Contraloría General de la República

PROYECTO MEJORAMIENTO DEL SISTEMA NACIONAL DE CONTROL PARA UNA GESTIÓN PÚBLICA EFICAZ E INTEGRA

	NOMBRE	CÓDIGO
COMPONENTE	CONSOLIDACIÓN DEL PROCESO DE DESCONCENTRACIÓN DEL SISTEMA NACIONAL DE CONTROL.	**1**
PRODUCTO	CGR CON NUEVO EQUIPAMIENTO TIC A NIVEL DESCONCENTRADO	**1.5**
PROYECTO DE UNIDAD ORGÁNICA	FORTALECIMIENTO TIC A NIVEL DESCONCENTRADO	

ESPECIFICACIONES TÉCNICAS

ADQUISICIÓN DE EQUIPAMIENTO INFORMÁTICO PARA LA CONTRALORÍA GENERAL DE LA REPÚBLICA:

SOLUCIÓN DE BALANCEADOR Y SEGURIDAD PARA LA PROTECCIÓN DE APLICACIONES WEB

1. Introducción
2. Antecedentes
3. Objetivo
4. Características de los bienes a adquirir
5. Consideraciones Generales
6. Soporte y Garantía
7. Lugar de entrega
8. Plazo de entrega
9. Garantía
10. Conformidad
11. Forma de pago
12. Confidencialidad

MARZO 2019

ESPECIFICACIONES TÉCNICAS PARA LA ADQUISICIÓN E IMPLEMENTACIÓN DE UNA SOLUCIÓN DE BALANCEADOR Y SEGURIDAD PARA LA PROTECCIÓN DE APLICACIONES WEB

1. INTRODUCCIÓN

La Contraloría General de la República (la Entidad) es el ente rector del Sistema Nacional de Control, dotado de autonomía administrativa, funcional, económica y financiera, que tiene por misión dirigir y supervisar con eficiencia y eficacia el control gubernamental, para lo cual aplica las tecnologías de la Información para optimizar sus procesos de gestión institucional y brindar un mejor servicio. Dentro de este contexto, se requiere adquirir una Solución de Balanceador y Seguridad para la protección de las Aplicaciones Web, con el propósito de mantener la disponibilidad y proteger las diversas aplicaciones web de la infraestructura tecnológica de la entidad, de esta manera se estaría reduciendo el riesgo de ataques informáticos de acceso no autorizados y la disponibilidad de los servicios. Lo cual contribuirá con la seguridad informática, continuidad de sus operaciones y en su labor de fiscalización y lucha contra la corrupción.

2. ANTECEDENTES

El 12 noviembre de 2013 se firmó el Contrato Préstamo N° 2969/OC-PE entre la República del Perú y el Banco Interamericano de Desarrollo (BID) para financiar el proyecto “Mejoramiento del Sistema Nacional de Control para una Gestión Pública Eficaz e Integra”, el mismo que está diseñado para incrementar la eficiencia del Sistema Nacional de Control para contribuir a una mayor eficiencia e integridad de la gestión pública.

El proyecto completa la ejecución de los siguientes componentes:

- Componente 1. Consolidación del proceso de desconcentración del Sistema Nacional de Control.
- Componente 2. Apoyo a la mejora del desempeño de la gestión pública.
- Componente 3. Optimización de los procesos de control.
- Componente 4. Promoción de los Sistemas de Control Interno.

El objetivo del Componente 1 es dotar a la Entidad de las capacidades técnicas, marco operativo y recursos necesarios para acompañar el proceso de descentralización en Perú y dar respuesta efectiva a la creciente demanda de control a nivel nacional.

En el marco de las actividades de “Fortalecimiento TIC” que es parte del proyecto “Mejoramiento del Sistema Nacional de Control para una Gestión Pública Eficaz e Integra”, se hace necesaria la adquisición de hardware, software y licencias que permitan a la Subgerencia de Operaciones y Plataforma Tecnológica de la Gerencia

de Tecnologías de la Información (GTI) organizar, dirigir y ejecutar las actividades relacionadas con la tecnología de la información, la disponibilidad de servicios y aplicaciones de TI, la operatividad de los equipos de procesamiento de información y el buen funcionamiento de la red de transmisión de comunicaciones que soporte los procesos de la institución.

Actualmente la Contraloría General de la República cuenta con equipos de seguridad para la protección y disponibilidad de las aplicaciones informáticas (no se cuenta con el soporte vigente de esos equipos debido que son de fabricación antigua), lo que constituye un servicio de vital importancia para las operaciones de la institución, la relación de equipos se señala en la Tabla N° 01:

Producto	Equipo	#	N° de Serie	Fecha Adquisición	Fecha de Fin de Soporte[1]
Repositorio de Logs del Firewall de Aplicaciones Web	FORTIANALYZER-1000C	1	FL-1KC3R12600097	19/12/2012	16/10/2018
Firewall de Aplicaciones Web	FORTIWEB-1000C	1	FV-1KC3R12700076	19/12/2012	16/10/2018
Firewall de Aplicaciones Web	FORTIWEB-1000C	1	FV-1KC3R13700043	07/07/2011	16/10/2018
Balanceador de carga	BIG-IP C112	1	F5-UIWO-VQUL	01/10/2014	15/11/2018
Balanceados de carga	BIG-IP C112	1	F5-IGPX-TBQZ	01/10/2014	15/11/2018

Tabla N° 01: Relación de Equipos Firewall de Aplicaciones Web, Balanceador y Repositorio de Logs.

