SERVICIO DE PROTECCIÓN EN LA NUBE CONTRA ATAQUES EN CAPA DE APLICACIÓN WEB PARA PORTAL WEB

Órgano	:	Gerencia de Operaciones
Fecha	:	Tacna, 15 de julio de 2026
Actividad del POI	:	
Forma parte del SGC	:	NO
N° de Producto SCI:	:	

I. FINALIDAD PUBLICA (Obligatorio)

La presente contratación tiene como finalidad pública fortalecer la seguridad, disponibilidad, integridad, confidencialidad y continuidad operativa de los portales web institucionales de ZOFRATACNA, alojados bajo los dominios zofratacna.com.pe y zofratacna.pe, mediante la implementación de una solución integral de ciberseguridad que comprende protección perimetral web en la nube (WAF/CDN), monitoreo centralizado de eventos de seguridad mediante una plataforma SIEM/XDR y la ejecución de pruebas de penetración web (ethical hacking).

Con ello se busca reducir los riesgos de ataques informáticos, accesos no autorizados, alteración o exfiltración de información, indisponibilidad del servicio y exposición de datos personales, garantizando la prestación segura y continua de los servicios digitales institucionales dirigidos a la ciudadanía, usuarios, operadores de comercio exterior y público en general.

II. OBJETO DEL SERVICIO (Obligatorio)

Objetivo General:

Contratar el servicio integral de ciberseguridad para la protección de los portales web institucionales de ZOFRATACNA (zofratacna.com.pe y zofratacna.pe), mediante la implementación, configuración y puesta en operación de una solución de protección perimetral web en la nube, una plataforma de monitoreo SIEM/XDR y la ejecución de pruebas de penetración web, con la finalidad de fortalecer la disponibilidad, confidencialidad, integridad, el monitoreo continuo y la capacidad de respuesta frente a amenazas cibernéticas.

Objetivos Específicos:

- Implementar y configurar una solución de protección perimetral web en la nube (WAF + CDN + DNS) que filtre el tráfico malicioso dirigido a los dominios institucionales antes de que alcance el servidor de origen.
- Desplegar y configurar una plataforma SIEM/XDR para la recolección, correlación, análisis y alertamiento centralizado de eventos de seguridad de los activos asociados al portal web.
- Ejecutar pruebas de penetración web (pentesting) sobre los portales institucionales para identificar, clasificar y reportar vulnerabilidades, con recomendaciones de remediación priorizadas por criticidad.
- Proveer soporte técnico, mantenimiento preventivo y correctivo, ajuste de reglas de seguridad y acompañamiento técnico durante **12 MESES** contado desde la conformidad de la puesta en operación.

- Transferir conocimiento al personal de ATIC-ZOFRATACNA mediante documentación técnica, capacitación funcional.

III. ALCANCES Y DESCRIPCIÓN DEL SERVICIO (Obligatorio)

PRESTACION PRINCIPAL

Condiciones generales de ejecución

- El contratista deberá coordinar previamente con ATIC el cronograma de migración y los cambios de DNS, minimizando la indisponibilidad de los portales.
- Las credenciales administrativas de todas las plataformas implementadas serán entregadas y serán de titularidad de ZOFRATACNA. Es decir, brindará acceso a la plataforma(s) de gestión de las soluciones solicitadas.
- El contratista garantizará la confidencialidad de la información a la que tenga acceso durante toda la prestación y luego de su culminación.
- Toda la documentación técnica (arquitectura, configuraciones, manuales de operación y procedimientos) será entregada a la Entidad.
- Toda la información generada por los servicios contratados será entregada a la entidad al culminar el servicio

El servicio consiste en la implementación de una solución integral de ciberseguridad para los portales web institucionales de ZOFRATACNA (zofratacna.com.pe y zofratacna.pe), incluye un SLA mínimo, la solución estará estructurada en tres (03) componentes funcionales:

(A) Protección Perimetral Web en la Nube;

(B) Monitoreo SIEM/XDR en la Nube; y

(C) Pruebas de Penetración Web.

El servicio incluye, además, soporte técnico, mantenimiento preventivo y correctivo, monitoreo, ajuste de configuraciones, actualización de reglas de seguridad y acompañamiento técnico por el periodo de un (01) año, contado a partir de la conformidad de la implementación o puesta en operación.

