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 Mantenimiento Preventivo de Sistemas de protección y seguridad para Red – Firewall.

I. FINALIDAD PÚBLICA.

La presente contratación tiene por finalidad la protección, disponibilidad, continuidad y operación segura de la red institucional del FISSAL, mediante un servicio gestionado de administración, monitoreo y soporte de la plataforma de protección de red.

El servicio permitirá fortalecer la postura de ciberseguridad de la entidad, optimizar la gestión de los controles de seguridad perimetral, reducir la exposición frente a amenazas informáticas y contribuir al cumplimiento de los objetivos institucionales, asegurando la continuidad de los servicios tecnológicos que brindan soporte a los procesos misionales y administrativos.

La contratación requerida según las actividades previstas en el Plan Operativo Institucional POI.

II. OBJETIVO DE LA CONTRATACIÓN.

Contratar a una empresa especializada que brinde el Servicio de Mantenimiento Preventivo de Sistemas de protección y seguridad para Red – Firewall para el Fondo Intangible Solidario de Salud – FISSAL, a fin de garantizar adecuados niveles de seguridad, disponibilidad, continuidad operativa, atención de eventos e incidentes de seguridad, soporte técnico especializado y gestión permanente de la plataforma de protección de red, durante un plazo de trecientos sesenta y cinco (365) días calendario.

III. CARACTERÍSTICAS Y CONDICIONES DEL SERVICIO A CONTRATAR.

Detalles de las características a desarrollar:

3.1 Descripción del servicio a contratar

Ítem	Cantidad	Descripción del servicio
1	01	Servicio de Mantenimiento Preventivo de Sistemas de protección y seguridad para Red – Firewall.
2	01	Soporte Técnico 24 x 7 x 365

La contratación del de Mantenimiento Preventivo de Sistemas de protección y seguridad para Red – Firewall permitirá contar con una gestión especializada de la infraestructura de seguridad de red de la entidad, incluyendo la administración de políticas de seguridad, monitoreo de eventos, soporte técnico, atención de incidentes, actualización de configuraciones, gestión de licenciamiento, revisión de alertas, generación de reportes y recomendaciones de mejora continua

Características del Servicio:

Funciones de la solución de Protección de Red

- Licenciamiento anual (vigencia de 365 días) de la solución de Protección de Red tipo Firewall UTM, que incluye consola de gestión, con capacidad para soportar al menos 3Gpbs como NGFW.
- Las características básicas de la solución de firewall perimetral tipo UTM serán las siguientes:
    - El licenciamiento deberá permitir un rendimiento de al menos 2.5 Gbps de prevención de amenazas medidos con tráfico Empresarial Mixto o Condiciones de Prueba Empresarial.
    - El licenciamiento deberá permitir el uso de al menos 16 interfaces GE, 4 SFP+ y 8 SFP.
    - El licenciamiento deberá permitir al menos 3M de sesiones concurrentes (TCP).
    - El licenciamiento deberá permitir el uso de una interfaz GE para administración dedicada.
    - El licenciamiento deberá permitir operar simultáneamente en modo sniffer (monitoreo y análisis de tráfico de red), capa 2 (L2) y capa 3 (L3).
    - Debe ser compatible con NAT estático y NAT dinámico
    - Para IPv4, soportar enrutamiento estático y dinámico (RIP, OSPF y BGP) Interface gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interface debe soportar SSL sobre HTTP (HTTPS)
    - Comunicación cifrada y autenticada con username y password, tanto como para la interface gráfica de usuario como la consola de administración de línea de comandos (SSH)
    - El administrador del sistema soporta las opciones incluidas de autenticarse vía password y vía certificados digitales.
    - Deberá ofrecer la flexibilidad para especificar que los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet, http o HTTPS.
    - Soporte de SNMP versión 2
    - Soporte de syslog para poder enviar bitácoras a servidores de SYSLOG remotos.
    - Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 2 perfiles para administración y monitoreo del Firewall.

- Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.
- Debe soportar el protocolo estándar de la industria VXLAN;
- Debe incluir capacidades de SD-WAN perpetuas o licenciadas durante el periodo de tres años.
- En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN.
- Debe soporta protección contra la suplantación de identidad (anti-spoofing);
- Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs
- Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall.
- Las reglas del firewall deberán tomar en cuenta dirección IP fuente (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando
- El análisis de firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;
- Las acciones de las reglas deberán contener al menos el aceptar o rechazar la comunicación
- Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.
- Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año)
- Capacidad de hacer traslación de direcciones estático, uno a uno, NAT.
- Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT.
- Deberá soportar reglas de firewall en IPv6.
- Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP
- Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs
- Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas
- Soportar Policy based routing o policy based forwarding;
- El soporte a políticas de ruteo deberá permitir que ante la presencia de dos enlaces a Internet, se pueda decidir cuál de tráfico sale por un enlace y qué tráfico sale por otro enlace
- Soporte a ruteo dinámico RIP, OSPF y BGP
- Soporte a ruteo de multicast
- Soportar alta Disponibilidad en modo Activo-Pasivo/Activo-Activo
- Posibilidad de definir al menos dos interfaces para sincronía de Cluster
- La configuración de alta disponibilidad debe sincronizar: sesiones, configuraciones, incluyendo, políticas de Firewalls, NAT, QoS y objetos de la red;

- La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;
- La configuración de alta disponibilidad debe sincronizar: Tablas FIB;
- Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);
- Debe soportar la integración con otras plataformas de ciberseguridad a través de API, a fin de proporcionar una solución integral que proteja diferentes vectores de ataque;
- Debe soportar integración con una plataforma de sandboxing en las instalaciones de la misma marca, para detectar amenazas avanzadas dentro de la red.
- La solución debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.
- Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto país/países;
- Debe permitir la visualización de los países de origen y destino en los registros de acceso;
- Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;
- Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo);

- Las características específicas de la solución de firewall perimetral tipo UTM relacionados a la identificación de usuarios serán los siguientes:

  - Capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;
  - Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;
  - Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios;
  - Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la política/control basados en usuarios y grupos de usuarios;
  - Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la

navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo);
- Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;
- Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;
- Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;

- Las características específicas de la solución de firewall perimetral tipo UTM para la función de control de aplicaciones serán los siguientes:

  - Reconocer miles de aplicaciones diferentes, distribuido en 18 categorías, incluyendo: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico.
  - La solución deberá tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo.
  - Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor.
  - Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante
  - Actualización de la base de firmas de la aplicación de forma automática.
  - Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas.
  - Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante.
  - Debe alertar al usuario cuando sea bloqueada una aplicación.
  - Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc).
  - Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación y categoría de Aplicación

- Las características específicas de la solución de firewall perimetral tipo UTM para la función de filtrado URL serán los siguientes:

  - Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora).
  - Debe ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad.

- Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está utilizando las URL esto mediante la integración con los servicios de directorio Active Directory y la base de datos local.
- Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local.
- Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL.
- Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL.
- Tener por lo menos 60 categorías de URL.
- Debe tener la funcionalidad de exclusión de URLs por categoría.
- Permitir página de bloqueo personalizada.
- Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio).

- Las características específicas de la solución de firewall perimetral tipo UTM para la función de prevención de amenazas serán los siguientes:

  - Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo.
  - Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware).
  - Las características de IPS, antivirus y anti-spyware deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante
  - Debe ser posible crear políticas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad
  - Excepciones por IP de origen o destino deben ser posibles en las reglas o en cada una de las firmas.
  - Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos.
  - Deber permitir el bloqueo de vulnerabilidades y de exploits conocidos.
  - Debe incluir la protección contra ataques de denegación de servicio.
  - Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc.
  - Detectar y bloquear los escaneos de puertos de origen.
  - Bloquear ataques realizados por gusanos (worms) conocidos.
  - Contar con firmas específicas para la mitigación de ataques DoS y DDoS.
  - Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow).
  - Debe poder crear firmas personalizadas
  - Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3.
  - Soportar el bloqueo de archivos por tipo.
  - Identificar y bloquear la comunicación con redes de bots.

- Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación.
- La solución debe proteger de amenazas avanzadas que utilizan conexiones DNS, de manera que permita filtrar las consultas de DNS de los hosts para bloquear conexiones hacia sitios maliciosos, conexiones de botnet, ya sea en base a categorías o firmas.
- La capacidad de filtro de DNS debe ser alimentada por un servicio de inteligencia de amenazas de la propia marca.
- Debe permitir la translación en el firewall de una consulta de DNS, a fin de redirigir la resolución hacia otro destino diferente del original.
- Los eventos deben identificar el país que origino la amenaza;
- Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms).
- Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP.

