de Sociedades, propietaria de la empresa de nombre comercial "ECSSA", inscrita en el Registro Mercantil General de la República de Guatemala con el número ochenta y seis mil quinientos setenta y cinco (86575), folio doscientos cincuenta (250), libro ochenta y tres (83) de Empresas Mercantiles, calidad que acredito con mi nombramiento contenido en Acta Notarial de fecha treinta de junio del dos mil veintiuno, autorizada en esta ciudad por el Notario Erick Rodrigo Spiegeler Herrera, debidamente inscrito en el Registro Mercantil General de la República de Guatemala, con el número seiscientos treinta mil cuatrocientos noventa y tres (630493), folio quinientos treinta y tres (533), libro setecientos ochenta y uno (781) de Auxiliares de Comercio; señalo como lugar para recibir notificaciones en la tercera (3) avenida diez guion noventa (10-90), zona nueve (9), de esta ciudad. En lo sucesivo será denominado "ECSSA". Ambos comparecientes manifestamos hallarnos en el libre ejercicio de nuestros derechos civiles y que las representaciones que se ejercitan son suficientes conforme a la Ley para la celebración del presente **CONTRATO** 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 veintiocho guion dos mil veintidós (28-2022), cuyo objeto es la contratación del servicio en nube para protección contra ataques en capa de aplicación (Cloud WAF); bajo el Número de Operación Guatecompras diecisiete millones quinientos noventa y dos mil cuatrocientos diez (NOG 17592410); Acta de recepción y apertura de plicas número SC guion ochenta y seis guion dos mil veintidós (SC-86-2022), de fecha veinticuatro de agosto de dos mil

veintidós; Acta de calificación y adjudicación de oferta número SC guion noventa y uno guion dos mil veintidós (SC-91-2022), de fecha treinta de agosto de dos mil veintidós; Cotización contenida en formulario electrónico COT guion dos mil veintidós guion diecisiete millones quinientos noventa y dos mil cuatrocientos diez guion cinco millones ciento cincuenta y un mil cuatrocientos cincuenta y siete (COT-2022-17592410-5151457), código de autenticidad CE cincuenta y seis F ochocientos treinta y uno (CE56F831), de fecha dieciocho de agosto de dos mil veintidós; oferta de "ECSSA", de fecha veinticuatro de agosto de dos mil veintidós; Acuerdo de aprobación de la adjudicación número GE guion seiscientos cincuenta y dos guion dos mil veintidós (GE-652-2022), de fecha diecinueve de septiembre de dos mil veintidós; y Memorando número SS guion noventa y siete guion dos mil veintidós (SS-97-2022), de fecha veintiuno de septiembre de dos mil veintidós. Se tiene por incorporada al presente contrato la documentación anteriormente citada.

**SEGUNDA: OBJETO DEL CONTRATO:** "ECSSA" se compromete ante el "INTECAP" a prestar el servicio en nube para protección contra ataques en capa de aplicación (Cloud WAF), con las siguientes características: el servicio de Cloud WAF cumple con: proteger un total de tres (3) aplicaciones con ancho de banda de treinta Mbps (30 Mbps); está en modelo de despliegue siempre activo; está basado en un WAF con certificación ICSSA Labs; soporta modificaciones programáticas sobre el servicio vía RESTful API; las conexiones tanto de los clientes hacía las aplicaciones, como de las aplicaciones a los clientes, pasan a través del servicio en la nube a contratar; la instalación del servicio será a través de modificación de registros de DNS y sin realizar instalación alguna de hardware o software en algún Data Center. Requerimientos seguridad web: el servicio de cloud WAF genera las políticas de seguridad de cada aplicación aprovisionada de forma automática a través de