SLA (Acuerdo de Nivel de Servicio, o *Service Level Agreement*), define exactamente qué servicio se entregará, el nivel de calidad esperado:

- **Disponibilidad del Servicio (Uptime):** mínimo 99.99% de disponibilidad de la plataforma WAAP.
- **Soporte Técnico (SLA de Respuesta):**
  - Severidad 1 (Crítica - Ataque activo o caída del servicio): Respuesta en < 15 minutos; resolución o mitigación inicial en <30 minutos.
  - Severidad 2 (Alta - Falso positivo bloqueando una API crucial): Respuesta en < 30 minutos; resolución en < 45 minutos.
  - Severidad 3 (Baja - Cambios de configuración o consultas): Respuesta en < 01 hora.

COMPONENTE A — PROTECCIÓN PERIMETRAL WEB EN LA NUBE (WAF / CDN / DNS)

A.1 Gestión DNS

- Administración de la zona DNS de los dominios institucionales zofratacna.com.pe y zofratacna.pe.
- Configuración de registros A, AAAA, CNAME, TXT, MX y demás registros requeridos.
- Validación de la propagación DNS y gestión segura de los cambios durante la migración.
- Soporte para registros de autenticación de correo: SPF, DKIM y DMARC, cuando aplique.

A.2 Red de Distribución de Contenido (CDN)

- Entrega acelerada de contenido web estático y caché de archivos CSS, JavaScript, imágenes y recursos públicos.
- Configuración de reglas de caché por rutas, con exclusión de rutas sensibles, paneles administrativos, formularios y endpoints dinámicos.
- Optimización del rendimiento del portal, compresión de tráfico y reducción de carga sobre el servidor de origen.

A.3 Firewall de Aplicaciones Web (WAF)

- Reglas administradas de seguridad basadas en el OWASP Core Rule Set (CRS).
- Protección frente a inyección SQL (SQLi), Cross-Site Scripting (XSS), inclusión de archivos local/remota (LFI/RFI) y explotación de vulnerabilidades conocidas.
- Protección frente a escaneo automatizado y herramientas de explotación.
- Reglas personalizadas por ruta, IP, país, método HTTP o patrón de tráfico.
- Modos de operación configurables: monitoreo (log), desafío (challenge) o bloqueo, según la criticidad.

A.4 Protección contra bots y tráfico automatizado

- Identificación y desafío/bloqueo de tráfico automatizado y bots maliciosos.
- Protección contra scraping abusivo, abuso de formularios y crawlers no autorizados.
- Limitación de solicitudes repetitivas desde una misma IP o rango.

A.5 Control de tasa de solicitudes (Rate Limiting)

- Limitación de solicitudes excesivas hacia rutas críticas: formularios públicos, rutas de autenticación, APIs expuestas, buscadores internos, endpoints sensibles y paneles administrativos.

A.6 Seguridad SSL/TLS y endurecimiento (hardening)

- Activación de tráfico HTTPS y redirección de HTTP a HTTPS, validación de certificado digital y configuración segura del modo SSL/TLS (full/strict).
- Revisión de contenido mixto, versión mínima TLS recomendada (TLS 1.2/1.3) y activación de HSTS previa validación técnica.

- Revisión y configuración de cabeceras de seguridad (HSTS, X-Content-Type-Options, X-Frame-Options, Content-Security-Policy, Referrer-Policy).
- Bloqueo de métodos HTTP innecesarios, restricción y protección de rutas administrativas y sensibles.
- Bloqueo o desafío por reputación de IP, reglas de geolocalización (previa autorización de la Entidad), reglas contra User-Agent maliciosos y ocultamiento del servidor de origen.

COMPONENTE B — MONITOREO SIEM / XDR EN LA NUBE

La plataforma SIEM/XDR será desplegada sobre un VPS (Virtual Private Server) o infraestructura equivalente provista y gestionada por el contratista, e integrará como mínimo las siguientes capacidades:

El contratista es responsable de dimensionar correctamente el VPS según la oferta técnica realizada, garantizando correctamente el almacenamiento y correlación de eventos.

