TÉRMINOS DE REFERENCIA

Órgano y/o Unidad Orgánica:	Oficina de Tecnologías de la Información
Actividad del POI/Acción Estratégica PEI:	Brindar un óptimo acceso a los servicios TIC
Denominación de la Contratación:	Servicio de Hackeo Ético

I. FINALIDAD PÚBLICA

La contratación del servicio de Ethical Hacking para los aplicativos informáticos del Fondo Intangible Solidario de Salud (FISSAL) tiene como finalidad identificar, evaluar y mitigar vulnerabilidades de seguridad presentes en los sistemas y aplicaciones institucionales que soportan los procesos operativos del FISSAL, a fin de prevenir accesos no autorizados, alteraciones de la información o interrupciones en la disponibilidad de los servicios.

II. OBJETIVO DE LA CONTRATACIÓN

Evaluar el nivel de seguridad de los aplicativos informáticos del FISSAL expuestos a internet mediante técnicas de Ethical Hacking, identificando vulnerabilidades de seguridad que puedan ser explotadas por actores maliciosos, y proponiendo recomendaciones para su mitigación.

III. CARACTERÍSTICAS Y CONDICIONES DEL SERVICIO A CONTRATAR

3.1. ALCANCE DEL SERVICIO

El servicio de Ethical Hacking comprenderá la evaluación de seguridad de los aplicativos informáticos del FISSAL expuestos a internet y de la infraestructura tecnológica que soporta dichos servicios.

El alcance del servicio considera los siguientes componentes:

a. Aplicativos Web Institucionales:

APLICATIVO	DESCRIPCIÓN	ENLACE
SAIRC	Sistema de Asignación de Pacientes con Insuficiencia Renal Crónica	https://sairc.fissal.gob.pe/
SIAP	Sistema Integrado de Aplicaciones	https://intranet.fissal.gob.pe/
SISCOP	Sistema de Control Prestacional	https://sso.fissal.gob.pe/frontend/auth
API REST	Web Services	https://api.fissal.gob.pe/swagger/index.html

b. Infraestructura alojada en proveedor externo (IaaS)

Los aplicativos institucionales se encuentran alojados parcialmente en infraestructura bajo modalidad Infrastructure as a Service (IaaS) provista por un proveedor externo.

El servicio deberá considerar el análisis de seguridad de los siguientes servidores asociados a los aplicativos evaluados:

SERVIDOR	FUNCIÓN
FISSAL-BD	Servidor de bases de datos
FISSAL-IIS	Servidor de aplicaciones

Las pruebas deberán realizarse considerando que la infraestructura es administrada por el proveedor externo.

c. Infraestructura interna del FISSAL

El servicio deberá considerar el análisis de seguridad de los siguientes servidores internos del FISSAL asociados a los aplicativos evaluados:

SERVIDOR	FUNCIÓN
PELI-APP02	Servidor web y FTP
PELI-FS01	Servidor de archivos
Server_AD01	Servidor de Directorio Activo
SIAF01	Servidor de base de datos y aplicativos SIGA y SIAF

3.2. ACTIVIDADES DEL SERVICIO

3.2.1. PLANIFICACIÓN DEL SERVICIO

El proveedor deberá iniciar el servicio elaborando un Plan de Trabajo, el cual deberá contener:

- Alcance de las pruebas
- Metodología que utilizará
- Herramientas a emplear
- Cronograma de actividades
- Identificación de los activos a evaluar

Esta fase permite coordinar con la Oficina de TI del FISSAL el inicio de las pruebas y evitar impactos en la disponibilidad de los sistemas.

3.2.2. RECONOCIMIENTO DE LA SUPERFICIE DE ATAQUE

El proveedor deberá realizar actividades de reconocimiento externo, que simulan el comportamiento de un atacante en internet, lo cual permitirá identificar la superficie de ataque expuesta a internet:

Las actividades incluyen:

- Identificación de dominios y subdominios
- Identificación de direcciones IP asociadas
- Enumeración de puertos abiertos
- Identificación de servicios expuestos
- Identificación de tecnologías utilizadas por los aplicativos

3.2.3. PRUEBAS DE SEGURIDAD DE APLICACIONES WEB

Las pruebas deberán incluir, entre otras:

- Pruebas de autenticación
- Pruebas de autorización
- Manipulación de parámetros
- Inyección SQL
- Cross Site Scripting (XSS)
- Carga de archivos maliciosos
- Validación de sesiones
- Exposición de información sensible

Estas pruebas deberán realizarse considerando las recomendaciones del **OWASP Top 10 (2021)**.