- Las características específicas de la solución de firewall perimetral tipo UTM para la función VPN serán los siguientes:

  - Soporte VPN de sitio-a-sitio y cliente-a-sitio.
  - Soportar VPN IPSec y VPN SSL.
  - La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512.
  - La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14.
  - La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2).
  - La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard).
  - Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución
  - Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
  - Las características de VPN SSL se deben cumplir con o sin el uso de agentes.
  - Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy.
  - Asignación de DNS en la VPN de cliente remoto.
  - Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL.
  - Suportar autenticación vía AD/LDAP, token, certificado y base de usuarios local.
  - Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL.
  - Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;
  - Deberá mantener una conexión segura con el portal durante la sesión;
  - La capacidad de conexión VPN SSL o IPSEC cliente-a-sitio debe disponer de un agente con compatibilidad al menos para Windows, Mac OS,

android y iOS. Además, debe contar con un método de conexión que no requiera de un agente instalado.
- La plataforma debe tener la capacidad de soportar al menos 16,000 conexiones VPN SSL concurrentes desde dispositivos endpoint y móviles, ya sea usando agente o sin agente.
- El agente de VPN client-to-site debe validar la configuración del dispositivo cliente antes de otorgar el acceso a la red. Debe soportar como mínimo los siguientes criterios de evaluación antes de brindar el acceso a la red: protección activa del antivirus, firewall de host y versión de sistema operativo, así como una combinación de estos criterios.
- Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;
- La solución debe considerar al menos dos tokens, permitiendo la autenticación de dos factores para los usuarios asignados hacia la interfaz de gestión del firewall y el acceso por VPN SSL;

- Las características específicas de la solución de firewall perimetral tipo UTM para la función "QoS traffic shaping" serán los siguientes:

  - Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming.
  - Soportar la creación de políticas de QoS y Traffic Shaping:
  - Por dirección de origen.
  - Por dirección de destino.
  - Por usuario y grupo.
  - Por aplicaciones.
  - Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto.
  - En QoS debe permitir la definición de tráfico con ancho de banda garantizado y máximo ancho de banda.
  - En QoS debe permitir la definición de colas de prioridad.
  - Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.
  - Soportar marcación de paquetes DiffServ, incluso por aplicación.
  - Soportar la modificación de los valores de DSCP para Diffserv.
  - Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service).
  - Proporcionar estadísticas en tiempo real para clases de QoS y Traffic Shaping.
  - Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes.

- Con la finalidad que el proveedor cumpla con proporcionar una solución de Protección de Red tipo Firewall UTM de acuerdo a las exigencias técnicas requeridas en el presente documento durante el plazo establecido, se aceptará el licenciamiento, la reposición y/o inclusión de hardware tipo appliance necesario.

Para tal efecto, se deberá tener en cuenta las diferentes vigencias tecnológicas publicadas por el fabricante en sus canales de comunicación oficiales.

Funciones de Servicio Gestionado

- Se entenderá por avería a una interrupción parcial o total de las soluciones adquiridas, así como a una pérdida de la calidad del mismo.
- El CONTRATISTA deberá indicar una lista o protocolo de escalamiento con la información (nombre, número telefónico, correo electrónico) del personal que será el segundo nivel de escalamiento para el reporte de averías y/o soporte técnico sobre toda la solución ofertada.
- El contratista debe proveer una herramienta online con interfaz Web disponible 24x7x365 para la generación de tickets de atención de averías y de solicitudes por parte de personal de la entidad; asimismo, se debe poder visualizar su estado de atención; debiendo contar con las siguientes funciones:

    - Portal web provisto por el contratista
    - Acceso permitido con al menos dos o más usuarios de la entidad, responsables por la gestión de incidencias, basado en perfiles de usuario y roles
    - Apertura guiada de tickets, que permita diferenciar el nivel de servicio que se requiere.
    - Historial de tickets que permita contar con número de ticket, fecha de creación y estado.
    - Información asociada al ticket, que contenga información sobre los ejecutivos a cargo del mismo, fechas y horas, y capacidad de adicionar mensajes o archivos adjuntos, que se indexen al caso.
    - Soporte de envío de notificación a correo
    - El contratista debe proveer una herramienta online con interfaz Web disponible 24x7x365 para la generación de tickets de atención de averías y de solicitudes

