SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

TÉRMINOS DE REFERENCIA PARA LA CONTRATACIÓN DEL SERVICIO DE SUSCRIPCIÓN DEL SOFTWARE PARA LA GESTION DE DNS, DHCP E IPAM (DDI)

Área usuaria / Área Técnica Estratégica:	Gerencia de Tecnologías de Información
Número de Cuadro Multianual de Necesidades	171
Denominación de la contratación:	Servicio de Suscripción del Software para la Gestión de DNS, DHCP e IPAM (DDI)
Objetivo Estratégico	C1. Optimizar la **infraestructura tecnológica** institucional y el **valor de los datos**

I. FINALIDAD PÚBLICA

El presente proceso tiene como finalidad la contratación del Servicio de Suscripción del Software para la Gestión de DNS, DHCP e IPAM (DDI), los cuales son servicios esenciales para la comunicación y continuidad operativa de las aplicaciones y servicios de TI que son empleadas por las entidades supervisadas y público en general, para el cumplimiento de las funciones y actividades propias de la Superintendencia en beneficio de sus usuarios.

II. DESCRIPCIÓN GENERAL DEL REQUERIMIENTO

Contratación del Servicio de Suscripción del Software para la Gestión de DNS, DHCP e IPAM (DDI). El Servicio será aplicado para la gestión de los Servicios DNS, DHCP e IPAM los cuales son servicios críticos para brindar conectividad y soporte a toda la infraestructura tecnológica y servicios de TI de la Superintendencia.

III. CONDICIONES DE CONTRATACIÓN

a. MODALIDAD DE PAGO

Suma alzada

b. PLAZO DE PRESTACIÓN

b.1 PLAZO DE ENTREGA, INSTALACION, CONFIGURACION Y PUESTA EN FUNCIONAMIENTO DEL SERVICIO DE SUSCRIPCIÓN DEL SOFTWARE PARA LA GESTIÓN DE DNS, DHCP E IPAM (DDI)

El plazo de entrega, instalación, configuración, pruebas de verificación y puesta en funcionamiento será de treinta (30) días calendario a partir del día siguiente de la fecha de suscripción del Acta de Inicio de proyecto entre el Departamento de Soporte Técnico de la Gerencia de Tecnologías de la Información (GTI) y el contratista. Dicha acta será suscrita en un plazo máximo de cinco (05) días calendario, contados a partir del día siguiente del perfeccionamiento del contrato.

.

Al término de la correcta instalación, configuración, pruebas de verificación y puesta en funcionamiento del servicio ofertado se realizará la suscripción del Acta de Conformidad e inicio de servicio.

Como requisito indispensable para la suscripción del Acta de Conformidad e inicio de servicio entre el Departamento de Soporte Técnico de la Gerencia de Tecnologías de la Información (GTI) y el contratista, el contratista debe hacer entrega del documento de Contrato del servicio de suscripción emitido por el fabricante., en referencia al servicio de soporte técnico del fabricante, este deberá especificar el tipo de soporte y periodo contratado con el fabricante para el servicio implementado.

b.2 PLAZO DEL SERVICIO DE SUSCRIPCION

El servicio de Suscripción del Software para la Gestión de DNS, DHCP e IPAM (DDI) así como el servicio de soporte técnico local y del fabricante, será de un (1) año y se contabilizará a partir del día siguiente a la firma del Acta de Conformidad e inicio de servicio.

c. LUGAR DE PRESTACIÓN DE SERVICIO

La instalación, configuración y puesta en funcionamiento del servicio de Suscripción del Software para la Gestión de DNS, DHCP e IPAM (DDI) se realizará previa coordinación con la Gerencia de Tecnologías de Información en la siguiente sede de la Superintendencia:

- Calle Los Laureles N° 214, San Isidro, Lima.

d. PENALIDADES

d.1 PENALIDAD POR MORA:

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable, de conformidad con el artículo 120 del Reglamento.

d.2 OTRAS PENALIDADES:

Adicionalmente a la penalidad por mora, se aplicarán las siguientes penalidades:

Supuesto de aplicación de penalidad	Forma de Cálculo	Procedimiento de Verificación
Retraso en la atención de un incidente	Monto total de la penalidad = 1% UIT, por cada retraso desde el minuto 31 al minuto 40.	De haberse registrado un retraso en la atención de un incidente, la Gerencia de Tecnologías de la Información (GTI) elaborará un informe con el detalle de los tiempos de atención por cada incidente registrada en la herramienta de
	Monto total de la penalidad = 3% UIT, por cada retraso desde el minuto 41 al minuto 50.	