3.2.4. ESCANEO DE VULNERABILIDADES

El proveedor deberá ejecutar herramientas especializadas para detectar vulnerabilidades en los sistemas evaluados.

El escaneo deberá incluir:

- Detección de vulnerabilidades en aplicaciones web
- Detección de vulnerabilidades en APIs
- Detección de vulnerabilidades en servidores
- Identificación de software desactualizado
- Identificación de configuraciones inseguras

El proveedor deberá validar manualmente los resultados obtenidos a fin de descartar falsos positivos.

3.2.5. PRUEBAS DE SEGURIDAD DE API

El proveedor deberá realizar pruebas de seguridad sobre la API REST utilizada por los aplicativos del FISSAL.

Las pruebas deberán incluir:

- Identificación de endpoints
- Validación de autenticación
- Manipulación de tokens
- Manipulación de parámetros
- Acceso no autorizado a servicios
- Exposición de información a través de la API

Estas pruebas deberán considerar las recomendaciones del OWASP API Security Top 10.

3.2.6. EVALUACIÓN DE SEGURIDAD DE INFRAESTRUCTURA

El proveedor deberá realizar un análisis de seguridad sobre la infraestructura tecnológica que soporta los aplicativos evaluados.

El análisis deberá incluir:

- Identificación de servicios expuestos
- Escaneo de puertos abiertos
- Detección de vulnerabilidades conocidas
- Análisis de configuraciones de seguridad
- Identificación de versiones de software vulnerables
- Evaluación de configuraciones TLS/SSL
- Identificación de protocolos inseguros

Esta evaluación deberá realizarse sobre:

- Infraestructura alojada en proveedor externo (IaaS)
- Infraestructura interna del FISSAL

Las pruebas deberán realizarse sin afectar la disponibilidad de los sistemas evaluados.

3.2.7. VALIDACIÓN Y CLASIFICACIÓN DE VULNERABILIDADES

El proveedor deberá verificar manualmente las vulnerabilidades detectadas con el objetivo de:

- Confirmar la existencia de la vulnerabilidad
- Descartar falsos positivos
- Validar el impacto potencial en los sistemas evaluados

Las vulnerabilidades identificadas deberán clasificarse utilizando el estándar **CVSS v3.1**, indicando el nivel de criticidad de cada hallazgo.

3.2.8. ELABORACIÓN DEL INFORME TÉCNICO

El proveedor deberá elaborar un informe técnico que incluya como mínimo:

- Descripción de la vulnerabilidad
- Evidencia técnica
- Capturas de pantalla
- Herramientas empleadas
- Prueba de explotación (cuando corresponda)
- Nivel de severidad según CVSS v3.1
- Impacto potencial
- Recomendaciones de mitigación

3.2.9. PRESENTACIÓN DE RESULTADOS

El proveedor deberá realizar una presentación técnica de los resultados del servicio dirigida al personal de la Oficina de Tecnologías de la Información del FISSAL.

La presentación deberá tener una duración mínima de dos (2) horas.

3.3. EJECUCIÓN DE PRUEBAS CONTROLADAS

3.3.1. El proveedor deberá ejecutar las pruebas de Ethical Hacking de manera controlada, asegurando en todo momento la continuidad operativa de los sistemas informáticos del FISSAL.

3.3.2. Las actividades de evaluación de seguridad deberán realizarse bajo la modalidad de pruebas no disruptivas, evitando la ejecución de pruebas que puedan generar degradación del servicio, interrupciones operativas o afectación de la disponibilidad de los sistemas institucionales.

3.3.3. En ese sentido, no se permitirá la ejecución de pruebas de denegación de servicio (DoS o DDoS), ataques de saturación, explotación masiva de vulnerabilidades ni cualquier otra actividad que pueda comprometer la estabilidad de los sistemas o la infraestructura tecnológica del FISSAL.