- En el caso de averías, el tiempo de respuesta para la solución deberá ser como máxima de (01) hora. El tiempo de inoperatividad del servicio se calculará desde el reporte de la falla por parte de la entidad hasta la verificación de la solución de la avería también por parte de la entidad. Para el caso de averías, el contratista deberá entregar un informe en el que se detallen las causes, acciones tomadas y tiempos de solución en estos casos. El tiempo acumulado mensual de indisponibilidad del servicio no deberá ser mayor a cuatro (04) horas.
- El tiempo de respuesta es de 30 minutos. Dentro de ese plazo, se realiza primeros descartes hasta que se genera el ticket de atención. El tiempo de atención de cualquier tipo de incidente será computado a partir de la generación del ticket de atención.
- El tiempo de solución de una avería se computa desde que se genera el ticket de atención hasta la validación de la solución de la avería. El tiempo de atención de cualquier tipo de avería será computado a partir de la generación del ticket de atención.
- El postor deberá contar con un Centro de Atención de llamadas o Atención al Cliente, disponible las 24 horas del día por un periodo de doce (12) meses, para atención de reportes de incidencias y requerimientos. El tiempo de respuesta máximo para la atención de cada incidente reportado será de 120 minutos,

entendiéndose como tiempo de respuesta el tiempo que transcurre desde que el incidente es reportado hasta que el contacto técnico de FISSAL recibe el nro. de ticket de registro de la incidencia.

- El servicio de soporte deberá contar con un Proceso de Gestión de Incidentes y Monitoreo, los cuales deben contar certificación ISO 27001, la acreditación se deberá realizar con la presentación de la copia simple de la certificación para la presentación de propuesta.

- **Servicio de análisis de vulnerabilidades y priorización de riesgos**

  - Realizar de manera semestral un servicio de análisis de vulnerabilidades y priorización de riesgos considerando lo siguiente:

    - Se deberá utilizar un equipo físico de propósito especifico.
    - El equipo utilizado deberá contar con Sistema Operativo Propietario, hardenizado.
    - El fabricante de la solución de análisis de vulnerabilidades y del equipo de propósito especifico debe ser el mismo.
    - Para la ejecución del servicio de Análisis de vulnerabilidades considerar al menos 50 dispositivos de la entidad (PCs y/o SERVIDORES).
    - La solución deberá contar con un poderoso motor para recopilar información, realizar evaluaciones de vulnerabilidad y analizarlos.
    - La solución deberá contar con opción de disponibilidad en la Nube o en la versión de Dispositivo Mainframe.
    - La solución deberá contar con más de 500,000 plugins.
    - Capacidad de conectarse con software populares de fuente abierta y de seguridad comercial para una revisión y explotación más profundas.
    - La solución deberá contar con un sistema de automatización y machine learning.
    - La solución deberá contar con capacidad de automatización, con el propósito de priorizar las amenazas, ampliar las respuestas, reducir la mano de obra y generar un flujo de trabajo consistente.
    - La solución deberá contar con capacidad de validación continua, y debe automatizar y acelerar el proceso para identificar plataformas y dispositivos de redes mal configurados.
    - La solución deberá contar con capacidad de revisar si el sitio web ha sido hackeado anteriormente o usado para fishing.
    - La solución deberá contar con capacidad de verificación para evitar falsos positivos, tales como:
      - Pruebas de bajo nivel, realizando fuzzing a los servicios y verificando las respuestas en lugar de solo revisar los banners, para encontrar vulnerabilidades potenciales.
      - Múltiples pruebas, la solución deberá comparar las pruebas de fuzzing, las pruebas de la Base de Datos y las pruebas de los plug-ins externos, llevando una vulnerabilidad potencial al nivel: Muy Probablemente.
    - La solución deberá contar con capacidad de identificación de soluciones.
    - La solución deberá contar con un Sistema de Monitoreo, siendo esta una plataforma dedicada a la validación continua de la seguridad.
    - La solución deberá permitir conectarte y personalizar VA, PT y Monitoring con la interfaz gráfica o con las API.