algoritmos de machine learning; las aplicaciones aprovisionadas se pueden configurar en modo activo, bloqueando los paquetes de ataques de forma proactiva o en modo monitoreo, simplemente reportando eventos, pero no bloqueándolos. Las políticas de seguridad cumplen con: ser políticas a la medida, ajustadas a cada aplicación aprovisionada; adaptarse a cambios en la aplicación, optimizándose y actualizándose automáticamente, aunque la aplicación aprovisionada se encuentre en modo bloqueo de tráfico; implementar filtros que soporten modelos de seguridad positivos y negativos. El servicio protegerá contra los siguientes ataques: Injections: SQL, OS and LDAP; Cross Site Scripting; Cross Site Request Forgery; Predictable Resource Location; Remote File Inclusions; Brute Force Attacks; Buffer overflow; Information leakage; Improper output Handling; Directory indexing; Access Control (White & Black list, Geolocation, Anonymous proxies); Known Vulnerabilities & Custom Rules; Session Hijacking; Cookie Manipulation & Poisoning; HTTP protocol manipulation; XML and Web Services Attacks; y Anti-scraping. El servicio permite limitar la tasa de tráfico con las siguientes funcionalidades: limitar la tasa de tráfico hacia todo el sitio; limitar la tasa de tráfico hacia un path específico; permitir configurar el tiempo de bloqueo para la IP origen que sobrepase la tasa de tráfico definida. El servicio de Cloud WAF bloquea conexiones que no sean HTTP RFC Compliance; incluye protección contra ataques de tipo cookie poisoning, permitiendo el cifrado de las cookies importantes para garantizar que estas no sean modificadas del lado del cliente y un mecanismo de Fingerprinting que permite identificar de forma única el dispositivo que está ingresando a la aplicación web sin necesidad de conocer su dirección IP; soporta TLS versión uno punto tres (1.3). Requerimientos de protección contra ataques DDoS: el servicio de cloud WAF incluye protección contra ataques DDoS de hasta un Gbps (1 Gbps); la protección

de ataques DDoS protege contra ataques: de capas de red y de aplicación a través de análisis de comportamiento y tipo slow rate; la protección de ataques DDoS incluye tecnología de reto y respuesta a nivel TCP y HTTP. Requerimiento del portal y funcionalidades: el servicio de cloud WAF incluye: un (1) portal desde donde se aprovisionen los certificados digitales, aplicaciones y que incluye dashboards, eventos, analítica, alertas y reportes; cuenta con chequeos de salud por aplicación aprovisionada que sean configurables desde el portal; soporta chequeos de salud TCP y HTTP/HTTPS personalizables por aplicación, permitiendo configurar el hostname, la URL y el código de respuestas esperado; permite configurar desde el portal el nivel de seguridad de TLS, permitiendo seleccionar el protocolo a utilizar y el nivel de seguridad de los ciphers, por cada aplicación aprovisionada; permite configurar desde el portal la forma en la cual se copia la dirección IP real de los clientes, al encabezado HTTP por cada aplicación aprovisionada; permite personalizar el campo del header en el cual se copiará la IP real de los clientes, por cada aplicación aprovisionada; tiene la capacidad, para cada aplicación protegida, de realizar balanceo de carga entre un mínimo de ocho (8) direcciones IP de servidores de origen o Failover (activo-pasivo) de dos (2) direcciones IP de origen; permite la configuración de listas blancas de IP desde el portal de servicios, por cada aplicación aprovisionada; permite la configuración de bloqueo por geografía desde el portal de servicios, por cada aplicación aprovisionada; permite crear excepciones de IP que se encuentren incluidas dentro del bloqueo por geografía; provee una página de bloqueo, la cual es mostrada a usuarios identificados como atacantes que intentan acceder la aplicación; soporta la personalización de la página de bloqueo a través de la redirección a un sitio web específico. El servicio de cloud WAF, a través del portal, permite: crear reglas de control de acceso por IP

a las aplicaciones protegidas; configuración del bloqueo de tráfico proveniente de Anonymous proxies hacia las aplicaciones desde el portal de servicios. El servicio de cloud WAF, a través del portal, y por cada aplicación, permite (considerando encabezados, métodos, IP/CIDR, país de origen y URI): redireccionar el tráfico en base al contenido de éste; creación de reglas manuales de seguridad en base al contenido; creación de reglas para remover o reescribir los encabezados. El portal de servicios permite: visualizar los cambios realizados por los administradores y conservar la información por al menos tres (3) meses; descargar los eventos asociados a los cambios en el servicio en formato CSV; la información de los cambios administrativos incluye modificaciones que realice directamente el fabricante; cargar o subir los certificados digitales asociados a las aplicaciones a proteger; la distribución de la política de seguridad de una aplicación; configurar la opción de distribución de política de forma calendarizada; visualizar los eventos de seguridad de aplicación. La información tienen los logos siguientes: acción tomada por el servicio; dirección IP origen; país origen; aplicación; fecha y hora del evento; severidad; tipo de ataque; clasificación del ataque de acuerdo con el OWASP Top diez (10); entrega el detalle del encabezado del request de HTTP del ataque; refinar el evento (crear una excepción) desde la vista de logs; filtrar los eventos (logs) de seguridad, utilizando: fecha y hora del evento; aplicación; host; dirección IP origen; protección; tipo de violación; categoría OWASP; severidad del evento; URI; parámetro; la descarga de los eventos de seguridad en formato CSV; configurar el envío de alertas que se activen bajo un patrón configurable; visualizar las alertas que han sido enviadas; la configuración de reportes para envío vía correo electrónico; personalizar el dashboard a través de: configurar el tiempo de visualización para todas las vistas o por cada una de ellas y seleccionar las