Cabe mencionar que hay varias aplicaciones y servicios son de acceso público, por lo que mantener la integridad y disponibilidad de la información de estos servicios constituyen un alto riesgo para la institución; por ello se propone contar con soluciones que den soporte a la disponibilidad y brinden la seguridad informática en el acceso de las aplicaciones.

3. OBJETIVO

Adquisición de una solución de Balanceador y Seguridad para la protección de Aplicaciones Web, esto permitirá la disponibilidad del servicio y la protección de las aplicaciones web de la infraestructura tecnológica de la Entidad reduciendo los riesgos a los cuales están expuestas con respecto a los ciberataques informáticos.

4. CARACTERÍSTICAS DE LOS BIENES A ADQUIRIR

[1] Fecha en la que se vence el soporte de fábrica contratado por la CGR.

4.1. SOLUCIÓN DE BALANCEADOR Y SEGURIDAD PARA LA PROTECCIÓN DE APLICACIONES WEB

4.1.1. Características Generales

- La solución debe contar como mínimo, con los siguientes componentes: Firewall para Aplicaciones Web y Balanceador de Aplicaciones Web las cuales podrían ser de fabricantes independientes.
- La solución debe de soportar un throughput en capa 4 y 7 de al menos 6 Gbps.
- La solución debe soportar al menos 150.000 solicitudes por segundo en capa 7.
- La solución debe soportar al menos 2500 conexiones o transacciones por segundo RSA (SSL- - llaves 2K).
- La solución debe incluir al menos 4 puertos de cobre Gigabit Ethernet.
- La solución debe incluir al menos 2 puertos de fibra óptica multimodo a 10 Gbps.
- La solución debe incluir 1 puertos de cobre Gigabit Ethernet para administración.
- La solución debe tener memoria RAM mínimo de 16GB[2].
- La solución debe tener como mínimo un disco duro de 240 GB, se aceptará también disco de estado sólido (SSD), pero con al menos 240 GB de almacenamiento.
- La solución ser appliance físico rackeable y deberá trabajar en alta disponibilidad y continuidad de los servicios, en cualquiera de las siguientes configuraciones:
    - Activo / Standby
    - Activo / Activo
- Los equipos que formen parte de la solución deben contar con fuentes de energía redundante, estás fuentes no pueden ser alimentadas por PoE.
- El proveedor deberá realizar las actividades necesarias para migrar la configuración actual a la nueva solución.

4.1.2. Características Técnicas del componente balanceador de Aplicaciones de la solución.

- La solución debe permitir el soporte de switching y balanceo en capas L2-L7 para servicios IP.
- La solución debe realizar funciones de balanceo de carga en capas L4-L7 para a todas las aplicaciones basadas en IP (TCP/UDP) soportando como

[2] En caso de ser independientes la solución de balanceo y la solución de firewall de aplicaciones web c/u debe tener como mínimo 16 Gb.

mínimo los protocolos: TCP, UDP, FTP, HTTP, HTTPS, DNS (TCP y UDP), SIP (sobre UDP), RTPS, RADIUS, IMAP, POP, RDP.

- La solución debe permitir la definición de dirección IP y puerto virtual para la prestación de un servicio, que permita atenderlo mediante una granja de servidores identificados mediante una dirección IP y un puerto del servicio igual o diferente del presentado al público.
- La solución debe incluir tecnología full Proxy, control de entrada y salida de conexiones distinguiendo conexiones del lado del cliente y del lado de servidor.
- La solución debe permitir hacer persistencia de conexiones hacia la aplicación con base en cualquier información contenida en cualquier parte del paquete completo, esto para poder adaptar la solución a las necesidades de las diferentes aplicaciones.
- La solución debe permitir hacer control de balanceo del tráfico según se defina con varios tipos de algoritmos especializados de balanceo:

    - Round Robin,
    - Menor número de conexiones,
    - Tiempo de respuesta,
    - Entre otros.

- La solución debe ser capaz de identificar fallos en servicios para redundancia de las aplicaciones.
- La solución debe realizar monitoreo del estado de los Servidores que gestione el equipo de Balanceo de tráfico, por medio de:
    - Ping.
    - Chequeo a nivel de TCP y UDP a puertos específicos.
    - Monitoreo http y https
    - Verificación de la salud de una combinación de servicios, permitiendo tomar la decisión del estado de salud aplicando varios monitores simultáneos.
    - Ejecución de scripts para determinar la respuesta emulando un cliente.
    - Configurar monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red.
    - Monitoreo en línea, donde el funcionamiento de la aplicación determine el estado de salud de la misma.
    - Monitoreo de aplicaciones de mercado:

        - TCP
        - ICMP
        - HTTP/S
        - DNS (TCP and UDP)

        - TFTP
        - SNMP
        - FTP
        - POP3
        - SMTP
        - IMAP
        - NNTP
        - RADIUS
        - SSL
        - LDAP/S
        - ARP
        - RTSP

- Control de las conexiones:
    - Dirección IP origen.
    - Cookies.
    - URL Hash, Header Hash
    - SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia.
    - Sesiones SSL.