3.3.4. Asimismo, el proveedor deberá coordinar previamente con la Oficina de Tecnologías de la Información del FISSAL el horario y la planificación de las pruebas, a fin de minimizar cualquier riesgo de impacto sobre los servicios informáticos institucionales.

3.3.5. En caso se identifique una vulnerabilidad que requiera una prueba de explotación para su validación, esta deberá realizarse de manera controlada y previa coordinación con el área responsable, evitando en todo momento la modificación o eliminación de información institucional.

3.4. LIMITACIÓN DE RESPONSABILIDAD DURANTE LA EJECUCIÓN DEL SERVICIO

3.4.1. El proveedor será responsable de ejecutar el servicio de Ethical Hacking conforme a las buenas prácticas internacionales de seguridad de la información y a las condiciones establecidas en los presentes Términos de Referencia.

3.4.2. El proveedor deberá informar de manera inmediata a la Oficina de Tecnologías de la Información del FISSAL cualquier situación que pudiera representar un riesgo para la disponibilidad, integridad o confidencialidad de los sistemas evaluados durante la ejecución de las pruebas.

3.4.3. Asimismo, el proveedor no será responsable por vulnerabilidades existentes en sistemas, aplicaciones o infraestructura que se encuentren fuera del alcance definido en los presentes Términos de Referencia.

3.5. CONFIDENCIALIDAD DE LA INFORMACIÓN Y DE LOS HALLAZGOS DE SEGURIDAD

3.5.1. El proveedor deberá mantener estricta confidencialidad respecto de toda la información a la que tenga acceso durante la ejecución del servicio, incluyendo información técnica, arquitecturas tecnológicas, configuraciones de sistemas, credenciales de acceso y cualquier otro dato relacionado con la infraestructura tecnológica del FISSAL.

3.5.2. De manera especial, el proveedor deberá mantener absoluta reserva respecto de las vulnerabilidades, debilidades de seguridad o riesgos identificados durante el desarrollo del servicio de Ethical Hacking, comprometiéndose a **no divulgar, publicar, transferir o compartir dicha información con terceros sin autorización expresa del FISSAL**.

3.5.3. Los informes técnicos, evidencias, hallazgos y resultados generados como producto del servicio serán de propiedad exclusiva del FISSAL y únicamente podrán ser utilizados por la entidad para fines de mejora de la seguridad de la información.

3.5.4. La obligación de confidencialidad establecida en la presente cláusula se mantendrá vigente incluso después de concluido el servicio contratado.

3.6. REQUISITOS MÍNIMOS DEL PROVEEDOR

3.6.1. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

REQUISITOS:

El postor debe acreditar un monto facturado acumulado equivalente a S/ 50,000.00 (Cincuenta Mil con 00/100 Soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los diez (10) años anteriores a la fecha de la presentación de ofertas que se computa desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran servicios similares a los siguientes:

- Servicio de análisis de vulnerabilidad

- Servicio de administración y monitoreo de plataformas de seguridad.
- Servicio de hacking ético
- Servicio de Pentesting
- Suscripción de plataformas de gestión de riesgo cibernético y/o antivirus y/o antispam.
- Servicio de análisis de código fuente
- Servicio de Test Intrusion

ACREDITACIÓN:

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con constancia de depósito, nota de abono, reporte o estado de cuenta, cualquier otro documento emitido por entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de veinte contrataciones. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados; para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de compra con conformidad o constancia de prestación.

En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los quince (15) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

3.6.2. CAPACIDAD TÉCNICA PROFESIONAL

PERSONAL CLAVE: ESPECIALISTA TÉCNICO

REQUISITOS:

- **Un (1) consultor en seguridad de la información**
  Experiencia mínima de tres (3) años como consultor en seguridad de la información en servicio de Hacking Ético y/o Servicio de Pentesting y/o servicio de Análisis de código fuente y/o servicio de revisión y monitoreo de seguridad para el desarrollo de software y/o servicio de trust de intrusión y/o servicio de test de vulnerabilidades y/o servicio de test de penetración y/o provisión de servicio de monitoreo intraoperativo y/o servicio de gestión de riesgos de TI, los mismos que serán contabilizados a partir de la fecha de emisión del grado académico requerido.