	Monto total de la penalidad = 5% UIT, por cada retraso mayor al minuto 50.	gestión de TI. Se notificará por correo electrónico al contratista en un plazo máximo de cinco (05) días hábiles. El contratista podrá presentar sus descargos dentro de los tres (03) días hábiles siguientes. La entidad evaluará los descargos y emitirá un informe en un plazo máximo de cinco (05) días hábiles
Retraso en la resolución de un incidente	Monto total de la penalidad = 1% UIT, por cada retraso mayor a 6 horas hasta 8 horas.	GTI registrará los tiempos de solución de los incidentes con base a los SLA definidos en la herramienta de gestión de servicios de mesa de ayuda. Se emite un informe y se notificará por correo electrónico al contratista en un plazo máximo de cinco (05) días hábiles. El contratista podrá presentar sus descargos dentro de los tres (03) días hábiles siguientes. La entidad evaluará los descargos y emitirá un informe en un plazo máximo de cinco (05) días hábiles
	Monto total de la penalidad = 3% UIT, por cada retraso mayor a 8 horas hasta 10 horas.	
	Monto total de la penalidad = 5% UIT, por cada retraso mayor a 10 horas.	

Las penalidades en el servicio de soporte serán aplicadas cuando sea responsabilidad del proveedor y de acuerdo con lo estipulado por la normativa aplicable.

El Departamento de Soporte Técnico de la Gerencia de Tecnologías de la Información (GTI) de la Superintendencia emitirá un informe indicando los motivos por los cuales corresponde la aplicación de penalidades, adjuntando los documentos que lo acrediten.

e. SUBCONTRATACIÓN

Se encuentra prohibida la subcontratación de las prestaciones objeto del contrato.

f. SOLUCIÓN DE CONTROVERSIAS CONTRACTUALES

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación, cuando se haya pactado, y arbitraje.

Para el caso de arbitraje, el postor ganador de la buena pro selecciona una de las siguientes
Instituciones Arbitrales para administrarlo:

N.º	INSTITUCIONES ARBITRALES	RUC
1	Centro de Análisis y Resolución de Conflictos de la Pontificia Universidad Católica del Perú	20155945860
2	Centro de Arbitraje del Colegio de Abogados de Lima	20154531921
3	Centro de Conciliación y Arbitraje Nacional e Internacional de la Cámara de Comercio de Lima	20101266819

g. PLAZO PARA RESPUESTAS ENTRE LAS PARTES

Para los plazos de respuesta de las partes sobre aspectos vinculados con la ejecución contractual que no han sido específicamente previstos en el Reglamento, aplica el plazo máximo de respuesta del siguiente cuadro:

Plazo máximo de respuesta	:	7 días calendario

Antes del vencimiento de este plazo máximo, las partes pueden acordar su prórroga para cada situación específica considerando la cláusula de notificaciones del contrato.

IV. TÉRMINOS DE REFERENCIA

4.1. DESCRIPCIÓN DEL SERVICIO A CONTRATAR

Se requiere contratar el servicio de Suscripción del Software para la Gestión de DNS, DHCP e IPAM (DDI) para la Superintendencia siendo responsabilidad del proveedor, realizar la entrega, instalación, configuración y puesta en funcionamiento del servicio ofertado, el software ofertado debe ser compatible con los Servidores DNS y DHCP de la Superintendencia.

El servicio a contratar comprende lo siguiente:

Ítem	*Cantidad*	*Descripción del Servicio*
1	1	Servicio de Suscripción del Software para la Gestión de DNS, DHCP e IPAM (DDI)

4.2. CARACTERISTICAS TÉCNICAS

4.2.1 SOFTWARE PARA LA GESTIÓN DE DNS, DHCP E IPAM (DDI)

Se requiere contratar el Servicio de Suscripción del Software para la Gestión de DNS, DHCP e IPAM (DDI) con las siguientes características:

-Suscripción del Software para la Gestión de los Servicios Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) e IP Address Management (IPAM), comercialmente conocido por sus siglas DDI.
-El Software deberá ser desplegado en la plataforma de virtualización VMware vSphere 6.7 u3 o 8.0 del Centros de Computo Principal y Secundario de la Superintendencia.
-El software ofertado por el contratista, deberá ser de fabricación o versión durante el año 2025, como mínimo. El postor no podrá ofertar un software que esté destinado a perder su vigencia tecnológica y que deje de ser soportado durante los doce (12) meses siguientes a la implementación de los mismos.

