UE 149 - PROGRAMA DE INVERSIÓN CREACIÓN DE REDES INTEGRADAS DE SALUD

	DENOMINACIÓN	**CÓDIGO**
COMPONENTE	GESTIÓN	**2416127**
PRODUCTO	GESTIÓN ADMINISTRATIVA	**S/N**
ACTIVIDAD	GESTIÓN ADMINISTRATIVA	**S/N**
ACCIÓN DE INVERSION	GESTIÓN ADMINISTRATIVA	**S/N**
CONTRATO DE PRESTAMO	N° 4726/OC-PE (BID)	
NORMA DE CONTRATACIÓN APLICABLE	**Políticas para la Adquisición de Bienes y Obras Financiados por el Banco Interamericano de Desarrollo GN-2349-15**, vigentes desde enero de 2020.	

TÉRMINOS DE REFERENCIA
CONTRATACIÓN DEL SERVICIO DE ACCESO DEDICADO A INTERNET Y SEGURIDAD GESTIONA PARA EL PCRIS

Programa Creación de Redes Integradas de Salud

Firmado digitalmente por CABREJOS BARRAGAN Pio Vladimir FAU 20608664387 soft
Motivo: Doy V° B°
Fecha: 07.05.2024 10:08:06 -05:00

MAYO – 2024

Programa Creación de Redes Integradas de Salud

Firmado digitalmente por QUIROGA PASTOR Ulises Gonzalo FAU 20608664387 soft
Motivo: Doy V° B°
Fecha: 06.05.2024 17:55:23 -05:00

INDICE

TÉRMINOS DE REFERENCIA

CONTRATACIÓN DEL SERVICIO DE ACCESO DEDICADO A INTERNET Y SEGURIDAD GESTIONA PARA EL PCRIS

1. ANTECEDENTES

El 23 de octubre de 2018, el Programa Nacional de Inversiones en Salud (en adelante **PCRIS**) declaró la viabilidad del programa de inversión "Creación de Redes Integradas de Salud" (en adelante **Programa de Inversión o Programa**) con código único de inversiones N° 2416127, cuyo objetivo es lograr un adecuado acceso de la población a servicios de salud oportunos, eficientes y de calidad en el primer nivel de atención, en función a sus necesidades. Para ello, se propone rediseñar y reorganizar las Instituciones Prestadoras de Servicios de Salud (IPRESS) en Redes Integradas de Salud (RIS).

El 13 de marzo de 2019, la República del Perú suscribió con el Banco Interamericano de Desarrollo (en adelante **BID**) y el Banco Internacional de Reconstrucción y Fomento (en adelante **BIRF**), los Contratos de Préstamo N° 4726/OC-PE y N° 8920-PE, respectivamente, cada uno hasta por los citados US$ 125´000,000.00 (Ciento veinticinco millones con 00/100 dólares americanos), destinadas a financiar parcialmente al **Programa de Inversión**, más el aporte local por la suma de US$ 65'650,000.00 (Sesenta y cinco millones seiscientos cincuenta mil con 00/100 dólares americanos), haciendo un total de US$ 315´650,000.00 (Trecientos quince millones seiscientos cincuenta mil con 00/100 dólares americanos).

Mediante Decreto Supremo N° 203-2021-EF publicado el 14 de agosto de 2021, se dispuso que la Unidad Ejecutora del **Programa de Inversión** fuese el Ministerio de Salud (en adelante **MINSA**). Después, mediante Resolución Ministerial N° 1015-2021/MINSA de fecha 20 de agosto de 2021, el **MINSA** encargó al **PCRIS** la ejecución del **Programa de Inversión**, en tanto se cree una nueva Unidad Ejecutora.

Luego, mediante Oficio Nº 728-2021-EF/52.04 del 20 de agosto del 2021, la Dirección General del Tesoro Público del Ministerio de Economía y Finanzas remitió al Despacho Viceministerial de Prestaciones y Aseguramiento en Salud (en adelante **DVMPAS**) del **MINSA** una copia de las enmiendas a los citados contratos, debidamente suscritos, las mismas que establecieron que el **MINSA**, a través del Programa de Inversión "Creación de Redes Integradas de Salud" (en adelante **PCRIS),** será el Organismo Ejecutor del Programa. Las funciones del **PCRIS** en su rol de unidad ejecutora, se especificarán en el Manual Operativo del Programa.

Mediante la Resolución Ministerial N° 1177-2021/MINSA de fecha 18 de octubre de 2021 se formalizó, entre otros aspectos, la creación de la Unidad Ejecutora N° 149 - Programa de Inversión "Creación de Redes Integradas de Salud" en el pliego 011. Ministerio de Salud, la misma que se encuentra vinculada al **DVMPAS** del **MINSA.**

Mediante la Resolución de Coordinación General N° 001-2022-PCRIS-CG de fecha 4 de enero de 2022 se aprobó el Manual Operativo del **PCRIS** vigente, en concordancia con los Contratos de Préstamo N° 4726/OC-PE y N° 8920-PE, sus enmiendas y la normativa nacional aplicable.

Para el cumplimiento de objetivos del **PCRIS** se plantea mejorar la capacidad resolutiva de la oferta asistencial actual, fortalecer los sistemas de información y comunicaciones, potenciar los servicios médicos de apoyo y optimizar la cadena de suministro.

En este marco, se requiere la contratación de **CONTRATACIÓN DEL SERVICIO DE ACCESO DEDICADO A INTERNET Y SEGURIDAD GESTIONA PARA EL PCRIS**, esta contratación se efectuará bajo políticas del BID

2. ÁREA USUARIA

Coordinación Administrativa Financiera.