- La solución debe permitir crear persistencia por cualquier header de HTTP o campo en el cuerpo del paquete.
- La solución debe garantizar afinidad del servidor, de tal forma que una solicitud de un cliente y cada solicitud posterior se dirijan al mismo servidor de la granja.
- La solución debe soportar un framework de programación para escribir scripts que permitan personalizar la configuración del balanceo de las aplicaciones.
- La solución debe incluir la capacidad de hacer compresión HTTP:

    - Soporte de GZIP y Deflate
    - Compresión tráfico HTTP.
    - Optimización de conexiones a la aplicación.

- La solución debe incluir Cache en RAM para aplicaciones Web.
- La solución debe tener soporte de seguridad SSL:
    - La solución debe incluir el soporte de Aceleración SSL.
    - La solución debe tener la capacidad de soportar al menos 4 Gbps de Throughput SSL.
    - Soporte de llaves SSL de 1024, 2048 y 4096 bits.
- La solución debe tener soporte a las siguientes funciones de seguridad:
    - Network Address Translation (NAT)
    - Limpieza de la cabecera HTTP

    - El equipo deberá permitir la manipulación del contenido de la aplicación para remover o alterar la información enviada al servidor o al cliente
- La solución deberá soportar Calidad de Servicio con reserva de ancho de banda (Rate Shapping) o aplicaciones.
- La solución deberá ser posible aplicar políticas diferentes a cada servidor virtual, permitiendo priorización y reserva de recursos en capa 7.
- La solución deberá ser capaz de abrir un número reducido de conexiones TCP hacia el servidor e insertar los requests HTTP generados por los clientes en estas conexiones ya abiertas, reduciendo la necesidad de establecimiento de nuevas conexiones con los servidores.
- La solución debe contar con los siguientes de niveles de optimización: Cache, Compresión, Multiplexación HTTP, optimización TCP, HTTP/2, SSL Offloading.

4.1.3. Características Técnicas del componente de Seguridad para Aplicaciones Web de la solución.

- La solución deberá ser cualquiera de las siguientes opciones:
  - Integrado dentro del balanceador de carga.
  - Hardware appliance independiente.
- La solución debe permitir, como mínimo, alguno de los siguientes mecanismos de despliegue (implementación):
    - Proxy Reverso.
    - Bridge L2.
- La solución debe permitir la integración y envío de alertas a terceros u herramientas de correlación (SIEM).
- La solución debe soportar el protocolo de gestión de red SNMP y SYSLOG para ser monitoreados por las herramientas de terceros y envíos a correo electrónico de ser requerido.
- La solución debe poder realizar todas sus funciones de aprendizaje, análisis y protección de tráfico web para una capacidad como mínimo 800 Mbps.
- La solución debe reconocer IPs de orígenes maliciosas (como por ejemplo de redes TOR, proxies anónimos, etc.) y también tener catalogación de direcciones IP por Geolocalización.
- La solución debe detectar, alertar y bloquear, en tiempo real, cualquier comportamiento malicioso conocido y/o desconocido.
- La solución debe contar con un modo de aprendizaje que permita definir cuáles son las acciones esperadas y aceptadas para los usuarios.
- El modo aprendizaje, deberá aprender la estructura y elementos de la aplicación y esta información deberá estar disponible para automatizar la configuración de seguridad. Como mínimo debe aprender sobre: Host válidos, URLs, parámetros, cookies, tipo de contenido de los parámetros.

- El modo aprendizaje debe ser capaz de seguir activo aun cuando se encuentra en modo de protección o bloqueo, permitiendo la incorporación de nuevos parámetros o características de los mismos.
- Respecto de algún ataque o alguna otra actividad no autorizada, la solución deberá ser capaz de tomar las acciones adecuadas, como mínimo: Bloquear la dirección IP origen y redirección a página de bloqueo.
- La solución debe contar con un conjunto de patrones correspondientes a los ataques conocidos. Esta base de datos de patrones debe poder actualizarse periódicamente en forma automática y no asistida.
- La solución debe proteger Web Servicies basados en SOAP y XML.
- La solución deber tener la capacidad de recibir y utilizar los certificados y par de llaves público/privadas para los servidores web protegidos.
- La solución debe inspeccionar y monitorear todos los datos HTTP y HTTPS de la aplicación, incluyendo, los encabezados http, campos de formularios, y el cuerpo de las peticiones HTTP y HTTPS.
- La solución debe inspeccionar tanto las peticiones como las respuestas HTTP y HTTPS.
- La solución debe permitir la validación de todos los tipos de datos ingresados, incluyendo URLs, formularios, cookies, cadenas de queries, campos y parámetros ocultos, métodos http, elementos XML y acciones SOAP.
- La solución debe poder identificar y mantener un registro de las sesiones Web a nivel aplicativo, por medio del seguimiento de cookies o parámetros de aplicación.
- La solución debe soportar la detección de herramientas automáticas de descarga, bots, scripts, etc., a fin de poder bloquear todas las consultas que no poseen un navegador real por detrás.
- La solución debe poder Implementar en forma nativa controles anti-scrapping, permitiendo bloquear intentos automatizados de robo de la información del sitio.
- La solución debe poder reconocer IPs de orígenes maliciosas (como por ejemplo de redes TOR, proxies anónimos, etc.) y también tener catalogación de direcciones IP por Geolocalización.
- La solución debe proporcionar protección automatizada para todas las vulnerabilidades expresadas en OWASP Top 10 más recientes (2017 en adelante).
- La solución debe permitir generar excepciones para las políticas de seguridad de validación de protocolo por URL o IP origen.
- La solución debe brindad protección de ataques DDoS en Capa 7.
- La solución debe proteger las aplicaciones Web contra ataques comunes como: SQL Injection, LDAP Injection, OS Commanding, SSI Injection, Remote/Local File Inclusion, Mail Command Injection, XML injection, XPath injection y XQuery injection, Cross Site Scripting (XSS), Cross Site Request