- **Formación académica**

  Título o bachiller en las carreras de Ingeniería de Sistemas o Ingeniería de Sistemas e Informática o Licenciatura en Computación y Sistemas o Ingeniería de Computación y Sistemas o Ingeniería Informática o Ingeniería Electrónica o Ingeniería de Telecomunicaciones o Ingeniería de Redes o Ingeniería de Software o Ingeniería en Redes y Comunicaciones o Licenciatura en Computación o Licenciatura en Ciencia de la Computación o Ingeniería de Seguridad y Auditoría Informática.

ACREDITACIÓN

El TITULO PROFESIONAL y/o GRADO DE BACHILLER REQUERIDO será verificado por los evaluadores en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente enlace:

https://enlinea.sunedu.gob.pe/

o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente enlace:

https://titulosinstitutos.minedu.gob.pe/ , según corresponda.

El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido.

En caso TITULO PROFESIONAL y/o GRADO DE BACHILLER REQUERIDO no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.

En caso se acredite estudios en el extranjero del personal clave, debe presentarse adicionalmente copia simple del documento de la revalidación o del reconocimiento ante SUNEDU, del grado académico o título profesional otorgados en el extranjero, según corresponda.

3.7. SEGUROS (NO CORRESPONDE)

3.8. LUGAR Y PLAZO DE PRESTACIÓN DEL SERVICIO

3.6.1. Lugar

El servicio será brindado en el Fondo Intangible Solidario de Salud: Sede Central del Fondo Intangible Solidario de Salud Calle 41 N.º 840, San Isidro - Lima 27, Perú San Isidro, Lima, Lima – 15027. Adicionalmente se considera que el proveedor podrá realizar actividades de gabinete en sus propias instalaciones.

3.6.2. Plazo

La duración del presente servicio será de hasta cuarenta y cinco (45) días calendario posteriores a la entrega del plan de trabajo, que será coordinado por la Oficina de Tecnología de la Información del FISSAL, quien indicará la fecha de inicio del servicio.

3.9. ENTREGABLES/PRODUCTO

El servicio brindado por el Postor incluye el siguiente entregable, que comprende:

Plan de trabajo: Hasta 7 días calendarios, contado a partir de la notificación de la orden de servicio. **La entrega del Plan de Trabajo no estará computada dentro del cronograma del servicio requerido**.
El Plan de trabajo deberá ser aprobado por el Personal de la Oficina de Tecnología de la Información del FISSAL.

Único entregable: Hasta 45 días calendarios, contado a partir de la entrega del plan de Trabajo.

Cabe indicar que los (productos y/o entregables) deberán ser presentados por el proveedor con atención a la Oficina de Tecnología de Información a través de la mesa de partes virtual: http://intranet.fissal.gob.pe/Usuario/NuevaCuentaMesaVirtual

De ser el caso, adjuntando los casos archivos digitales (editables), que no deben contener contraseña, o en dispositivos de almacenamiento de datos (CD, USB u otro medio digital).
El proveedor acepta que será responsable por los daños y perjuicios que pudieran ocasionarse al FISSAL como consecuencia de cualquier acto de confidencialidad del contratista o su personal a lo antes mencionado.

IV. OTRAS CONSIDERACIONES PARA LA EJECUCIÓN DE LA PRESTACIÓN

4.1 CONFIDENCIALIDAD

El proveedor se compromete a no revelar información oral, escrita, servicios, políticas o prácticas de negocio del FISSAL, y en la virtud, divulgación, comunicación, transmisión o utilización para beneficio de cualquier persona distinta al FISSAL, será considerado ilegal.
El PROVEEDOR y el personal designado por éste para el desarrollo del SERVICIO asumen los siguientes compromisos:

- No revelar, comentar, suministrar o transferir de cualquier forma a terceros, cualquier información que hubiese recibido directa o indirectamente de FISSAL o que haya sido generada en relación con el SERVICIO.