3. OBJETIVOS DE LA CONTRATACIÓN

Objetivo general

Realizar la Contratación de una persona jurídica para que brinde el SERVICIO DE ACCESO DEDICADO A INTERNET y SEGURIDAD GESTIONADA, a fin de asegurar el óptimo desarrollo de las actividades y el cumplimiento de los objetivos propuestos en el Programa Creación de Redes Integradas de Salud – PCRIS hacia internet.

Objetivo específico:

- Acceso a internet para el desarrollo de las actividades diarias de los usuarios del PCRIS
- Contar con Seguridad perimetral gestionada asegurando la confidencialidad, integridad y disponibilidad de la Información a través de la administración de equipos de Seguridad.

4. ALCANCE Y ENFOQUE

1. Característica y condición del Servicio:

1.1. Servicio de Internet

a. El servicio de acceso a Internet provisto debe estar configurado como mínimo a una velocidad 400 Mbps debidamente garantizado, con un grado de concentración del servicio de 1:1 en el tramo local e internacional.
b. El proveedor deberá demostrar técnicamente que el tramo local es un enlace simétrico y dedicado 100%, sin utilizar esquemas de acceso compartido acceso del tipo asimétrico.
c. El backbone de la red local del proveedor debe ser en Fibra Óptica.
d. El backbone de la red local del proveedor deberá ser redundante y se deberá contar con ruta (enlace) de contingencia en la salida internacional (demostrados 2 salidas diferentes, sea red propia o subcontratando a terceros cada uno con la velocidad de 400 Mbps)
e. Permitir el transporte de voz, datos y video sobre el Protocolo IP.
f. Capacidad de Monitorear el nivel de uso del ancho de banda a través de su centro de gestión.
g. Poseer servidores DNS redundantes y distribuidos en locales distintos.
h. Poseer NOC (Network Operations Center) propio acreditable o mediante documento que describa el nivel de servicio y/o disponibilidad de servicio que la entidad espera de su proveedor y/o los niveles de escalamiento para la atención del servicio de internet.
i. Disponibilidad de Crecimiento Asegurada del ancho de banda.
j. El servicio deberá estar disponible y operativo las 24 horas del día durante el tiempo de duración del contrato.
k. El proveedor deberá instalar todos los equipos nuevos y en primer uso los dispositivos y/o componentes necesarios para la puesta en funcionamiento del servicio sin que esto implique costo adicional para PCRIS.
l. El proveedor deberá proporcionar un pool de IP Públicas, como mínimo cuatro (04) IPs.
m. Como parte del Servicio, el proveedor deberá considerar el equipamiento necesario hasta el ingreso al Puerto del Firewall de PCRIS.
n. El nivel de disponibilidad del servicio deberá ser de 99.0%, medido mes a mes,

durante el tiempo de duración del contrato.

o. El proveedor puede ser miembro activo, formal e integrante de Asociación NAP Perú, además de poseer conexión activa y directa al NAP Perú con infraestructura propia. Esto deberá de ser acreditado mediante Constancia o Certificado. En caso no sea miembro, deberá presentar Constancia de Proveedores que tengan punto de acceso de intercambio a través de un miembro activo.
p. El proveedor del Servicio deberá garantizar que el ancho de banda contratado para el enlace deberá ser de uso exclusivo para la Entidad, desde el puerto WAN del router en el local de PCRIS hasta el router de borde del Proveedor del servicio de Internet Nacional.
q. El Servicio deberá considerar la gestión y mantenimiento de los equipos de acceso a Internet instalados por el proveedor.
r. Soporte técnico 24x7x365 con un tiempo máximo de respuesta menor a las 4 horas luego de generado la avería.
s. El proveedor debe contar con doble salida internacional a Internet. Esto deberá de ser acreditado mediante Declaración Jurada.
t. El protocolo de transporte del Backbone del proveedor debe ser MPLS o superior.
u. El proveedor deberá permitir un crecimiento de un ancho de banda en múltiplos de 1Mbps.
v. El proveedor deberá proveer una herramienta de monitoreo del consumo vía web, la cual muestre la información en línea del consumo del ancho de banda real del enlace la cual permita un acceso seguro (HTTPS) y autenticación del usuario. La herramienta de monitoreo debe permitir realizar el reporte de estadísticas de uso, que contemple el volumen de tráfico mensual, semanal y anual.

1.2. Seguridad Gestionada

1.2.1. Descripción:

a. Como parte del servicio, se deberá incluir una solución de protección de redes con características de Next Generación Firewall (NGFW) para la seguridad de la información perimetral de la entidad que incluye filtro de paquetes, control de aplicaciones, administración de ancho de banda (QoS), VPN IPSec y SSL, IPS, prevención contra amenazas de virus, spyware y malware, así como controles de transmisión de datos y acceso a internet componiendo una plataforma de seguridad integrada y robusta. Para ello el equipo cumplir con las siguientes características:
b. Arrendamiento de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red empresarial.
c. La solución consta de 01 appliance nuevo de primer uso, sin EOL ni EOS anunciados
d. El fabricante debe pertenecer al cuadrante de líderes de Gartner para “Enterprise Network Firewall” o “Firewalls de Redes Empresariales” En los últimos reportes desde el 2017 en adelante, considerando que aún no se genera el reporte del 2022
e. El fabricante debe estar catalogado como líder en el último informe de Forrester Wave Enterprise Firewalls
f. El fabricante deberá tener una efectividad de seguridad mayor o igual al 97% según el último reporte de NSS Labs para Next Generation Firewall.
g. La plataforma propuesta por el fabricante debe contar con certificación USGv6 para trabajar IPv6 tanto en Firewall como en IPS.
h. La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7.
i. Los equipos NGFW deberán tener soporte vigente de fabrica durante la fecha de contrato del servicio, el soporte del fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware.

j. Como parte de la propuesta, se deberá proporcionar el acceso a una herramienta que permita evaluar el nivel de adopción de buenas prácticas de configuración en el Next Generation Firewall implementado, con la finalidad de mejorar la postura de seguridad de red proporcionada por la solución.