Forgery (CSRF), Web Scrapping, Forceful Browsing y protección de modificación de campos ocultos.

- La solución debe protege la información confidencial, ocultando los campos y cifrando los datos confidenciales en tiempo real.
- La solución debe permitir inspeccionar las conexiones SSL (SSL v3, TLS v1.2 y v1.3) implementadas en los servidores web.
- La solución debe validar que el contenido y longitud del protocolo http, incluyendo los encabezados, cuerpo y cookies sea correcto. A su vez, debe poder restringir los métodos http utilizados en una aplicación Web (GET, POST, PUT, etc.).
- La solución debe realizar una verificación estricta del cumplimiento del protocolo HTTP.
- La solución debe permitir que por cada aplicación Web debe ser posible deshabilitar la prevención de ataques (bloqueo) y dejar habilitado solo la detección (log) de forma granular con el fin de facilitar el troubleshooting por tipos de ataque.
- La solución debe permitir que ante un bloqueo, dependiendo del modo de operación, la respuesta (página) que se le envía al usuario debe tener la posibilidad de personalizarse.
- La solución debe permitir que los hosts o clientes confiables puedan ser excluidos de las medidas de protección.
- La solución debe soportar la identificación de IP origen en caso que este pase por proxy, interpretando el campo X-forwarded-for del encabezado http.
- La solución debe validar que el contenido y longitud del protocolo http, incluyendo los encabezados, cuerpo y cookies sea correcto.

4.1.4. Características de la Consola de Gestión de la solución.

- Esta solución debe ser independiente del hardware de la solución de balanceo y de la solución de firewall de aplicaciones web.
- La consola de gestión de la solución puedes ser un appliance físico o virtual. De ser appliance físico debe de ser del mismo fabricante; de ser virtual puede utilizarse un servidor tradicional y proporcionado por el proveedor.
- En caso de ser appliance virtual, el servidor debería tener las siguientes características:
    - Contar con mínimo 32GB de RAM.
    - 4 Interface de consola (tipo RJ45) para administración.
    - Contar con Discos Duros intercambiable en caliente, redundantes, capacidad mínima de efectiva de 8 TB, configurados en Raid 1 o Raid 5. Además la solución debe contar fuentes de energía redundantes, estás fuentes no pueden ser alimentadas por PoE.

- En caso de appliance físico, la consola de gestión de la solución debe contar con los siguientes requisitos mínimos de hardware:
    - Contar con mínimo 16GB de RAM.
    - 2 Interface de consola (tipo RJ45) para administración.
    - Contar con Discos Duros intercambiable en caliente, redundantes, capacidad mínima de efectiva de 4 TB, configurados en Raid 1 o Raid 5. Además la solución debe contar fuentes de energía redundantes, estás fuentes no pueden ser alimentadas por PoE.
- La solución debe permitir el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH, interfaz de administración gráfica basada en Web seguro (HTTPS)
- La solución deberá de soportar 3 niveles de usuario (Super-user, usuario con permisos reducidos, solo lectura).
- La solución debe de soportar administración vía SNMP (SNMPv1, SNMPv2 y SNMPv3).
- La solución de integrarse con Directorio Activo Windows 2008 r2 o superior, LDAP, RADIUS. Debe incluir los componentes requeridos para la autenticación de administradores/supervisores al equipo.
- La solución debe incluir comunicación cifrada.
- La solución debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante:
    - Protocolo SysLog
    - Notificación vía SMTP
    - SNMP versión.2.0 o superior.
- Los logs del sistema[3] deberán tener la opción de ser almacenados internamente en el sistema o en un servidor externo.
- La solución debe tener la opción de realizar Backup diario de toda la información almacenada en el mismo, incluyendo las configuraciones de todos los balanceadores de carga administrados y transferirlos a un servidor remoto, proporcionado por la Entidad, utilizando protocolo SSH y/o HTTPS.
- Toda la configuración, administración y monitoreo de la solución de balanceadores de carga se efectuará a través de la consola de administración.
- El equipamiento de administración deberá realizar backup diario en forma automática de toda la información almacenada en el mismo, incluyendo las configuraciones de todos los módulos administrados y tener la capacidad de transferirlos automáticamente a un servidor remoto.
- La solución de administración permitirá, como mínimo, lo siguiente:
    - Agregar, eliminar o modificar la configuración en un entorno gráfico.
    - Modificar las reglas de los diferentes equipos.
    - Efectuar la configuración de los componentes de la solución.