aplicaciones sobre las cuales se mostrará la información de cada una de las vistas.

El portal de servicios: incluye analítica de seguridad que, agrupando múltiples eventos en actividades recurrente, usando algoritmos de análisis de Big Data; cuenta con un dashboard con las siguientes vistas: tabla resumen de la actividad del WAF; gráfico con el tráfico limpio hacia las aplicaciones en bps, gráfico con las transacciones por segundo por aplicación, gráfico con los eventos de seguridad registrados en las aplicaciones, gráfico de ataques clasificados por el OWASP top diez (10), top de orígenes de ataques en capa de aplicación y top de las aplicaciones atacadas; proporciona un mapa que indica el origen geográfico de los ataques en capa de aplicación Web. El portal soporta doble factor de autenticación y FIM (Federated Identity Management). El portal muestra: respecto al plan adquirido: número de aplicaciones adquiridas / número de aplicaciones aprovisionadas; ancho de banda adquirido / ancho de banda promedio / ancho de banda pico; periodo de suscripción; servicios adicionales contratados; las aplicaciones aprovisionadas y el estado de protección de estas, especificando si la aplicación está brindando protección activa o solo reportando eventos de seguridad; por cada aplicación: la fecha de creación; el Data Center donde se encuentra aprovisionada; el CNAME que se debe usar para realizar el desvío de tráfico. Servicio administrado de seguridad del fabricante: la disponibilidad mínima del servicio es de noventa y nueve punto novecientos noventa y nueve por ciento (99.999%); el servicio de Cloud WAF es un servicio de seguridad administrado por el fabricante con disponibilidad de siete por veinticuatro por trescientos sesenta y cinco (7x24x365). El servicio administrado incluye: monitorear constantemente el estado de salud de las aplicaciones configuradas; proporcionar asistencia durante la fase de onboarding de las aplicaciones; generar alertas proactivas automáticas de seguridad; contar con una

Antecap  
1565

1565



línea para emergencias, con tiempo de respuesta máximo de treinta (30) minutos; contar con los siguientes mecanismos de contacto: portal Web de soporte, soporte vía correo electrónico, soporte telefónico, contar con los siguientes estándares de seguridad y calidad: - PCI-DSS v3.1 (Payment Card Industry Data Security Standard); - ISO/IEC 27001:2013 (Information Security Management Systems); - ISO/IEC 27032:2012 (Security Techniques – Guidelines for Cybersecurity); - ISO 27017:2015 (Information Security for Cloud Services); - ISO 27018:2014 (Information Security Protection of Personally identifiable information (PII) in public clouds); - ISO 28000:2007 (Specification for Security Management Systems for the Supply Chain); US SSAE16 SOC-1 Type II, SOC-2 Type II. El servicio de nube para protección contra ataques en capa de aplicación (Cloud WAF), además de las especificaciones descritas, deben cumplir con las indicadas en la oferta de "ECSSA".

**TERCERA: VALOR DEL CONTRATO Y FORMA DE PAGO:** El monto a que asciende el servicio de nube para protección contra ataques en capa de aplicación (Cloud WAF), descrito en la cláusula segunda del presente contrato es de **CIENTO NOVENTA Y NUEVE MIL OCHENTA QUETZALES (Q199,080.00)**, valor que incluye el Impuesto al Valor Agregado (IVA); para los efectos de pago, "ECSSA" 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 el servicio ha sido recibido de conformidad por el "INTECAP". Dicho pago se hará con cargo a la partida presupuestaria número dos mil veintidós guion once millones doscientos mil treinta y cuatro guion cero cero cero guion cero cero guion once guion cero cero guion cero cero guion cero cero uno guion cero cero cero guion cero ciento uno guion



ciento cincuenta y ocho (2022-11200034-000-00-11-00-000-001-000-0101-158) de Administración Institucional, Informática, y/o en la que en el futuro corresponda.