1.2.2. Capacidad:

a. Throughput de Next Generation Firewall de 2.2Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño). No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.
b. Throughput de Prevención de Amenazas de 0.9 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, control de amenazas avanzadas de día cero (Sandboxing), Filtro de Archivos, y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el nivel o modo más alto de inspección. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido por la Entidad cuando se vayan habilitando los módulos de seguridad indicados en el modo más alto de inspección. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.
c. No se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, se deberá comprobar el requerimiento de throughput con documentación pública del fabricante adjuntando el link que lo respalde.
d. El equipo debe soportar como mínimo 200.000 sesiones simultaneas y 37.000 nuevas sesiones por segundo, medidos con paquetes HTTP de 1 byte.
e. Disco de estado sólido interno de 120 GB o superior.
f. Mínimo ocho (08) interfaces de red 10/100/1000 en cobre, formato RJ45 para tráfico de datos de la red, las mismas que deberán estar habilitadas.
g. Mínimo una (01) interfaz de consola RJ45,
h. El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.
i. Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).
j. Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Descifrado SSL/TLS y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), OSPFv3, QoS, DHCPv6 Relay, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones.
k. Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP.
l. Permitir NAT de destino basado en dominio en lugar de IP. El equipo deberá ser capaz de balancear el tráfico entrante por esa regla de NAT de destino.
m. Soportar DNS Dinámico en las interfaces de red del equipo de seguridad.
n. Soportar túneles GRE como punto inicio o finalización del túnel.
o. Capacidad de inspeccionar el contenido en túneles GRE, GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el equipo de seguridad sea el punto final del túnel.

1.2.3. Funcionalidades de firewall

a. Control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones grupos

estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en sus atributos) y categorías de aplicaciones.
b. Deberá ser posible la identificación de la aplicación y la inspección de malware, spyware y exploits dentro del tráfico cifrado por los protocolos en mención.
c. Permitir el agendamiento de las políticas de seguridad.
d. Debe ser posible especificar en las reglas de seguridad un grupo de objetos basados en IP y/o URL que se alimenten dinámicamente de una fuente externa.
e. Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método.
f. Permitir añadir un comentario de auditoría cada vez que se cree o se edite la política de seguridad. Cada comentario deberá estar asociado a la versión de la política editada. Esto con el fin de garantizar buenas prácticas de documentación, organización y auditoria.
g. Debe permitir realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules).

1.2.4. Descifrado de tráfico SSL/TSL

a. Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos.
b. Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall.
c. Debe ser capaz de inspección el tráfico cifrado, incluyendo el protocolo TLS 1.3.
d. Debe tener la capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos e inseguros.
e. Debe contar con un dashboard de reportes y logs dedicados a monitorear el tráfico de descifrado SSL/TLS, este dashboard deberá estar disponible en la interfaz gráfica, con el objetivo de identificar rápidamente problemas relacionados con las técnicas de descifrado de tráfico, el mismo debe tener varios estados de troubleshooting y proveer de las herramientas a los administradores para encontrar rápidamente las causas por las cuales se puede producir una falla en la descifrado del tráfico (por ejemplo, informar sobre certificados expirados, claves de cifrado débiles, certificados revocados, cierre de la conexión por parte del cliente, entre otros).

1.2.5. Control de aplicaciones

a. Reconocer por lo menos 3000 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email.
b. Debe procesar e inspeccionar aplicaciones que utilicen HTTP/2
c. Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.
d. Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de expresiones regulares, firmas u otro mecanismo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389.
e. Debe poder identificar y crear políticas de seguridad basadas en aplicaciones de Sistemas de Infraestructura Crítica (ICS) como addp, bacnet, modbus, dnp3, coap, dlms, iccp, iec-60870-5-104, mms-ics, rockwell, siemens, entre otros.
f. Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado.
g. Con el objetivo de identificar aplicaciones propietarias a nivel de capa 7, la solución debe permitir nativamente la creación de aplicaciones personalizadas desde la interfaz de gestión, sin la necesidad de acción por parte del fabricante.
h. Debe ser posible la creación de grupos estáticos de aplicaciones y grupos

dinámicos de aplicaciones basados en sus atributos.

i. Debe contar con un módulo de optimización de políticas, que identifique las aplicaciones que han pasado sobre políticas basadas en puertos o de Capa 4, indicando consumo en Bytes, Hits y Fechas de visualización. Este módulo deberá facilitar la migración de la política de Capa 4 a una política de Capa 7 a través de un wizard.

1.2.6. Prevención de amenazas conocidas

a. Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.
b. Las funcionalidades de IPS, Antivirus y Antispyware/Antibot deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones debido a caducidad de soporte con el fabricante.
c. El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.
d. Las firmas deberán estar basadas en patrones del malware y no únicamente en hashes, con el objetivo de detectar malware polimórfico que pertenezca a una misma familia.
e. Debe sincronizar las firmas de seguridad cuando el Firewall se implementa en alta disponibilidad.
f. Debe identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que el Firewall pueda bloquear dichas consultas DNS.
g. Los eventos deben identificar el país que origino la amenaza.
h. Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.
i. Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: HTTP, HTTPS, HTTP/2, FTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3; tanto en IPv4 como en IPv6, para todos los protocolos en mención.