[3] Incluye la solución de balanceador, solución de firewall de aplicaciones web y la consola de gestión.

    - Visualizar los registros de auditoria, alertas de seguridad y eventos del sistema.
    - Generar reportes ajustables por el usuario.
- La solución debe permitir la generación de reportes de la actividad registrada en los logs, en los formatos PDF y CSV.
- La solución debe permitir seleccionar la información que se incluirá en los reportes.
- La solución debe tener la capacidad de automatizar la generación de reportes y su posterior remisión por email.

4.2. INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE LOS EQUIPOS Y EL SOFTWARE.

1) El postor debe instalar y licenciar todo lo necesario para dejar la solución completamente habilitada y a entera satisfacción de la Entidad. Esto quiere decir que el proveedor se hará responsable de proporcionar los accesorios (ejemplo: cables UTP, cables poder, conectores, etc.) que se requieran para que dicha solución funcione de acuerdo a lo requerido para el buen funcionamiento de los equipos solicitados.
2) Previo a la implementación, el postor entrega a la Entidad un plan de trabajo, el cual consistirá en el cronograma de las acciones a realizar para la implementación de la solución ofertada, que debe incluir:
    a) Relación detallada del jefe de proyecto y personal especialista, encargados de realizar las actividades de desinstalación de la solución actual (Fortinet y F5) e instalación y configuración de la solución ofertada.
    b) La descripción y configuración final de arquitectura que tendrá la solución ofertada.
    c) Plan de desinstalación de la solución actual (Fortinet y F5): desmontaje de equipos y desinstalación de las políticas, con su respectiva duración en días.
    d) Plan de instalación, configuración y pruebas de la solución ofertada por el proveedor, indicando las actividades a realizar con su respectiva duración en días.
    e) Protocolo de pruebas para validar el cumplimiento de las especificaciones técnicas y la correcta instalación y configuración de la solución, el cual deberá ser aprobado por la Subgerencia de Operaciones y Plataforma Tecnológica de la Gerencia de Tecnologías de la Información de la Entidad o quien haga sus veces.

    El proveedor tendrá un plazo máximo de cinco (05) días calendario, contados a partir del día siguiente de la firma del contrato, para la entrega del plan de trabajo.
3) La implementación debe comprender como mínimo:
    a) Plan de Trabajo.
    b) Suministro de equipos.
    c) Configuración de equipos según los requerimientos indicados.
    d) Trabajos de montaje e instalación de equipos.
    e) Prueba de funcionamiento del Sistema (protocolo de prueba).
    f) Puesta en servicio-prueba.

g) Puesta en servicio-producción.
h) Capacitación al personal de la Entidad en la solución implementada.

4) La configuración que debe tener cada equipo será de acuerdo a las funcionalidades solicitadas en el punto 4.1.
5) Luego de finalizada la implementación de la solución, se ejecutará el protocolo de pruebas. Una vez aprobado el protocolo de pruebas, se firmará un acta de validación de la solución.

4.3. CAPACITACIÓN

1) Se debe incluir curso oficial de administración y configuración de la solución ofertada, de una duración de veinticuatro (24) horas como mínimo.
2) Para tres (03) personas designadas por la Subgerencia de Operaciones y Plataforma Tecnológica de la Gerencia de Tecnologías de la Información o quien haga sus veces.
3) Deberá ser realizada por un instructor que cuente con las certificaciones vigentes en la solución ofertada y autorizado por la marca para el dictado del curso.
4) El Postor debe contar con la infraestructura necesaria para la capacitación.
5) El postor deberá contar físicamente con los equipos, medios didácticos, herramientas, programas y material que se requiera para desarrollar los laboratorios y cumplir con los objetivos del curso.
6) La capacitación se debe realizar en las instalaciones del Postor o local adecuado que lo determine.
7) Antes del inicio de la capacitación, el Postor debe proporcionar los materiales relacionado a los temas a capacitar.
8) Los horarios a realizar la capacitación serán propuestos por el Postor y aprobados por la Subgerencia de Operaciones y Plataforma Tecnológica de la Gerencia de Tecnologías de la Información de la Entidad.
9) Los temas a dictarse deben ser del syllabus oficial de la marca.
10) La capacitación será dentro de los 180 días calendario posterior a la culminación del servicio de instalación (indicado en el punto 4.2).
11) Se deberá entregar certificado de participación, indicando en el certificado el nombre completo del participante, nombre del curso de la solución ofertada, las fechas en las que se realizó la capacitación y el número de horas dictadas.