- Capacidad de probar como mínimo: Cross Site Scripting, SQL Injection, Path Disclosure, Denial of Service, Code Execution, Memory corruption, Cross Site Request Forgery, Information Disclosure, Arbitrary File Disclosure, Local File Inclusion/Remote File Include, Buffer overflow, Otros (PHP/Javascript/Path Injection, Directory Traversal, etc.).
- Deberá tener integrado herramientas tales como:
  - Herramientas de PentTesting: Nmap, Metasploit, Hydra, etc.
  - Herramientas de análisis de Vulnerabilidades (AV) de red como Nessus, OpenVas, Rapid7 Nexpose, Nmap, Amap, etc.
  - Herramientas de análisis de Aplicaciones Web: Acunetix WVS, Nikto, OWASP ZAP, Burp Suite, DirBuster, W3af, etc.
  - Herramientas de manipulación de URL: Burp Suite, OWASP ZAP. Acunetix WVS, W3af, etc.
  - Herramientas de Seguridad en Base de Datos: SQLninja, SQLmap,etc.
  - Herramientas de Craking de Constraseñas: Joht the ripers, etc.
- Deberá soportar escaneo de Servicios Web: Apache, Internet Information Services (IIS), Tomcat y NGINX.
- Soportar Aplicaciones basadas en: HTML, PHP, .NET, JSP, Phyton, JAVA, ASPX, JAVASCRIPT, AJAX, FLASH, XML y SOAP.
- Soportar escaneos de Bases de Datos: MySQL, MS-SQL, PostgreSQL, Oracle, DB2 y Informix.
- Soportar integración con sistemas de autenticación: LDAP, Active Directory, TACACS y Radius.
- Soportar integración con sistemas: SIEM, IPS, Va, Pentest.
- Capacidad de exportar los resultados en formatos: HTML, PDF, CSV, RTF y XML.
- El proveedor deberá ser canal o Partner autorizado por el fabricante de la herramienta a utilizar, se acreditará con la presentación de la carta emitido por el fabricante.
- El proveedor deberá entregar un informe detallando las acciones realizadas, las evidencias encontradas y las soluciones implementadas en idioma español.
- Se debe presentar documentación técnica en la etapa de propuesta que indique el cumplimiento con la herramienta a utilizar, mediante hojas técnicas, y/o datasheets, y/o guías de usuario y/o guías de administración en idioma inglés o español. No se aceptará carta o declaración jurada de cumplimiento.

3.2 Actividades

Otras actividades a considerar
Implementación:

- Elaborar y presentar un plan de implementación del servicio.
- Realizar el levantamiento técnico de la infraestructura actual de red y seguridad.
- Validar, suministrar, activar o renovar el licenciamiento requerido para la operación de la solución de Protección de Red durante el periodo de 365 días calendario.
- Realizar respaldo inicial de la configuración actual.
- Revisar la configuración existente del equipo.
- Aplicar configuraciones de administración segura.

- Implementar el esquema de monitoreo inicial del servicio gestionado, considerando disponibilidad, rendimiento, eventos de seguridad, estado de licencias, estado de interfaces, túneles VPN y salud general del equipo.
- Ejecutar pruebas funcionales de conectividad, navegación, publicación de servicios, VPN, filtrado web y control de aplicaciones.
- Presentar el informe final de implementación, incluyendo actividades ejecutadas, licencias activadas, configuración aplicada, pruebas realizadas, hallazgos, recomendaciones y estado de configuración del servicio.
- Suscribir con FISSAL el acta de conformidad de implementación, dejando constancia del inicio formal de la etapa de operación del servicio gestionado.

Soporte Técnico:

- El proveedor deberá brindar el servicio de soporte técnico (24x7x365) para averías mediante un servicio de SOC, en línea, por correo y/o por teléfono con 24x7 (24 horas durante los 7 días calendario de la semana), con un tiempo máximo de respuesta de treinta (30) minutos, luego de colocado el pedido de soporte.

- El servicio de soporte deberá contar con un Proceso de Gestión de Incidentes y Monitoreo, los cuales deben contar certificación ISO 27001, la acreditación se deberá realizar con la presentación de la copia simple de la certificación para la presentación de propuesta.

- Este servicio será provisto durante todo el tiempo de vigencia de la prestación principal.

- También debe ser provisto un nivel de soporte directo con el fabricante que pueda ser escalado de ser necesario por la Oficina de Tecnologías de la Información del FISSAL para casos críticos.