1.2.7. Análisis de malware de día cero

a. La solución propuesta debe incluir mecanismos de detección de amenazas de día cero, incluyendo una plataforma Sandboxing.
b. La plataforma de Sandboxing deberá ser ofrecido en Nube (Cloud). Como mínimo se requiere que el Sandbox propuesto pueda detectar el malware de día cero en un tiempo no mayor a 5 minutos utilizando la emulación completa de malware en entornos Windows, Linux, Android y Mac (este tiempo de análisis se debe cumplir de manera paralela para todos los archivos enviados al Sandbox, considerando análisis dinámico completo, es decir, no incluye Firmas o Prefiltros)
c. Deberá tener una disponibilidad del servicio de al menos 99.9% contabilizados mensualmente.
d. Deberá ser un servicio propio del fabricante, no se aceptarán plataformas que tercericen el servicio de Sandboxing con entidades terceras.
e. El Next Generation Firewall deberá ser capaz de actualizar las firmas de malware en tiempo real, con el objetivo de tener información de malware detectado a nivel global por el fabricante.
f. El Next Generation Firewall debe ser capaz de enviar al sandbox de manera automática los archivos sospechosos que se propaguen por los protocolos HTTP, HTTPS, HTTP/2, FTP, SMTP, POP3, IMAP y SMB, tanto en IPv4 como en IPv6.
g. Debe permitir al administrador la descarga del archivo original analizado por el Sandbox.
h. Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de

administración.

i. Deberá soportar el análisis de archivos ejecutables (EXE), DLLs, ELF (Linux), archivos comprimidos (ZIP, 7ZIP, RAR) archivos office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), archivos de tipos script (.vbs, .ps1, .js), email link, flash, archivos de MacOS (mach-o, dmg, pkg) y Android APKs en el ambiente controlado.

j. Permitir la subida de archivos al sandbox de forma manual y via API

1.2.8. Filtro de contenido web

a. Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora)
b. Deberá incluir la capacidad de creación de políticas basadas en la visibilidad e identificar el usuario que accede a una URL a través de la integración con servicios de directorio, autenticación vía Active Directory, LDAP en general y base de datos local.
c. Debe soportar un cache local de URLs en el appliance, evitando el delay de comunicación/validación de las URLs
d. Debe poseer al menos 70 categorías de URLs, incluyendo las de malware y phishing.
e. Debe permitir la creación de categorías personalizadas.
f. Debe contar con multi categorías de URL, que permita que un sitio web pertenezca a dos categorías distintas.
g. Debe identificar y categorizar los dominios nuevos, menores a 30 días de antigüedad.
h. Debe permitir la customización de la página de bloqueo.
i. Permitir la inserción o modificación de valores en la cabecera HTTP del tráfico de aplicaciones SaaS que pasen por el equipo de seguridad.
j. Debe permitir notificar al usuario, mostrándole solo una página de alerta, pero permitiéndole continuar la navegación al site.
k. Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío

1.2.9. Protección avanzada de DNS

a. El servicio de protección de DNS debe alimentarse de telemetría provista por clientes a nivel mundial y más de 30 fuentes de inteligencia de amenazas de terceros.
b. La solución debe ser capaz de predecir y detener dominios maliciosos de malware basados en algoritmos de generación de dominio (DGA).
c. Debe utilizar machine learning y/o inteligencia artificial para detectar nuevos dominios nunca vistos autogenerados por algoritmos DGA
d. Debe poseer políticas para bloquear dominios DGA o interrumpir las consultar de DNS a dichos dominios.
e. Debe ayudar a contener ataques emergentes basados en DNS, que utilicen técnicas de tunelizacion lenta sobre tráfico DNS, técnicas de entradas de DNS pendientes y adquisición de subdominios
f. Debe ser capaz de predecir nuevos dominios maliciosos inmediatamente luego de su registro, antes de que puedan ser utilizados en ataques
g. Debe detectar e interrumpir robo de datos ocultos o tunelizados en tráfico DNS
h. Debe analizar las consultas de DNS, incluyendo las tasas de consultas y patrones, entropía y frecuencia de n-grams para detectar posibles intentos de tunelización.
i. Debe bloquear resoluciones de DNS que usen técnicas de SNI Spoofing utilizadas para eludir los controles de descifrado.

1.2.10. Identificación de usuarios

a. Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de

autenticación vía LDAP, Active Directory, E- Novell Directory, Exchange y base de datos local.

b. Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente.
c. Debe poder identificar la IP y el usuario de Dominio en base a Event Viewer y WMI.
d. Debe poder monitorear eventos de login y logout del Active Directory utilizando el protocolo WinRM.
e. Debe soportar la recepción de eventos de autenticación de Controladores Wireless con 802.1x, Soluciones NAC y Proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API para la identificación de direcciones IP y usuarios.
f. Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación.
g. Debe permitir la definición de grupos dinámicos de usuarios.

1.2.11. Filtro de datos

a. Los archivos deben ser identificados por extensión y firmas.
b. Permite identificar y opcionalmente prevenir la transferencia (subida o bajada) de varios tipos de archivos (incluidos MS Office, PDF, PE, APK, Flash, DLL, BAT, CAB, PIF, REG, archivos comprimidos en RAR, ZIP u otro) identificados sobre aplicaciones.
c. Permitir identificar y opcionalmente prevenir la transferencia de información sensible basados en el contenido del archivo, incluyendo, más no limitando al número de tarjetas de crédito; y permitiendo la creación de nuevos tipos de datos vía expresión regular.