5. CONSIDERACIONES GENERALES

1) Cada equipo físico perteneciente a la solución será de propiedad de la Contraloría General de la República.
2) Se debe considerar licenciamiento para todos los componentes y funcionalidades requeridas de la solución.
3) El hardware deberá ser certificado por el fabricante.
4) El uso de todos los componentes de la solución debe ser a perpetuidad.
5) La vigencia de los componentes de la solución deberán de ser por el periodo de treinta y seis (36) meses, e iniciará luego que se haya firmado el Acta de Validación de la Solución. Además, deberán encontrarse a nombre de la Entidad.

6) Opcionalmente, el proveedor podrá realizar una visita a las instalaciones4, con el fin de que elabore su propuesta técnica acorde con los requerimientos expresados en el presente documento. Para tal efecto, deberá realizar las coordinaciones necesarias, de lunes a viernes de 09:00 a 12:00 horas, a la dirección de email proporcionada por la Entidad.
7) Todos los bienes que involucren la solución deben ser equipos nuevos sin uso los cuales deben llegar en cajas nuevas a las oficinas de La Contraloría General de la República sin señales de uso anterior y en donde los rótulos permitan identificar las características y la marca respectiva.
8) No se aceptarán equipos reciclados, re ensamblados o re acondicionados, tampoco se aceptarán aquellos que tengan como denominación “refurbished”, “remarketing” o su equivalente comercial.
9) El proveedor deberá entregar las licencias debidamente membretadas por la marca respectiva, así como los CD´s de instalación, si los hubiere.
10) El postor deberá considerar en su propuesta todo el accesorio, drivers, manuales, conectores, cables, etc. requeridos para el buen funcionamiento de los equipos solicitados, bajo la modalidad de “llave en mano”.

5.1. REQUERIMIENTO DEL POSTOR

1) El postor debe acreditar a través de una carta del fabricante, ser partner autorizado y habilitado para la instalación y configuración, así como para la prestación de soporte técnico de los equipos ofertados, que le asegure a la Entidad que se encuentra en condiciones de cumplir con lo estipulado en los numerales 6.1, 6.2 y 6.3.
2) El postor debe acreditar que posee un NOC o un SOC y una mesa de ayuda para poder realizar los servicios especificados en los numerales 6.1, 6.2 y 6.3.
3) Cada postor debe presentar la mejor arquitectura de implementación de la solución en términos de seguridad, calidad y disponibilidad.
4) El postor debe proponer una solución que deberá estar compuesta por todos los componentes necesarios para cumplir con todas las funcionalidades descritas.
5) El postor deberá remitir los números de contacto y la lista de escalamiento para la atención de los problemas en la solución, la cual deberá ser presentada al fin de la implementación.
6) Deberá brindar transferencia de conocimiento mínimo para seis (06) personas en la implementación de la Solución ofertada la cual se realizará en los ambientes de la Entidad, la cual se efectuará dentro de un plazo máximo de treinta (30) días calendarios culminados el servicio de instalación (indicado en el punto 4.2).

5.2. PERSONAL CLAVE PARA CONFIGURACIÓN, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE LA SOLUCIÓN

1) Jefe de proyecto

[4]Cumpliendo las condiciones y políticas de seguridad de la Entidad.

- Debe contar con el título de Ingeniero de Sistemas, Informática o carreras afines, además de titulado, colegiado y habilitado.
- Debe contar con certificación PMP (Project Manager Professional).
- Experiencia laboral mínima de cinco (05) años realizando actividades de Gerente o Jefe de Proyectos de Seguridad de Información.
- Experiencia mínima de tres (03) años en dirección de proyectos de instalación de soluciones de seguridad.

2) Especialistas para la instalación de la solución

- Deben contar como mínimo con el título de técnico o profesional (con el grado de Bachiller) en las especialidades de Sistemas/Informática, Redes y Comunicaciones o carreras afines.
- Debe tener certificación oficial vigente del Fabricante de la solución.
- Experiencia no menor a cuatro (04) años en implementaciones de la solución propuesta. Dicha experiencia se acreditará con documentos que indiquen la participación de este personal en implementaciones similares con el rol requerido.