B.1 Centralización de logs

- Recolección de logs del sistema operativo, del servidor web, de autenticación, de accesos remotos y del firewall local. capacidad de almacenamiento de mínimo 90 dias para preservación historico
- Recepción de logs mediante agentes y/o Syslog, e integración con los logs de la solución de protección perimetral cuando el mecanismo contratado lo permita, capacidad de almacenamiento de mínimo 90 días para preservación histórico.
- Entrega de Respaldo/exportación de logs mensualmente (cada 30 días) para preservación de estos por parte de la entidad.

B.2 Correlación y análisis de eventos

- Aplicación de reglas de correlación y clasificación de eventos por criticidad.
- Detección de patrones sospechosos, múltiples intentos fallidos de acceso, ataques de fuerza bruta y accesos anómalos.
- Detección de cambios no autorizados e identificación de posibles indicadores de compromiso (IoC).

B.3 Monitoreo de integridad de archivos (FIM)

- Supervisión de archivos críticos del sistema y de los directorios del portal web.
- Detección de creación, modificación o eliminación de archivos y alertas por cambios en configuraciones sensibles, archivos de autenticación y de aplicación.

B.4 Gestión de vulnerabilidades

- Inventario del sistema operativo y de los paquetes instalados, identificación de software vulnerable y detección de CVE asociados a los activos monitoreados.
- Clasificación de vulnerabilidades por criticidad y reporte con recomendaciones de remediación.

B.5 Inventario de activos

- Registro de agentes conectados, estado de conexión, sistema operativo, dirección IP, información básica de hardware/software, paquetes instalados y última conexión del agente.

B.6 Alertamiento

- Alertas por eventos críticos, desconexión de agentes, accesos sospechosos, cambios en archivos críticos, vulnerabilidades críticas y eventos de seguridad web.
- Notificación por correo electrónico, webhook u otro mecanismo acordado con la Entidad.

B.7 Tableros de visualización (Dashboards)

- Paneles, como mínimo, para: estado general de seguridad; agentes conectados/desconectados; eventos por severidad y por origen; eventos de autenticación; eventos del servidor web; cambios en archivos críticos; vulnerabilidades detectadas; eventos de protección perimetral (cuando aplique); y tendencias de alertas.

COMPONENTE C — PRUEBAS DE PENETRACIÓN WEB (PENTESTING)

El contratista ejecutará pruebas de penetración web sobre los portales institucionales bajo una metodología reconocida (OWASP Web Security Testing Guide – WSTG, OWASP Top 10, PTES y/o NIST SP 800-115), en modalidad de caja gris (gray-box) salvo indicación distinta de la Entidad, evaluando como mínimo las siguientes categorías de vulnerabilidades:

- Broken Access Control (control de acceso roto).
- Cryptographic Failures / Sensitive Data Exposure (exposición de datos sensibles).
- Injection (incluye SQLi, XSS, command injection).
- Insecure Design (diseño inseguro).
- Security Misconfiguration (configuración insegura).
- Vulnerable and Outdated Components (componentes vulnerables y desactualizados).
- Identification and Authentication Failures (fallas de identificación y autenticación).
- Software and Data Integrity Failures (fallas de integridad de software y datos).
- Security Logging and Monitoring Failures (fallas de registro y monitoreo).
- Server-Side Request Forgery (SSRF).
- Exposición de directorios o archivos sensibles; cabeceras de seguridad ausentes; configuración débil de cookies; métodos HTTP inseguros; versiones de software expuestas; y errores de configuración del servidor web.
- incluye el front-end público y también los paneles administrativos (Internet Information Server), el alcance incluye APIs REST/SOAP expuestas.
- Las pruebas se ejecutarán en ventanas horarias coordinadas y autorizadas formalmente por la Entidad, sin afectar la disponibilidad de los servicios en producción, y bajo estricta confidencialidad.

- El contratista entregará un informe técnico (Entregable 2) con el detalle de hallazgos, evidencias, nivel de criticidad (escala CVSS v3.1) y plan de remediación recomendado, así como realizar un re-test de verificación de las vulnerabilidades críticas y altas subsanadas, actividad que se coordinara con la entidad para su realización posterior a la implementación de las recomendaciones y se incluirá como parte de las actividades de soporte mensual que el contratista debe brindar, para luego de su realización informar el resultado del mismo como anexo al informe mensual del servicio(entregables del 4 al 15) en el mes que se haya efectuado.