-El software deberá integrarse con los servidores DNS y DHCP On-Premise de la Superintendencia (contamos con 4 Servidores en total con S.O Windows Server 2016 donde se ejecutan los servicios DNS y DHCP), en ninguna circunstancia el software reemplazará estos servicios, solo se integrará para una mejor Gestión de estos servicios.
-El software debe soportar como mínimo la gestión de 50 VLAN's, 50 scopes DHCP y 12000 direcciones IP.
-El software debe brindar visibilidad centralizada que consolide las configuraciones de los clusters de DNS-DHCP externos e internos en una interfaz unificada para obtener una visibilidad centralizada.
-El software debe tener un sistema de gestión de redes optimizado para centralizar la planeación y administración del espacio de DNS, DHCP y direcciones IP (IPv4 e IPv6).
-El Software debe tener la capacidad de monitorear de la carga y el rendimiento de los servidores de DNS o DHCP con un dashboard de servidor que detalle el estado del servidor en tiempo real. Este debe incluir estadísticas como la red, la dirección IP, la memoria, y el uso de disco y CPU del servidor.
-El software debe tener la capacidad de monitorear para obtener información visual en tiempo real de las asignaciones de IP, las resoluciones de DNS y los estados de asignación de DHCP.
-El software debe brindar información visual jerárquica que muestre cómo distintos ámbitos se relacionan entre sí dentro de la red. La vista de árbol de ámbitos DHCP deberá permitir a los administradores ubicar y acceder rápidamente a ámbitos y subredes específicos.
-El software debe tener la capacidad de monitoreo y visibilidad detallada de los ámbitos DHCP individuales para espacios de direcciones IPv4 e IPv6., mostrando efectivamente el uso y la disponibilidad de las direcciones IP, y controlar las direcciones reservadas y abandonadas.
- El software debe tener la capacidad de monitoreo y visibilidad de la gestión y uso de direcciones IP, así como el uso de los Servidores DHCP y Servidores DNS
-El software debe tener el control preciso sobre el acceso al DNS con listas de control de acceso. De esta forma permitirá los administradores de redes definir y aplicar permisos específicos para una seguridad mejorada.
-El software debe tener la capacidad de identificar y aislar rápidamente servidores DHCP maliciosos con alertas oportunas por correo electrónico.
- El software debe tener la capacidad de auditoría integrada del uso de los servidores de DNS y DHCP, la auditoría se realizará mediante el historial y registro de eventos, visibilidad centralizada de DNS y DHCP, y reportes y seguimiento (auditoría operativa)
-El software debe permitir evaluar los registros del historial de alquileres para una IP particular con el fin de encontrar las transiciones de IP a lo largo del tiempo, con el objetivo de analizar las dependencias y resolver conflictos para restablecer rápidamente la conectividad.
-El software debe tener la capacidad de analizar patrones en el tráfico de consultas para identificar rápidamente tendencias en el comportamiento de usuarios, dominios populares y posibles áreas de mejora. Debe permitir detectar y abordar problemas al identificar cualquier anomalía o irregularidad en la consulta y los patrones de respuesta y evaluar la demanda de recursos entendiendo la frecuencia y naturaleza de las consultas.
-El software debe tener la capacidad de identificar y analizar patrones en consultas para dominios bloqueados. Esto facilitará la detección de posibles amenazas de seguridad o actividades no autorizadas. Obteniendo información sobre el comportamiento de los usuarios al examinar qué dominios bloqueados son los más consultados.

-El software debe tener un panel (Dashboard) donde se pueda colocar información gráfica importante de los servicios a monitorear, la información debe actualizarse al pasar el tiempo.
-El software debe tener la capacidad de enviar alertas instantáneas para agilizar la resolución de problemas de DHCP y DNS y reducir el tiempo de degradación y/o inactividad.

4.2.2 SOPORTE TECNICO

El proveedor deberá ofertar el servicio de soporte técnico local y del fabricante para el servicio de suscripción del Software para la Gestión de DNS, DHCP e IPAM (DDI).

Asimismo, el proveedor deberá contar con un centro de soporte técnico o similar, bajo el formato 24x7x365, las 24 horas del día durante los 365 días del año durante la vigencia del soporte técnico del fabricante. Este centro de soporte debe contar con personal especializado para la resolución de incidentes bajo servicio de soporte técnico. Para tal fin, se entenderá por avería una interrupción parcial, total y/o degradación del software ofertado bajo soporte técnico.