6. SOPORTE Y GARANTÍA

1) El adjudicatario ganador deberá brindar el servicio de Soporte Técnico remotamente y/o en sitio según el nivel de incidencia que se debe atender a través de su personal especialista en redes propuesto con experiencia de campo, especializado y certificado por el fabricante. Este servicio tiene como finalidad recomendar, supervisar y hasta atender diseños e implementaciones de nuevas características como consecuencia de necesidades de planeamiento futuro, así como analizar aspectos de performance de los equipos ofertados. El servicio de Soporte Técnico estará vigente mientras dure la garantía de los equipos propuestos (36 meses).
2) El adjudicatario ganador deberá ofertar como mínimo la garantía de treinta y seis (36) meses a los equipos propuestos. Para efecto de garantía de equipamiento, se requiere un documento emitido por el fabricante dirigido al concurso. La garantía que el adjudicatario ganador brinde al equipamiento (incluyendo los accesorios que la conforman) entrará en vigencia a partir del acta de conformidad firmada por el responsable designado por la Subgerencia de Operaciones y Plataforma Tecnológica de la Gerencia de Tecnologías de la Información de la Entidad y debe cubrir condiciones, requerimientos, insumo, etc.
3) Se debe incluir un mantenimiento preventivo semestral para los equipos propuestos por el postor, los cuales se encuentren instalados en los locales de la ciudad de Lima, durante los tres años de garantía, el mantenimiento debe incluir la revisión en sitio del estado de los equipos y su diagnóstico. La ejecución del servicio será realizada previa coordinación del personal asignado por la Subgerencia de Operaciones y Plataforma Tecnológica de la Gerencia de Tecnologías de la Información de la Entidad y el encargado de los servicios designado por el postor.
4) Para el servicio de Soporte y Garantía, el Postor deberá contar con un centro de atención de requerimientos de servicios, de reparación o asistencia técnica, de tal manera que le asegure a la Entidad que se encuentra en condiciones de cumplir con los servicios estipulado en las bases durante todo el tiempo de la garantía este

servicio debe estar disponible 24x7x365 deberá indicar número de atención 0800, ofrecer servicios en español. Asimismo, deberá adjuntar en su propuesta el procedimiento de atención de requerimientos.

6.1. Servicio de Soporte gestionado de seguridad

1) El soporte al monitoreo y la administración de seguridad de la solución deberá ser realizado por el postor por un periodo de treinta y seis (36) meses con tiempo de respuesta de 30 minutos.
2) El soporte debe brindar reportes tipo dashboard del monitoreo de seguridad de las plataformas monitorizadas de tal forma que se pueda observar los eventos e incidentes de las plataformas críticas del negocio.
3) El soporte de monitoreo deberá enviar alertas tempranas y hacer un análisis de amenazas y comportamiento inusual de los usuarios de base de datos.
4) El soporte gestionado deberá unificar la recopilación de registros, almacenar y realizar análisis de los registros de los dispositivos monitorizados para brindar indicadores de seguridad.
5) El soporte al monitoreo y administración de seguridad deberá contar con personal especializado en seguridad en un servicio 24 x 7 por el periodo de treinta y seis (36) meses.
6) Se requiere que el soporte gestionado de seguridad cuente con las siguientes características:
   a) Administración remota de la configuración instalada.
   b) Administración de requerimientos.
   c) Administración de incidentes.
   d) Tareas recurrentes de mantenimiento.
   e) Monitoreo de variables correlacionadas.
   f) Reportes semanales y mensuales: informes operativos, gerenciales y de gestión.
   g) Monitoreo de seguridad.
   h) Monitoreo de protección.
   i) Atención de incidentes.
   j) Mantención preventiva.
7) El soporte gestionado de seguridad debe dar respuesta a los incidentes de seguridad asociados a las plataformas monitorizadas, esta respuesta debe estar basada en mejores prácticas de la industria y certificada.
8) El NOC o SOC deben cumplir cabalmente los siguientes objetivos:
   k) Detección oportuna de amenazas de seguridad que estén en proceso de materializarse o se hayan materializado.
   l) Respuesta a incidente que permita mitigar el riesgo al cliente.
   m) Entrega de información de contexto al cliente durante el incidente
   n) Identificación de nuevas amenazas asociadas al ámbito del servicio.
   o) Desarrollo o modificación de reglas de correlación, cambios de configuración en dispositivos y sintonización que permitan la detección.
   p) Análisis de eventos correlacionados.
   q) Validación de eventos positivos.

r) Calificación de severidad.
s) Escalamiento a segundo nivel.
t) Escalamiento a grupo de respuesta a incidente.

9) El soporte gestionado debe brindar soporte in-situ ante requerimientos que demanden esta actividad o incidentes que requieran apoyo en las dependencias de la Entidad.
10) Se requiere que el soporte gestionado de seguridad tenga la capacidad de control, permitiendo la identificación y bloqueo de situaciones de riesgo previamente identificadas.
11) Deberá encargarse de aplicar las actualizaciones de la solución por un periodo de tres (03) años.
12) Deberá incluir el soporte de fábrica 7x24.
13) Para el tiempo de atención del soporte gestionado se contabiliza desde que se notifica al proveedor vía correo electrónico y se genera un ticket de atención correspondiente.