III. REGLAMENTOS TECNICOS, NORMAS METROLOGICAS Y/O SANITARIAS (De corresponder)

Resultan aplicables, en lo pertinente, las siguientes normas técnicas y disposiciones:

- NTP-ISO/IEC 27001:2014 – Sistema de Gestión de Seguridad de la Información (SGSI).
- ISO/IEC 27002 – Controles de seguridad de la información.
- Decreto Legislativo N° 1412 – Ley de Gobierno Digital, y su Reglamento (D.S. N° 029-2021-PCM).
- Decreto de Urgencia N° 007-2020 – Marco de Confianza Digital.
- Ley N° 29733 – Ley de Protección de Datos Personales y su Reglamento.
- Lineamientos del marco de ciberseguridad (NIST CSF) y guías OWASP (Top 10, WSTG).
- Disposiciones de seguridad digital emitidas por la Secretaría de Gobierno y Transformación Digital (SGTD-PCM) y el equipo de respuesta ante incidentes (PECERT).

En todo lo no previsto, se aplicará la buena práctica internacional de la industria y la normativa peruana vigente en materia de seguridad digital.

IV. SEGUROS (De corresponder)

NO APLICA

V. PRESTACIONES ACCESORIAS (De corresponder)

El servicio incluye, como prestaciones accesorias durante el periodo contratado lo siguiente:

- Soporte técnico 24x7 y mantenimiento preventivo y correctivo de las plataformas implementadas.
- Monitoreo 24x7 , ajuste de configuraciones y actualización de reglas de seguridad del WAF y del SIEM/XDR ante nuevas amenazas.
- Acompañamiento técnico y atención de incidentes de seguridad relacionados con los portales institucionales, con tiempos de respuesta definidos en el plan de trabajo. mediante mesa de ayuda con correo/número telefónico para registro de incidentes
- Capacitación funcional y transferencia de conocimiento al personal de la Oficina de TIC (ATIC).
- Actualización de reglas administradas y ajuste por falsos positivos/falsos negativos.
- Monitoreo funcional de eventos, disponibilidad de consola y alertamiento configurado.

- Entrega de reportes mensuales de servicio, bitácora de cambios y recomendaciones de mejora.
- Se mantendrá las condiciones generales del servicio principal.
- Al finalizar el periodo del servicio, el contratista deberá entregar a la entidad, junto con su informe final (Entregable 15), toda la documentación correspondiente a las configuraciones, reglas y políticas implementadas en el WAF, en un formato exportable y portable.

VI REQUISITOS DEL PROVEEDOR Y/O PERSONAL (De corresponder)

Del proveedor (persona natural con negocio o persona jurídica):

- Suscribir Declaración Jurada de CONTRATOS MENORES según modelo que alcance el área de Logística.
- Contar con RUC activo y habido.
- Contar con RNP, de corresponder.
- suscribir la autorización de pago.
- Suscribir la declaración Jurada sobre prohibiciones e incompatibilidades.
- Suscribir la Declaración Jurada para prevenir casos de nepotismo.
- Acreditar experiencia en, al menos, cuatro (04) servicios similares a la solución solicitada (servicios de ciberseguridad, protección web/WAF, SIEM/SOC y/o pruebas de penetración).

Acreditación de la experiencia:

La experiencia del postor se acreditará con: (i) contratos u órdenes de compra/servicio y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente mediante constancia de depósito, nota de abono, reporte de estado de cuenta u otro documento emitido por una entidad del sistema financiero, o mediante la cancelación consignada en el propio comprobante de pago.

Del personal clave:

El equipo de trabajo deberá de estar conformado como mínimo por 04 especialistas con los siguientes roles:

- 01Jefe proyecto
- 01 especialista Componente A
- 01 especialista Componente B
- 01 especialista Componente C

Solo el JEFE DEL PROYECTO podrá desempeñar también el rol de especialista en alguno de los 03 componentes, el resto de los componentes deberá de contar con 01 especialista a dedicación exclusiva para cada uno de ellos.