**CUARTA: LUGAR, FORMA, PLAZO DE ENTREGA Y VIGENCIA:** "ECSSA" se compromete a entregar, instalar, configurar y dejar funcionando al cien por ciento (100%), el servicio en nube para protección contra ataques en capa de aplicación (Cloud WAF), descrito en la cláusula segunda de este contrato, en el Departamento de Informática, ubicado en Calle Doroteo Guamuch Flores siete guión cincuenta y uno (7-51), zona cinco (5), séptimo (7mo.) nivel, de esta ciudad; "ECSSA" debe entregar el usuario y credenciales de la consola web de administración del software, así como demostrar en la consola de administración que está activo; en un plazo de diez (10) días hábiles, computados a partir del día siguiente de que el INTECAP le notifique por escrito la aprobación del contrato. La vigencia del servicio será de doce (12) meses, contados a partir de la activación del mismo; plazo que podrá ser prorrogado, a solicitud del INTECAP y con la aceptación tácita o expresa del contratista.

**QUINTA: SEGURO DE CAUCIÓN: DE CUMPLIMIENTO:** "ECSSA" 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 "ECSSA". En caso de incumplimiento del presente contrato por parte de "ECSSA", 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 "ECSSA" ha cumplido con las condiciones del contrato, extendiendo la constancia respectiva para la cancelación.

**SEXTA: SUMINISTRO DE MANTENIMIENTO Y SOPORTE TÉCNICO: "ECSSA",** garantiza: a) Que tiene soporte técnico, como también la capacidad de cubrir las necesidades de mantenimiento, con personal técnico calificado y que este puede prestarlo localmente de forma presencial y a distancia (chat en línea, correo electrónico y/o vía telefónica mediante número local); y b) Que tiene la capacidad de cubrir las necesidades de mantenimiento con personal técnico calificado, en un plazo de cinco (5) días, computados a partir del momento en que se le notifique el incidente, por parte del INTECAP.

**SÉPTIMA: PROHIBICIONES:** "ECSSA" 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.

**OCTAVA: DECLARACIÓN JURADA:** Yo, **DOUGLAS GAMALIEL SOLARES LARIOS**, 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 soy deudor moroso del Estado ni de las entidades a que se refiere el artículo uno (1) de la referida Ley.

**NOVENA: CLÁUSULA RELATIVA AL COHECHO:** Yo, **DOUGLAS GAMALIEL SOLARES LARIOS**, 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: 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 PRIMERA: TERMINACIÓN DEL CONTRATO:** El presente contrato se dará por terminado cuando ocurran cualesquiera de las circunstancias siguientes:  
a) Por incumplimiento de las obligaciones contractuales; b) Por vencimiento del plazo siempre que no se haya acordado prórroga alguna; c) Por rescisión unilateral del INTECAP, al determinarse atraso en la entrega del servicio; con base a la fecha establecida y fijada en la cláusula cuarta del 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; y d) Por casos fortuitos o de fuerza mayor que hagan innecesario el contrato o que afecten su cumplimiento.

**DÉCIMA SEGUNDA: 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 TERCERA: SANCIONES:** a) Retraso en la entrega: El retraso de "ECSSA" en la prestación del servicio, 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, "ECSSA" 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 CUARTA: RECEPCIÓN Y LIQUIDACIÓN:** "ECSSA" al disponer del servicio y estar listo para la entrega del mismo, deberá hacerlo del conocimiento de la Gerencia del "INTECAP", por escrito, quien nombrará la comisión receptora para que proceda a la recepción del mismo, de conformidad con el contrato, oferta y Ley; la liquidación deberá practicarse dentro de los noventa (90) días siguientes a la fecha de finalización del servicio.

**DÉCIMA QUINTA: 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 SEXTA: 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 siete (7) hojas de papel membretado del "INTECAP".




Dr. Arnaldo-Ademar Alvarado Cifuentes  
Sub Gerente -



**Subgerencia**



Douglas Gamaliel Solares Larios  
Presidente del Consejo  
de Administración y  
Representante Legal



EMPRESA DE TELECOMUNICACIONES DE GUATEMALA S.A.  
ELECTRÓNICA, COMUNICACIONES Y SERVICIOS, S.A.  
3ra. AV. 10-90, ZONA 9  
TELÉFONO: 2 379 91000