3.3 Plan de trabajo (NO CORRESPONDE)

3.4 Requisitos mínimos del proveedor

REQUISITOS DE CALIFICACION

- Deberá tener Inscripción vigente en el Registro Nacional de Proveedores (RNP) en el rubro de servicios.
- No estar impedido de contratar con el estado de acuerdo al Art. 30 de la LEY GENERAL DE CONTRATACIONES PÚBLICAS.
- Tener experiencia en el rubro.
- El contratista deberá ser canal y/o partner y/o distribuidor autorizado de la solución de Protección de Red a utilizar.
- El contratista deberá ser canal y/o partner y/o distribuidor autorizado de la herramienta de análisis de vulnerabilidades a utilizar.
- El proveedor deberá contar con certificación ISO 27001 en el proceso de Gestión de Incidentes y Monitoreo en servicios de SOC para el servicio de soporte técnico (24x7x365) requerido.

Acreditación:

- La acreditación se realizará con la presentación de copia simple de certificados.

- La acreditación de partner o canal autorizado en la marca de la solución de Protección de Red y de la herramienta de análisis de vulnerabilidades a utilizar, se debe acreditar, con la presentación de una carta oficial emitida por los fabricantes propuestos, con referencia al presente requerimiento.
- La acreditación de la certificación ISO 27001 en el proceso de Gestión de Incidentes y Monitoreo en servicios de SOC para el servicio de soporte técnico (24 X7X365) requerido, deberá sustentarse mediante la presentación de copia simple del certificado vigente correspondiente.

A. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Requisitos:
El postor deberá acreditar un monto facturado acumulado de S/ 35,000.00 (treinta y cinco mil quinientos y 00/100 soles) por la prestación de Servicio de Mantenimiento Preventivo de Sistemas de protección y seguridad para Red, o servicios similares en los últimos ocho (8) años anteriores a la fecha de presentación de ofertas, contados desde la conformidad o fecha de emisión del comprobante de pago.

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 de 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 (20) 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.

Se consideran servicios similares, mantenimiento de servidores y/o equipos de comunicaciones, venta de servidores, appliances y equipos de seguridad UTM, implementación de soluciones Cloud, Servicios de suscripción y soporte en general, servicios de implementación y suscripción de licencias de software en general como: firewall y soluciones de seguridad perimetral y endpoints.

B. CAPACIDAD TÉCNICA Y PROFESIONAL (personal técnico y/o personal clave)

Formación académica del Personal Clave:

UN (01) JEFE DE PROYECTO

Profesional Titulado en Ingeniería Electrónica y/o Sistemas y/o Telecomunicaciones y/o

Computación y/o Ingeniería Empresarial y de Sistemas, y/o Ingeniería de Seguridad y Auditoria informática. Colegiado

DOS (02) ESPECIALISTAS PARA GESTION DE INCIDENTES Y MONITOREO

Profesional Titulado o Bachiller en Ingeniería Electrónica y/o Sistemas y/o Telecomunicaciones y/o Computación y/o Ingeniería Empresarial y de Sistemas, y/o Ingeniería de Seguridad y Auditoria informática. Colegiado

Acreditación:

La formación académica, se acreditará con copia simple de Título profesional y/o técnico y/o constancias, certificados, u otros documentos, según corresponda. La formación académica será verificada por el comité de selección 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 link: 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 link: http://www.titulosinstitutos.pe/, según corresponda. En caso de que el ingeniero y/o técnico no se encuentren inscritos en el referido registro, el portor debería presentar el original del Título profesional y técnico, según corresponda.

Capacitaciones:

UN (01) JEFE DE PROYECTO

- Certificación oficial en PMP vigente.
- Certificación Oficial en Ciber Seguridad.
- Certificación en ITIL oficial.

DOS (02) ESPECIALISTAS PARA GESTION DE INCIDENTES Y MONITOREO

- Certificación Profesional en Operaciones de Seguridad emitida por el fabricante de la solución de Protección de Red ofertada.
- Certificación oficial en Ciberseguridad emitida por el fabricante de la solución de Protección de Red ofertada.
- Certificación oficial como analista de vulnerabilidades emitida por el fabricante de la solución de Análisis de Vulnerabilidades ofertada.
- Certificación oficial en ITIL Foundation vigente.
- Certificación o constancia de curso en Ethical Hacking emitida por una entidad internacional de certificación, como: Mile2 y/o ECCouncil y/o Ofensive Security.

Acreditación:

Se deberá acreditar con la presentación de copia simple de las constancias de estudios y/o certificaciones.