• Manejar de manera confidencial la información de reportes o información generada durante el SERVICIO, así como no emplearla en beneficio propio o de terceros.

• Suscribir el correspondiente acuerdo de confidencialidad

4.2 PROPIEDAD INTELECTUAL

El contratista, no tendrá ningún título, patente u otros derechos de propiedad sobre ninguno de los documentos preparados con el Fondo Intangible Solidario de Salud, tales derechos pasarán a ser propiedad de FISSAL.

4.3 MEDIDAS DE CONTROL DURANTE LA EJECUCIÓN CONTRACTUAL

4.3.1 Conformidad de la prestación

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025. La conformidad es otorgada por la Oficina de Tecnología de la Información del Fondo Intangible Solidario de Salud – FISSAL, en el plazo máximo de siete (07) días computados desde el día siguiente de recibido el entregable.

De existir observaciones, LA ENTIDAD CONTRATANTE las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar. Si pese al plazo otorgado, EL CONTRATISTA no cumpliese a cabalidad con la subsanación, LA ENTIDAD CONTRATANTE puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar sin considerar los días en los que pudiera incurrir la entidad contratante para efectuar las revisiones y notificar las observaciones correspondientes.

Este procedimiento no resulta aplicable cuando los servicios manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso LA ENTIDAD CONTRATANTE no efectúa la recepción o no otorga la conformidad, según corresponda, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.

4.3.2 Forma de pago

El pago por el presente servicio se realizará bajo la modalidad de pago a suma alzada, previa conformidad del servicio y envío de comprobante de pago.

LA ENTIDAD CONTRATANTE se obliga a pagar la contraprestación a EL CONTRATISTA, luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

Para tal efecto, el responsable de otorgar la conformidad de la prestación debe hacerlo en un plazo que no excederá de los siete (7) días contabilizados desde el día siguiente de recibido el entregable, salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, en cuyo caso la conformidad se emite en un plazo máximo de veinte (20) días, bajo responsabilidad de dicho servidor.

LA ENTIDAD CONTRATANTE debe efectuar el pago dentro de los diez (10) días hábiles siguientes de otorgada la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del servidor competente.

En caso de retraso en el pago por parte de LA ENTIDAD CONTRATANTE, salvo que se deba a caso fortuito o fuerza mayor, EL CONTRATISTA tiene derecho al pago de intereses legales conforme a lo establecido en el artículo 67 de la Ley N° 32069, Ley General de Contrataciones Públicas.

4.3.3 Penalidad por mora

Si EL CONTRATISTA incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, LA ENTIDAD CONTRATANTE le aplica automáticamente una penalidad por mora por cada día de atraso, de acuerdo con la siguiente fórmula prevista en el Art. 120 del RLGCE:

Penalidad diaria = 0.10 x Monto vigente
F x Plazo vigente en días

Donde F tiene el siguiente valor:
F = 0.40

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando EL CONTRATISTA acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso la calificación del retraso como justificado por parte de LA ENTIDAD CONTRATANTE no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme el numeral 120.4 del artículo 120 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 0092025-EF.

4.3.4 Otras penalidades aplicadas (NO CORRESPONDE)

4.3.5 Responsabilidades por vicios ocultos

La recepción conforme de la prestación por parte de LA ENTIDAD CONTRATANTE no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 69 de la Ley N° 32069, Ley General de Contrataciones Públicas y 144 de su Reglamento aprobado por Decreto Supremo N° 009-2025-EF.

El plazo máximo de responsabilidad del contratista es de un (01) año contado a partir de la conformidad otorgada por LA ENTIDAD CONTRATANTE

4.4 Declaración Jurada de Interés (NO CORRESPONDE)

4.5 Otros (NO CORRESPONDE)

V. CLAUSULA DE ANTICORRUPCIÓN Y ANTISOBORNO

A la suscripción de este contrato, 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 CONTRATANTE.

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 CONTRATANTE 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.

VI. GESTIÓN DEL RIESGO

LAS PARTES realizan la gestión de riesgos de acuerdo con lo establecido en el presente contrato y los documentos que lo conforman, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación.

VII. SOLUCION DE CONTROVERSIAS

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación, según el acuerdo de las partes.