1.2.12. VPN

a. Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL.
b. La VPN IPSec debe soportar como mínimo:
c. DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard)
d. Autenticación MD5, SHA-1, SHA-2;
e. Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;
f. Algoritmo Internet Key Exchange (IKEv1 & IKEv2);
g. Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.
h. Las VPN client-to-site deben poder operar usando el protocolo IPSec o SSL y permitir la conexión por medio de agente instalado en el sistema operativo.
i. Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA).
j. Debe permitir los siguientes tipos de conexión del cliente al túnel VPN:
k. Antes del usuario se autentique en la estación;
l. Después de la autenticación del usuario en la estación usando Single Sign On (SSO);
m. Bajo demanda del usuario;
n. El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10, MacOS X, Linux., y debe permitir la conexión desde equipos PC, laptop, equipo móvil.
o. Debe contar con un dashboard gráfico que permita monitorear a los usuarios conectados por VPN.

1.2.13. Consola de administración y monitoreo

a. Con la finalidad de no degradar el performance de procesamiento de red y seguridad del Next Generation Firewall, la administración del equipo, gestión de

reportes y gestión de logs deben contar con recursos dedicados de CPU, Memoria RAM y Disco Duro, ya sea integrado dentro del mismo appliance u otro appliance independiente del mismo fabricante

b. Permitir exportar las reglas de seguridad en formato CSV y PDF
c. Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad del tráfico malicioso, actividad de los usuarios VPN. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad.
d. Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables.
e. Debe permitir el monitoreo de eventos basados en SNMP, integración con SIEM a través de Syslog, y envío de alertas por correo electrónico (integrándose a un servidor SMTP).
f. Debe permitir la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizo, su IP y el horario de la alteración;
g. Debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema.
h. Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.
i. La plataforma de seguridad debe permitir realizar tareas de gestión a través del API basado en XML

1.3. Solución de Mitigación anti-ataques de DDoS:

1.3.1. Arquitectura

a. El contratista debe contar con una solución de protección contra ataques DDoS/DoS a través de un entorno en nube perteneciente a su propia red e infraestructura.
b. No se aceptarán soluciones en las que la protección DDoS sea una funcionalidad adicional de equipos firewall, NGFW, ADC y/o Routers.
c. Servicio en la nube Anti-DDoS, proporcionados a través de la protección basada en el rendimiento del tráfico limpio bajo demanda

1.3.2. Características Básicas El "tráfico limpio" se define como el tráfico que no se origina en ataques DoS o DDoS. El tráfico identificado como ataques no puede caracterizarse como tráfico limpio.

a. La protección en nube debe garantizar una capacidad de mitigación e inspección de tráfico de al menos 2 Gbps.
b. El servicio debe proporcionar protección DDoS para las capas 3 (tres), 4 (cuatro) y 7 (siete).
c. El servicio debe proteger al menos los siguientes protocolos: FTP, HTTP, HTTPS, POP3, SMTP, SNMP, DNS, PNT.

1.3.3. Funcionalidades y Operación: El servicio debe contar con los mecanismos necesarios para mitigar los ataques DDoS, ya sea en base a volumen, a protocolos de red (capas 3 y 4) ya nivel de aplicación básica (capa 7), considerando al menos la siguiente lista (no exhaustiva).

a. Inundación SYN
b. Inundación ACK
c. Inundación UDP

d. Inundación ICMP
e. Inundación nula del indicador TCP
f. Inundación HTTP
g. Inundación HTTPS
h. Inundación de consultas de DNS
i. Inundación FIN/RST
j. Inundación de conexión
k. Mal uso de TCP
l. Fragmento TCP
m. Fragmento UDP
n. Ataques de amplificación: DNS, PNT, SSDP, SNMP
o. Low-Slow, como Slowloris y Slow Read
p. SYN+UDP o ICMP+UDP (mixto)
q. DNS mal formado;
r. Trama ICMP incorrecta;
s. Suma de comprobación ICMP incorrecta;
t. Frame ICMP demasiado grande;
u. Longitud del encabezado demasiado corta;
v. Suma de comprobación de TCP incorrecta;
w. Indicadores de TCP defectuosos;
x. Ataques de reflexión. El contratista deberá brindar mensualmente un informe técnico con las estadísticas sobre las amenazas y/o ataques mitigados por la solución; esta información deberá ser enviada al siguiente correo institucional de soporte@pcris.gob.pe.

1.4. Administrador de Ancho De Banda

1.4.1. Se requiere un (01) administrador de ancho de banda de propósito específico de hardware tipo appliance que incluya las siguientes características como mínimo:

a. Un equipo dedicado a la funcionalidad de gestionar ancho de banda, este componente o función no deberá estar embebida sobre enrutadores, firewalls, NGFW, UTM entre otras.
b. Deberá contar con al menos 3,000 aplicaciones identificadas.
c. El equipo deberá contar con almacenamiento interno de por lo menos 100GB
d. El equipo deberá soportar como mínimo 750,000 de flujos concurrentes, 300,000 paquetes por segundo, así mismo, el equipo estará dimensionado para soportar hasta 1Gbps de ancho de banda y deberá contar con las siguientes interfaces 2 bridges RJ45, es decir 4 puertos RJ45 (10/100/1000), con bypass interno que impida la interrupción ante eventos de falla por energía 2 puertos de administración RJ45, un puerto serial RJ45, 2 puertos USB 3.0
e. Deberá estar licenciado para poder gestionar 250Mbps de throughput simétrico inicialmente con capacidad de poder incrementar (con licenciamiento adicional) a de hasta 1Gbps.
f. La solución deberá proveer la funcionalidad de Calidad de Servicio (QoS) para proteger el ancho de banda de aplicaciones críticas y contener el tráfico no deseado tanto en IPv4 e IPv6.
g. Las políticas o reglas de control de ancho de banda deben permitir: priorización de tráfico, definir un mínimo ancho de banda garantizado y un máximo de ancho de banda permitido.
h. Deberá contar con la funcionalidad de distribución de tráfico equitativo, la cual reparte el ancho banda por igual entre todos los dispositivos conectados. Este cálculo de repartición se realiza de forma dinámica constantemente, no es un valor estático y podrá ejecutarse para el tráfico excedente luego de que se haya priorizado las aplicaciones críticas de la Entidad.

i. Posibilidad de crear múltiples políticas de control independientes entre sí, para las distintas áreas de la Entidad
j. Deberá soportar la creación de políticas basadas en tiempo. Los periodos se pueden configurar de acuerdo a las necesidades de la Entidad.
k. La solución deberá integrarse con mínimamente 2 Directorios Activos (AD) de la Entidad con la finalidad de manejar políticas basadas en usuarios.
l. Permitir la creación de aplicaciones personalizadas de la propia Entidad para su visibilidad y control. Estas aplicaciones se podrán crear a través de IP y/o puerto y/o url.
m. Deberá agrupar aplicaciones en categorías existentes y/o personalizadas como: Redes Sociales, P2P, Actualizaciones de Software, Video y Música, entre otros.
n. Monitoreo en tiempo real con actualizaciones de como mínimo 5 segundos, que permita realizar un análisis de tráfico en profundidad hasta la búsqueda de una estación de trabajo y un servicio específico, para el diagnóstico de problemas y cuellos de botella en la red.
o. Deberá permitir el envío de alarmas por medio de email y por traps (snmp)
p. El sistema debe soportar la exportación de información a aplicaciones de colección externa a través de NetFlow, donde el puerto de envío UDP sea configurable
q. Deberá permitir la generación reportes basados en gráficos en los cuales se muestre el consumo por IP, subred, aplicaciones, usuarios (requiere integración con el Directorio Activo).
r. La solución deberá mostrar estadísticas del tráfico de descarga y de subida en un periodo de tiempo configurable
s. La solución deberá ser capaz de mostrar la geografía del tráfico, es decir contra que países se está realizando el intercambio de datos. Así como soportar la creación de políticas que permitan bloquear el tráfico desde o hacia uno o varios países.
t. La solución debe contar con un dashboard que muestre en tiempo real y en simultáneo distintos gráficos de indicadores del comportamiento y consumo de la red. Estos indicadores (tráfico total, aplicaciones de mayor consumo, ip internas o usuarios de mayor consumo, ip externas de mayor consumo, entre otros) deben mostrarse en simultáneo con actualizaciones de al menos cada 5 segundos.
u. El equipo deberá detectar y mostrar anomalías en la red correspondientes a diversos tipos de ataques, generando alertas y permitiendo la ejecución de acciones que minimicen su impacto.
v. El equipo debe garantizar el almacenamiento de datos en su disco duro de por lo menos los últimos 12 meses, independiente de la presencia de un sistema de colección externa, para la posterior generación de reportes y estadísticas.
w. Deberá considerar una consola de administración gráfica en el mismo equipo que permita administrar, configurar y generar reportes del equipo Administrador de Ancho de Banda. Se deberá poder mostrar información de reportes al menos de los últimos 12 meses.
x. El equipo debe poseer un puerto de gestión específico para la administración del sistema. No permitiéndose su administración a través de las interfaces que procesan el tráfico de red del usuario.
y. La Entidad deberá contar con acceso de lectura al equipo (4 usuarios) para la obtención de reportes en cualquier momento. Estos usuarios serán distintos a los que tendrá el proveedor del servicio.
z. Capacidad de limitar el acceso a la consola de Gestión del equipo para un grupo estático de direcciones IP, previniendo el acceso no autorizado al equipo.
aa. La solución deberá poder conectarse con el servidor de actualizaciones del fabricante para que pueda descargar e instalar las actualizaciones remotamente. De esta forma se garantizará que el equipo siempre se encuentre actualizado con la última versión publicada por el fabricante.

bb. El equipo deberá ser nuevo, de primer uso, con garantía del fabricante, sin EOL y EOS anunciados.
cc. Garantía del fabricante por el HW a través de RMA (Return Merchandise Authorization, Autorización de Devolución de Mercadería) por el tiempo que dure el contrato.
dd. El reemplazo por RMA de partes o hardware cubre únicamente en caso de fallas del equipo. No cuando se deba a fallas eléctricas, ni uso impropio, accidentes, abuso, fuego o desastres naturales. El proveedor se encargará del proceso del RMA en caso fuese necesario. Este proceso de RMA no deberá ser mayor a 45 días calendarios contados a partir de que el cliente entregue el equipo averiado al proveedor.