Profesional Líder / Jefe de Proyecto: (01 ESPECIALISTA MINIMO)

- Ingeniero Electrónico y/o de Telecomunicaciones (o de Sistemas/afín) titulado, colegiado y habilitado.

- Experiencia mínima de DOS (02) años en el rubro de ciberseguridad o infraestructura tecnológica.
- Deberá contar con certificación oficial vigente en alguna marca de firewall ubicada como líder en el Cuadrante Mágico de Gartner para Hybrid Mesh Firewall.
- Deberá contar con certificación oficial de nivel experto en alguna marca líder del Cuadrante Mágico de Gartner para tecnologías SASE (Secure Access Service Edge).

Profesional especialista COMPONENTE A (01 ESPECIALISTA MINIMO) y B (01 ESPECIALISTA MINIMO):

- Ingeniero Electrónico y/o de Telecomunicaciones (o de Sistemas/afín) titulado, colegiado y habilitado
- Experiencia mínima de DOS (02) años en el rubro de ciberseguridad o infraestructura tecnológica.
- Deberá contar con certificación oficial vigente en alguna marca de firewall ubicada como líder en el Cuadrante Mágico de Gartner para Hybrid Mesh Firewall.
- Deberá contar con certificación oficial de nivel experto en alguna marca líder del Cuadrante Mágico de Gartner para tecnologías SASE (Secure Access Service Edge).

Profesional especialista COMPONENTE C (01 ESPECIALISTA MINIMO):

- Ingeniero Electrónico y/o de Telecomunicaciones (o de Sistemas/afín) titulado, colegiado y habilitado, con experiencia mínima de DOS (02) años en el rubro de ciberseguridad o infraestructura tecnológica.
- Especialista en pruebas de penetración (deseable): profesional con certificación reconocida en hacking ético / pentesting (p. ej. OSCP, CEH, eWPT o equivalente), que sustente la ejecución del Componente C.

La acreditación de los requisitos del personal clave se realizará mediante copia de títulos, constancia de habilitación del colegio profesional correspondiente, certificaciones vigentes y documentación que sustente la experiencia.

VII LUGAR Y PLAZO DE EJECUCIÓN (Obligatorio)

Lugar: El servicio se prestará principalmente de forma remota sobre la infraestructura web institucional de ZOFRATACNA y los dominios zofratacna.com.pe y zofratacna.pe. Las coordinaciones técnicas, reuniones y conformidades se realizarán con el Área de Tecnologías de la Información y Comunicaciones - ATIC, en la sede institucional de ZOFRATACNA, Panamericana Sur Km 1308, Tacna, o por medios virtuales autorizados.

Plazo: El plazo total del servicio será de un (01) año o doce (12) meses o trescientos sesenta y cinco (365) días calendario, contados desde el día de la activación del servicio, la cual no deberá de excederse de los quince días calendario para la implementación y activación/puesta en operación del servicio, salvo causa justificada no atribuible al contratista y aceptada por la Entidad.

VIII ENTREGABLES (Obligatorio)

Entregable	Contenido	Plazo de entrega
Entregable N° 1 Implementación y puesta en operación	Informe de implementación que acredite: configuración de DNS/CDN/WAF para zofratacna.com.pe y zofratacna.pe; despliegue y configuración de la plataforma SIEM/XDR; arquitectura de la solución; pruebas de funcionamiento; entrega de credenciales administrativas.; y correo electrónico/número telefónico de su mesa de ayuda, matriz de configuración final.	Hasta treinta (30) días calendario desde la notificación de la orden de servicio / suscripción del contrato.
Entregable N° 2 Pruebas de penetración web	Informe de pentesting con metodología empleada, alcance, hallazgos, evidencias, criticidad (CVSS v3.1), plan de remediación priorizado y re-test de verificación de hallazgos críticos y altos.	Hasta treinta y cinco (35) días calendario desde la notificación de la orden de servicio.
Entregable N° 3 Transferencia de conocimiento	Manual operativo, grabación o material de capacitación, lista de participantes, matriz de configuración final y procedimiento de atención/escalamiento.	Hasta treinta y cinco (35) días calendario desde la notificación de la orden de servicio.
Entregables N° 4 al N° 15 Operación, soporte y monitoreo	Informes mensuales de operación, SLA, monitoreo de eventos SIEM/XDR, ajustes de reglas WAF, mantenimientos realizados, incidentes atendidos y recomendaciones de mejora.	Mensual (los 05 primeros días del mes vencido), durante los doce (12) meses del servicio. (requisito indispensable para el pago del servicio)

Los entregables deberán presentarse en formato digital editable y/o PDF, con evidencias técnicas suficientes. La Entidad podrá solicitar sustento adicional razonable cuando el entregable no acredite la prestación.