Cualquiera de las partes tiene derecho a iniciar el arbitraje a fin de resolver dichas controversias dentro del plazo de caducidad previsto en la Ley N° 32069, Ley General de Contrataciones Públicas y su Reglamento, aprobado por Decreto Supremo N° 009-2025-EF.

El Laudo arbitral emitido es inapelable, definitivo y obligatorio para las partes desde el momento de su notificación, según lo previsto en el numeral 84.9 del artículo 84 de la Ley N° 32069, Ley General de Contrataciones Públicas

VIII. RESOLUCIÓN DEL CONTRATO

La resolución de contrato puede ser de forma total o parcial. La resolución parcial sólo involucra a aquella parte del contrato afectada por el incumplimiento y siempre que dicha parte sea cuantificable, separable e independiente del resto de las obligaciones contractuales.
El apercibimiento previo y la resolución que se efectúe precisan con claridad qué parte del contrato queda resuelta, de no hacerse tal precisión, se entiende que la resolución es total.
Cualquiera de las partes puede resolver, total o parcialmente, el contrato en los siguientes supuestos:

a. Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.
b. Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple.
c. 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.
d. Por incumplimiento de la cláusula anticorrupción.

e. Por la presentación de documentación falsa o inexacta durante la ejecución contractual.
f. Configuración de la condición de terminación anticipada establecida en el contrato, de acuerdo con los supuestos que se establezcan en el reglamento para su aplicación.

Cuando la resolución del contrato se produce por causa imputable a una de las partes, corresponde resarcir los daños y perjuicios acreditados.
En caso de corrupción de funcionarios o servidores no corresponde el pago de resarcimiento por daños y perjuicios al contratista, aun cuando este último no lo haya propiciado.

DEL PROCEDIMIENTO DE RESOLUCION:
En el supuesto del literal b), la parte afectada por el incumplimiento observa el siguiente procedimiento.

a. La parte perjudicada requiere a la otra parte que ejecute la prestación materia de incumplimiento, bajo apercibimiento de resolver el contrato. El plazo para el cumplimiento de la prestación debe ser razonable y no debe ser menor del 10% del plazo del contrato, ítem, o entregable materia de incumplimiento, según corresponda, y en ningún caso puede superar el 15% del plazo del contrato, ítem o entregable materia de incumplimiento. Cuando el plazo obtenido como resultado de la aplicación del porcentaje sea una cifra decimal, corresponde que la entidad contratante efectúe el redondeo a favor del contratista, computándose como un día completo adicional en dicho supuesto. En los casos en que el plazo del contrato, ítem o entregable materia de cumplimiento es menor a treinta días, se otorga tres días.

b. Vencidos los plazos establecidos en el literal precedente sin que la otra parte cumpla con la prestación correspondiente, la parte perjudicada puede resolver el contrato en forma total o parcial.
Este apercibimiento previo no es aplicable en caso se haya llegado a completar el monto máximo de penalidad al contratista o la entidad contratante sustente de manera objetiva que, la situación de incumplimiento ya no pueda ser revertida, de acuerdo con el pronunciamiento que emite el área usuaria. En estos casos, la entidad contratante notifica al contratista la resolución del contrato de forma parcial o total, según corresponda.
En los supuestos establecidos en los literales a) y c), la parte que resuelve debe justificar y acreditar que la situación que alega hace imposible la continuidad de la ejecución de las prestaciones a su cargo, de manera definitiva.

En los supuestos señalados en los literales a), c), d), e) y f), las partes pueden resolver el contrato sin apercibimiento previo, quedando el contrato resuelto de pleno derecho a partir de la notificación.

La resolución del contrato por incumplimiento de la cláusula anticorrupción y antisoborno no impide el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

Fissal

Firmado digitalmente por:
DIAZ BAZAN Pepe Hernando
FAU 20546736718 soft
Motivo: Doy fé
Fecha: 10/03/2026 16:29:18-0500

Firmado digitalmente por:
MENDOZA ORTIZ Agripino
Fredy FAU 20546736718 soft
Motivo: Doy V° B°
Fecha: 10/03/2026 16:27:47-0500