Experiencia del Personal Clave:

Requisitos:

UN (01) JEFE DE PROYECTO

Experiencia mínima de cinco (05) años brindando servicio jefe y/o supervisor de proyectos iguales o similares a Servicio Gestionado de Administración, Monitoreo y Soporte de Protección de Red.

DOS (02) ESPECIALISTAS PARA GESTION DE INCIDENTES Y MONITOREO

Experiencia mínima de cinco (05) años brindando servicio de implementación, administración, Monitoreo y Soporte de Protección de Red mediante proyectos de servicios gestionados de soluciones de seguridad informática de Protección de Red.

Acreditación:

El postor debe señalar la denominación del puesto, cargo y/o posición, y tiempo de experiencia del personal clave propuesto (años, meses y días), adjuntando en su oferta, copia simple de cualquiera de los siguientes documentos: (i) contratos y su respectiva conformidad; (ii) constancias; (iii) certificados; o (iv) cualquier otra documentación que, de manera fehaciente, demuestre la experiencia del personal propuesto.

Estos documentos deben señalar los nombres y apellidos del personal clave; el cargo desempeñado indicando el día, mes y año de inicio y culminación; el nombre de la entidad u organización que emite el documento; la fecha de emisión y nombres y apellidos de quien suscribe el documento.

En caso los documentos que acreditan la experiencia establezcan esta en meses sin especificar los días se debe considerar el mes completo. Se considera aquella experiencia que no tenga una antigüedad mayor a veinticinco años anteriores a la fecha de la presentación de ofertas. De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo de la misma solo se considera una vez el periodo traslapado. En ningún caso corresponde exigir que el mismo personal clave acredite experiencia en más de un cargo.

3.5 Seguros (No aplica)

3.6 Lugar y plazo de prestación del servicio

3.6.1 Lugar.

El lugar de ejecución del servicio será dentro de las instalaciones del Fondo

Intangible solidario de salud sito en Calle 41 N° 840 Urb. Corpac, San Isidro – Lima.

El Servicio se realizará de manera remota, y de ser requerido se solicitará asistencia de soporte técnico en sitio.

3.6.2 Plazo

El plazo para la implementación del servicio será de hasta 15 días calendarios, que será coordinado por el Especialista en Soporte Técnico y Gestión del Centro de Procesamiento de Datos del FISSAL, quien indicará la fecha de inicio para la implementación.

3.7 Entregables/Producto

El contratista debe entregar por mesa de partes de FISSAL lo siguiente:

- Informe técnico, detallando el cumplimiento de las actividades mencionadas, indicando las conclusiones y recomendaciones del caso
- Carta de compromiso para el Soporte Técnico.

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).

IV. OTRAS CONSIDERACIONES PARA LA EJECUCION DE LA PRESTACION

4.1 Confidencialidad

El contratista se obliga a mantener y guardar estricta reserva y absoluta confidencialidad de todos los documentos e información que tenga acceso o sea proporcionada por la Entidad durante la ejecución del servicio.

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 Información del 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 (OBLIGATORIO)

LA ENTIDAD CONTRATANTE se obliga a pagar la contraprestación a EL CONTRATISTA, con MONEDA en soles, en PAGO ÚNICO, 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° 009-2025EF.

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 (OBLIGATORIO)

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 a la siguiente fórmula prevista en el Art. 120 del RLGCE:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{Monto vigente}}{F \times \text{Plazo vigente en días}}$$

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 Aplicables (NO CORRESPONDE)

4.3.5 Responsabilidad por vicios ocultos (OBLIGATORIO).

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 DECLARACION JURADA DE INTERESES (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. CLAUSULA DE CUMPLIMIENTO

"Son causales de resolución de contrato la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad."

VII. GESTION 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.

VIII. 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.

IX. RESOLUCION 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.

X CLAUSULA DE CUMPLIMIENTO

"Son causales de resolución de contrato la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad."

Fissal
Firmado digitalmente por:
DIAZ BAZAN Pepe Hernando
FAU 20546736718 soft
Motivo: Doy fé
Fecha: 27/05/2026 14:06:01-0500

Firmado digitalmente por:
FLORES DOMINGUEZ Victor
Julian FAU 20546736718 soft
Motivo: Doy V° B°
Fecha: 27/05/2026 13:58:55-0500