La aprobación o validación deberá de ser realizada por el Área de Tecnologías de la Información y Comunicaciones mediante acta, luego de haberse recibido cada entregable del contratista.

IX SUPERVISION Y CONFORMIDAD DEL SERVICIO (Obligatorio)

La supervisión técnica estará a cargo de la Sección de Soporte Técnico del Área de Tecnologías de la Información y Comunicaciones y la conformidad del servicio estará a cargo del Área de Tecnologías de la Información y Comunicaciones – ATIC con el visto bueno de la Sección de Soporte Técnico, previa verificación del cumplimiento de los entregables, activación del servicio, evidencias técnicas, niveles de servicio y funcionamiento de los dominios protegidos.

De existir observaciones la entidad las comunica al contratista indicando claramente el sentido de estas, otorgándole un plazo para subsanar. El plazo de subsanación no debe ser mayor del 30% del plazo del entregable correspondiente. Si pese al plazo otorgado, el contratista no cumpliese a cabalidad con la subsanación, la entidad puede otorgar plazos adicionales o resolver el contrato. En

caso de otorgarse plazo adicional corresponde aplicar la penalidad por mora desde el vencimiento del plazo inicial para subsanar, sin considerar los días en los que pudiera incurrir la entidad contratante para efectuar las revisiones y notificar las observaciones correspondientes.

X FORMA Y CONDICIONES DE PAGO (Obligatorio)

El pago se efectuará mediante abono en cuenta bancaria o cheque de gerencia, para cuyo efecto el contratista comunicará el medio elegido, mediante una Carta de Autorización según el modelo que remitirá el Área de Logística.

El pago será realizado en 12 armadas mensuales, según la conformidad del servicio debidamente suscrita por el Área de tecnologías de la información y comunicaciones de la Gerencia de Operaciones.

XI CONFIDENCIALIDAD (De corresponder)

El contratista firmará un Acta de Confidencialidad para la reserva absoluta en el manejo de información a la que tenga acceso y que se encuentre relacionada con la prestación, quedando prohibido revelar dicha información a terceros sin autorización expresa de la Entidad.

Esta obligación comprende credenciales, configuraciones, dominios, IP, arquitectura, logs, eventos de seguridad, vulnerabilidades, incidentes, certificados, tokens, reportes, datos personales y cualquier información institucional obtenida durante la ejecución.

XII RESPONSABILIDAD DEL CONTRATISTA

El contratista es responsable por la calidad del servicio ofrecido, la correcta configuración de la solución, la confidencialidad de la información, la atención de incidentes atribuibles, la oportunidad de soporte, la entrega de evidencias y la subsanación de observaciones por un plazo no menor de un (01) año contado desde la conformidad final otorgada por la Entidad, sin perjuicio de responsabilidades por vicios ocultos o incumplimientos detectados posteriormente conforme a la normativa aplicable.

XIII RESPONSABILIDAD POR LA ASIGNACION DE BIENES

En caso la Entidad asigne al contratista bienes, credenciales, cuentas, certificados digitales, tokens, accesos temporales, documentación técnica u otros recursos para la ejecución del servicio, el contratista será responsable de su uso, custodia, conservación, confidencialidad y devolución o eliminación segura al cierre del servicio. Queda prohibido reutilizar, transferir, compartir o almacenar credenciales fuera de los mecanismos autorizados por la Entidad.