1.5. Otros

a. El servicio debe incluir certificado digital SSL para servidores

- Los certificados digitales deberán ser de la siguiente forma:
  - Sello del sitio web de confianza que emite el certificado, donde una autoridad acreditada garantiza la identidad del propietario del certificado.
  - Autenticación y verificación completa de dominio e identidad de la institución como el propietario del certificado, evitando la suplantación de la identidad.
  - Cifrado de la información confidencial durante las transacciones en línea, evitando que la información sensible sea interceptada y/o alterada.
  - El servicio debe incluir:
    - Certificado Digital SSL para Servidor
    - Tipo: Wildcard
    - Cantidad: ilimitado
    - Validez: 1 año.
    - Estándar X.509 v3
    - Algoritmo de cifrado mínimo: SHA256.
    - Soporta: TLS 1.0, 1.1 y 1.2
    - Deberá asegurar nombres de dominio o subdominios adicionales.
    - Debe incluir certificación de dominio e identidad de la organización.
    - Nivel de Cifrado: Hasta 256 bits de encriptación.
    - Extended Validation: Si
    - Barra verde visible: Si
    - Debe incluir sello de confianza online del proveedor.
    - Soporte de OCSP (online certifícate Status protocol) y CRL.
    - Soporte IDN (Internacional Domain names).
    - Reediciones gratuitas ilimitadas todo el tiempo contratado.
    - Compatibilidad con el 99.9% de navegadores (IE, Mozilla, Chrome, Opera, etc.).
    - Garantía de 12 meses ó 1 año para el servicio.
    - Certificado emitido por Root certifícate Authority – CA Raíz reconocido mundialmente
    - Soporte e instalación gratuitos

1.6. Responsabilidades

a. El proveedor del servicio deberá contar con sus propios recursos de equipos y productos que estimen necesario para la prestación del servicio.
b. El proveedor deberá garantizar la operatividad de los equipos instalados, si alguno de ellos presenta fallas deberá efectuar la revisión del mismo en un plazo no mayor de dos (02) horas de reportado el incidente, luego de superado dicho plazo el proveedor deberá informar el estado del equipo, de persistir el incidente, el equipo deberá ser cambiado y/o reemplazado por un equipo de similares o superiores características en un plazo no mayor de 24 horas.
c. En caso de cambio de sede u lugar de instalación inicial dentro del periodo de contrato, el proveedor asumirá a todo costo el traslado del servicio.
d. El caso de ser necesario realizar obras civiles dentro o fuera de local del PCRIS para la instalación del servicio requerido, estos deberán ser realizados por el Proveedor del servicio.
e. El pool de direcciones IP actual de PCRIS deberá mantenerse si es que tuviesen asignados.

2. Capacitación

El PROVEEDOR deberá brindar cuarenta (40) horas durante el período del servicio, para dictar capacitación por el fabricante en las herramientas de seguridad propuestas, así como capacitación para curso el Certified Information Security Manager, ambos cursos para dos (02) personas, la capacitación podrá ser de manera presencial o virtual previa coordinación con el área usuaria.
Finalizado la capacitación, EL PROVEEDOR deberá otorgar constancias y/o certificados al personal capacitado.

3. Actividades del Servicio

El plazo de entrega del servicio total será de cuarenta (40) días calendario como máximo, contados a partir del día siguiente de suscrito el contrato y/o orden de servicio.

4.1 Al inicio del servicio:

a. Plan de Trabajo:

El plazo de entrega del Plan de Trabajo es dentro de los tres (03) días calendario siguientes de la firma del contrato, debiendo contar como mínimo con los siguiente:
- Etapa de planeamiento (Objetivos, fechas tentativas de ejecución de pruebas, riesgos identificados y las acciones de respuesta, otros que el proveedor considere).
- Etapa de levantamiento de información.
- Etapa de capacitación.
- Etapa de documentación de resultados obtenidos.
- Etapa de entrega y configuración de Equipos.

Este Plan de Trabajo deberá ser aprobado por el Equipo de Tecnologías de la Información y Comunicación.

b. Informe final de la implementación del servicio:

El plazo de entrega del Informe Final es de tres (03) días calendario, contabilizados a partir del día siguiente de la firma del acta fin de la implementación del servicio, con los siguientes documentos:
- Informe técnico final referente al servicio, se firmará un acta de inicio por ambas partes.

- Acta de Activación servicio habilitado, firmada por el especialista de Informática y Jefe de Proyecto del Contratista
- Documento de niveles de escalamiento, en el cual se precise por cada nivel de escalamiento los siguientes datos: contacto, número de teléfono fijo y celular.
- Acuerdo de confidencialidad.
- Cada informe o documentación debe presentarse en formato digital adjuntando los documentos sustentatorios.

4.2 <u>Durante el servicio:</u>

Para los pagos mensuales, el PROVEEDOR deberá hacer presentar el entregable mensual del servicio, el mismo que debe presentar lo siguiente:

- Registro de interrupciones y/o averías con el servicio (Fecha y Hora de Inicio, incidencia y/o avería, diagnóstico, solución, fecha y hora de culminación).
- Reporte mensual de incidencias en temas de seguridad de la información y acciones ejecutadas.
- Reporte de estado del servicio contratado.
- Reporte de Eventos y vulnerabilidades a nivel técnico y analítico.