6.2. Servicio de Mantenimiento preventivo

1) Se debe incluir un mantenimiento preventivo semestral solo para los equipos propuesto por el postor, los cuales se encuentren instalados en los locales de la ciudad de Lima, durante los tres años de garantía.
2) Servicio de diagnóstico y reconocimiento del buen funcionamiento (test) de equipo, en cada servicio de mantenimiento.
3) Configuración y/o reconfiguración de los equipos de ser necesario.
4) Actualizaciones del firmware de ser necesario para su operación correcta. Al finalizar la actualización es responsabilidad del postor dejar el equipo 100% operativo.
5) Actualizaciones del sistema operativo (IOS) de ser necesario para su operación correcta. Al finalizar la actualización es responsabilidad del proveedor dejar el equipo 100% operativo.
6) Pruebas del equipo.
7) El horario y días para realizar este mantenimiento, se definirá previa coordinación entre el personal asignado por la Subgerencia de Operaciones y Plataforma Tecnológica de la Gerencia de Tecnologías de la Información de la Entidad y el encargado de los servicios designado por el postor.
8) La empresa deberá generar un reporte de servicio por cada mantenimiento preventivo, el cual deberá reflejar el estado en el que se encuentra el equipo, así como las recomendaciones técnicas correctivas que deberá efectuarse, de ser necesario.
9) El servicio preventivo debe incluir la presentación de un informe semestral de mantenimiento preventivo, a presentar dentro de los siguientes diez (10) días hábiles de finalizado el semestre. Dicho informe debe incluir:
    - Listado de casos atendidos en el periodo, incluyendo fecha y descripción del caso, acción tomada por el proveedor, desempeño de la solución durante el incidente y recomendaciones relacionadas.
    - Listado de actividades relacionadas con la operación de la solución, como, por ejemplo: instalación, reinstalación, actualización y configuración

de firmware o agentes, incluyendo las fechas, descripción, equipos relacionados y recomendaciones.

- Indicadores del estado de funcionamiento de la solución (uso de memoria, uso de cpu, uso de disco duro, entre otros).

6.3. Servicio de Mantenimiento Correctivo

1) Al ocurrir una falla en la implementación o desperfecto en los equipos propuesto, la Entidad comunicará de inmediato al proveedor del servicio y facilitará el acceso al equipo (o los equipos), bajo las condiciones de seguridad establecidas por la Entidad. El proveedor deberá acatar y cumplir en su desempeño con las normas de seguridad establecidas.
2) La atención del servicio será las 24 horas del día, los 07 días de la semana los 365 días del año (24x7x365) mientras dure la garantía de los tres años.
3) Como tiempo de solución, se define al período desde que se genera el requerimiento del servicio por parte de la Entidad, hasta el instante en que el técnico designado por el proveedor deje en forma operativa y funcionando el equipo. Este tiempo no deberá exceder las cuatro (4) horas.
4) La garantía de buen funcionamiento debe incluir el reemplazo de los equipos o partes, por repuestos originales, en caso de fallo, se deberá colocar un equipo de características similares o superiores hasta que se efectúe el RMA correspondiente, esto se deberá de efectuar en un periodo no mayor a 24 horas a partir de la notificación de avería. *Se debe considerar un equipo de reposición en la sede del cliente para garantizar la disponibilidad de la solución*.

7. LUGAR DE ENTREGA

El proveedor deberá entregar la solución en la sede central de la Contraloría General de la República, Edificio Camilo Carrillo N° 114, Jesús María.

8. PLAZO DE ENTREGA

El plazo de entrega máximo será no mayor de sesenta (60) días calendario (contados a partir de la suscripción del Contrato) para la entrega de los equipos y la respectiva configuración.

9. GARANTÍA

La garantía de todos los bienes ofertados será por 36 meses.

10. CONFORMIDAD

Para la emisión de la conformidad deberán haberse cumplido las siguientes acciones:

1) Puesta en servicio de los equipos y software propuesto, de acuerdo a lo indicado en el punto 4.2, para lo cual, en cada caso se procederá con la emisión de actas de

conformidad firmada por la Subgerencia de Operaciones y Plataforma Tecnológica de la Gerencia de Tecnologías de la Información de la Entidad.

2) Protocolo de pruebas realizado satisfactoriamente para cada caso, de acuerdo a lo indicado en el punto 4.2.
3) Informe de diseño de equipamiento instalado en físico y digital.
4) Informe de la configuración de los cada uno de los equipos ofertados, archivos de respaldo de la configuración.
5) Informe del procedimiento y escalamiento de soporte post-venta en físico y digital.
6) Acta de realización de la capacitación al personal de la Entidad.
7) Conformidad Final, firmada por la Subgerencia de Operaciones y Plataforma Tecnológica de la Gerencia de Tecnologías de la Información de la Entidad.

11. FORMA DE PAGO

Se realizará el pago con la siguiente documentación:

- Factura de los bienes
- Guía de remisión
- Actas de Conformidades

12. CONFIDENCIALIDAD

El Contratista se compromete a guardar la más absoluta reserva a fin de garantizar la seguridad de los activos de información pertenecientes a la Contraloría General de la República. Así como también a no violar la confidencialidad, seguridad y propiedad de los archivos, programas y sistemas de aplicación, absteniéndose, sin la respectiva autorización por escrito de la Contraloría General de la República, a efectuar cualquier tipo de cambio, transacción, modificación y adición de información a los archivos, programas y sistemas de aplicación, no pudiendo facilitar a terceros bajo ningún concepto, información alguna. Dicha información comprende, pero no está limitada a:

- Toda información generada sobre la instalación de los bienes ofertados.
- Toda documentación generada para cumplir con los entregables.
- Toda la información generada por los logs de auditoría, tráfico y demás información generada durante el proceso de aprendizaje de la solución, y a la que se tendrá acceso al gestionar la solución.
- Toda la información a la que tendrá acceso durante la ejecución del soporte gestionado.