XIV. PENALIDADES (Obligatorio)

Penalidad por Mora en la ejecución de la prestación:

En caso de retraso injustificado del contratista en la ejecución de las prestaciones, objeto del contrato, LA ENTIDAD le aplica automáticamente una penalidad por mora por cada día de atraso, de acuerdo con la

siguiente fórmula:

$$\text{Penalidad Diaria} = \frac{0.10 \times \text{monto}}{F \times \text{plazo}}$$

Donde:

F = 0.40

- Tanto el monto como el plazo se refieren, según corresponda, a la ejecución total o a la obligación parcial, de ser el caso, que fuera materia de retraso.
- Se considera justificado, el retraso cuando el contratista acredite de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable.
- Esta calificación del retraso como justificado no da lugar al pago de gastos generales de ningún tipo.
- Las penalidades se deducen de los pagos a cuenta, pagos parciales o del pago final, según corresponda.
- Cuando se llegue a cubrir el monto máximo de la aplicación de la penalidad por mora y otras penalidades, de ser el caso, LA ENTIDAD puede resolver el contrato por incumplimiento.
- El monto máximo a aplicar es del diez por ciento (10%) del contrato vigente.

XV. OTRAS PENALIDADES

Se establecen las siguientes penalidades objetivas, razonables y proporcionales al objeto del servicio, sin perjuicio de la penalidad por mora, resolución contractual o acciones legales que correspondan:

Supuesto de aplicación	Forma de cálculo	Procedimiento de verificación
Incumplimiento injustificado del SLA de respuesta para incidente crítico atribuible al contratista.	0.5% del monto mensual del servicio por evento verificado.	Ticket, correo, acta o bitácora con hora de reporte, atención y cierre.
Disponibilidad mensual del servicio SaaS WAF menor a 99.9% por causa atribuible al contratista/proveedor.	1% del monto mensual por periodo mensual incumplido.	Reporte de disponibilidad de plataforma y validación técnica de la Entidad.
Cambio crítico no autorizado en DNS, certificados, reglas de bloqueo, listas permitidas/denegadas o configuración que afecte el servicio.	1% del monto mensual por evento, sin perjuicio de reversión inmediata.	Bitácora de cambios, evidencia DNS, consola, correo o acta técnica.
No entrega de informe mensual dentro del plazo, sin justificación aceptada.	0.5% del monto mensual por cada día calendario de atraso.	Fecha de vencimiento, cargo de recepción y registro del área usuaria.
Incumplimiento de confidencialidad, exposición de credenciales o uso no autorizado de información institucional.	Resolución contractual y acciones legales; adicionalmente 5% del monto contractual si el hecho es verificable y atribuible.	Informe técnico, auditoría, evidencia de acceso, notificación de incidente o acta institucional.

XVI RESOLUCION CONTRACTUAL

Se puede resolver el contrato u orden de servicio, en los siguientes casos:

a) Por acumulación del monto máximo de la penalidad por mora o por el monto máximo para otras penalidades, en la ejecución de la prestación a su cargo.

b) Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.

c) Incumplimiento de obligaciones contractuales, por causa atribuible al contratista.

d) Hecho sobreviniente al perfeccionamiento del contrato, de supuesto distinto al caso fortuito o fuerza mayor, no imputable a ninguna de las partes, que imposibilite la continuación del contrato.

e) Por incumplimiento de la cláusula anticorrupción y antisoborno.

f) Por la presentación de documentación falsa o inexacta durante la ejecución contractual.

g) Por la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley N° 31564, Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público.

De encontrarse en alguno de los supuestos de resolución del contrato, LAS PARTES proceden de acuerdo a lo establecido en el artículo 122 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

XVII CLÁUSULA ANTICORRUPCION Y ANTISOBORNO

EL CONTRATISTA declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de la entidad contratante.

Asimismo, EL CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente.

Aunado a ello, EL CONTRATISTA se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

Adicionalmente, EL CONTRATISTA se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con LA ENTIDAD.

Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier

persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA ENTIDAD el derecho de resolver total o parcialmente el contrato. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

XVIII. SOLUCION DE CONTROVERSIAS

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación, conforme a lo establecido en Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas.

FIRMA Y SELLO DEL JEFE DEL ÁREA USUARIA

FIRMA DIGITAL

Firmado digitalmente por: ROJAS MORALES Ivan Cesar FAU 20147797011 hard
Motivo: Soy el autor del documento
Fecha: 15/07/2026 16:57:58-0500