5. REQUISISTOS DEL PROVEDOR

Requisitos:

- Autorización o Registro del Ministerio de Transporte y Comunicaciones (MTC) para brindar los servicios de internet y transmisión de datos o Registro de Empresas prestadoras de Servicios de Valor Añadido, acreditado con copia simple del documento en la cual se acredite que cuenta con la autorización del Ministerio de Transportes y Comunicaciones (Certificado de Registro de Empresas prestadoras de Servicios de Valor Añadido).
- No encontrarse impedido para contratar con el Estado, según lo dispuesto en el Artículo 11º de la Ley Nº 30225 “Ley de Contrataciones del Estado”.
- El postor debe acreditar un monto facturado acumulado equivalente a S/. 250,000 por la contratación de servicios similares al objeto de la convocatoria y/o en la actividad, durante un periodo de 8 años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.
  Se consideran servicios similares a los siguientes:
  - Servicio de internet.
  - Servicio de Seguridad Gestionada Virtual.g
  - Servicio de Acceso dedicado a internet.
  - Servicio de Backbone a internet.
  - Servicio Internet y Enlace de datos.
  - Servicio de transmisión de datos a Internet.
  - Instalación y/o implementación y/o gestión de firewall y/o gestión y/o soporte técnico de firewall o de firewall de siguiente generación o de equipos de seguridad perimetral.
  - Servicio de Gestión de Seguridad Informática.

Acreditación:

Mediante la presentación de cualquiera de los siguientes documentos: (i) copia simple de contratos u orden de servicio y su respectiva conformidad y/o constancia de prestación o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia solicitada.

6. PLAZO DE ENTREGA Y EJECUCIÓN DEL SERVICIO

El plazo de entrega del servicio será de cuarenta (40) días calendario como máximo, contados a partir del día siguiente de suscrito el contrato y/o orden de servicio.

El plazo de ejecución del servicio será de doce (12) meses como máximo, contados a partir de la firma del acta de activación del servicio.

La activación del servicio se refiere a la instalación y puesta en funcionamiento del servicio.

7. FORMA DE PAGO

El pago se efectuará en una UNICA armada, luego de la firma del acta activación del servicio, previa presentación del comprobante de pago, y la conformidad del servicio.

Para tal efecto, el proveedor deberá adjuntar en el anexo correspondiente el número de su Código de cuenta Interbancaria (CCI) y el banco al que pertenece.

8. COORDINACIÓN, SUPERVISIÓN Y CONFORMIDAD

El supervisor del servicio será el responsable del Equipo de Tecnologías de la Información.

La conformidad será otorgada por la Coordinación Administrativa Financiera, previo informe del responsable de Tecnologías de la Información.

La entidad debe pagar las contraprestaciones pactadas a favor del contratista dentro de los quince (15) días calendario siguientes de la conformidad de los bienes, siempre que se verifiquen las condiciones establecidas en el contrato y/ o orden de compra.

9. PENALIDADES

Penalidad por mora en la ejecución de la prestación del servicio: En caso de retraso injustificado en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso, hasta por un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente, o, de ser el caso del ítem que debió ejecutarse. Esta penalidad será deducida de los pagos a realizarse. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente formula:

$$\text{Penalidad diaria} = \frac{\textbf{0.10 x monto}}{\textbf{F x plazo en días}}$$

Donde F tiene los siguientes valores:

- Para plazos menores o iguales a sesenta (60) días, para bienes y servicios: F=0.40
- Para plazos mayores a sesenta (60) días, para bienes y servicios: F = 0.25

Tanto el monto como el plazo se refieren, según corresponda al monto vigente del contrato o ítem que debió ejecutarse o, en caso de que estos involucran obligaciones de ejecución periódica o entregas parciales, a la presentación individual que fuera materia de retraso.

10. RESPONSABILIDAD DEL PROVEEDOR Y SUBCONTRATACIÓN

El proveedor es responsable por errores, deficiencias, calidad ofrecida y/o vicios ocultos, por un plazo no menor de un (1) años contados a partir de la conformidad otorgada por el PCRIS. La Entidad, no asumirá ninguna responsabilidad por las obligaciones que por Ley corresponde al contratista que prestará el servicio.

11. DERECHOS DE PROPIEDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN

El PROVEEDOR acepta que en la medida de que la prestación es por encargo, y el costo es asumido por el PCRIS; todo producto o materiales (impresos, estudios, informes, gráficos, programas, software de computación u otros), que se genere por la prestación, es de propiedad del PCRIS, no constituyéndose títulos de propiedad, derechos de autor y otro tipo de derechos para el PROVEEDOR; el mismo que a mérito de los presente documento, cede en forma exclusiva y gratuita, sin generar retribución adicional a lo estipulado en el presente documento.

Asimismo, durante la vigencia de la prestación y dentro de los dos (2) años siguientes a su término, el PROVEEDOR no podrá revelar ninguna información confidencial o de propiedad del PCRIS relacionada con la prestación, con el contrato que se generé o las actividades u operaciones del PCRIS. Toda la información a la que el PROVEEDOR tuviere acceso, durante o después de la ejecución de la prestación, tendrán carácter confidencial, quedando expresamente prohibido su divulgación a terceros por parte del PROVEEDOR, a menos que el PCRIS otorgue mediante pronunciamiento escrito la autorización correspondiente.

12. CONFLICTO DE INTERÉS, ELEGIBILIDAD Y PRÁCTICAS PROHIBIDAS

Para efectos de la decisión de participar en el proceso de selección y/o aceptación de la contratación, los candidatos deberán tener en cuenta las causales de conflicto de interés, las condiciones de elegibilidad y las acciones que constituyen prácticas prohibidas establecidas en las **Políticas para la Selección y Contratación de Consultores Financiados por el BID, GN-2350-15**, (párr. 1.11 - 1.13 y 1.23), las cuales podrán ser consultadas en el link:

https://idbdocs.iadb.org/wsdocs/getdocument.aspx?docnum=EZSHARE-1132444900-23304