La Superintendencia podrá reportar una avería telefónicamente o por correo electrónico, considerándose todas estas formas igualmente válidas. Finalizado el reporte de la avería, el centro de soporte deberá proporcionar un código de avería para el posterior seguimiento de la misma. Posteriormente, a solicitud de la Superintendencia, el proveedor deberá proporcionar información del estado de la avería reportada. La Superintendencia deberá contar con acceso prioritario al centro de servicio, para la atención inmediata de las notificaciones de avería.

El tiempo de atención de una avería, no deberá ser mayor de treinta (30) minutos, es decir, el tiempo transcurrido desde que se reporta la avería, hasta que el proveedor responde para iniciar el diagnóstico, brinda el número de ticket de atención e inicia el diagnóstico. El tiempo máximo para la resolución de una avería no deberá ser mayor a seis (06) horas (de lunes a viernes).

Para la resolución de averías reportadas, el personal técnico del proveedor deberá apersonarse a las instalaciones de la Superintendencia, salvo que previamente y por mutuo acuerdo entre el personal técnico de ambas partes (proveedor y Superintendencia), se convenga que dicho soporte sea remoto.

Las atenciones de averías deberán estar disponibles sin límite de horas por intervención, ni cantidad de intervenciones mensuales, dándose por atendido una avería cuando es solucionado en su totalidad y a satisfacción de la Superintendencia.

El servicio de soporte técnico del fabricante deberá incluir las actualizaciones de software bajo el contrato de soporte, cuando estas sean requeridas por la Superintendencia o necesarios para mitigar alguna falla o avería, o para mejora o incorporación de nuevas funcionalidades. Las actualizaciones serán solicitadas al fabricante a través del contratista.

El proveedor deberá proporcionar la información de los contactos respectivos (número de teléfonos y correos electrónicos) y un cuadro de escalamiento comercial, de post-venta y atención de averías. Dicha información deberá ser entregada como requisito para el perfeccionamiento del contrato.

Cada vez que ocurra una avería, y finalizada la atención de esta a satisfacción de la Superintendencia, el proveedor debe entregar un informe técnico detallado en

documento físico o electrónico. El informe se entregará en un plazo no mayor de siete (07) días calendarios, luego de finalizada la atención de la avería. Dicho informe debe contener como mínimo lo siguientes puntos:

- Causas de origen de avería(s).
- Diagnósticos, escalamiento, solución de avería y tiempos empleados.

El servicio de soporte técnico local debe incluir el respaldo del fabricante por el Servicio de Suscripción del Software para la Gestión de DNS, DHCP e IPAM (DDI) y durante el plazo del soporte.

La Superintendencia debe tener acceso al TAC (Centro de Asistencia Técnica) del fabricante para generar casos o tickets de atención. Este acceso debe ser entregado por el proveedor a la SBS, donde figure que la SBS es titular del mismo.

No podrá modificarse los tiempos de respuesta y atención, ni periodicidad, o cualquier otra característica de estos servicios durante el período de duración del soporte técnico, sin consentimiento previo de la Superintendencia.

4.3 ENTREGA, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO

El proveedor será el responsable de la entrega, instalación, configuración y puesta en funcionamiento del Servicio de Suscripción del Software para la Gestión de DNS, DHCP e IPAM (DDI) ofertado, para la cual deberá proveer los recursos necesarios para el correcto funcionamiento del servicio.

El proveedor deberá entregar un Plan de Trabajo, a los cinco (05) días calendario, contabilizados a partir del día siguiente del perfeccionamiento del contrato, donde se indique entre otros puntos:

- Cronograma de los trabajos.
- Listado de personal involucrado (personal clave), datos (nombres completos, DNI, Números telefónicos, correos electrónicos, entre otros) y responsabilidad de cada uno de ellos.

Al finalizar la instalación, configuración y puesta en funcionamiento del Servicio de Suscripción del Software para la Gestión de DNS, DHCP e IPAM (DDI), el proveedor deberá entregar en formato digital mediante correo electrónico al personal de la Superintendencia responsable del proyecto como requisito para la firmar del acta de conformidad e inicio de servicio, los siguientes documentos:

- Procedimientos para el soporte técnico del servicio con sus respectivos niveles de escalamiento y responsables.
- Entregar toda bibliografía (en formato físico o electrónico) considerada necesaria para utilizar el software, actualizada a la última versión y con la obligación permanente, durante la vigencia del soporte del fabricante, de remitir toda modificación.
- Contrato del servicio de soporte del fabricante.

El personal del proveedor deberá contar con seguro contra todo riesgo (SCTR) vigente, e indumentaria adecuada (EPP – Equipos de Protección Personal) al momento de ingresar a cada una de las instalaciones de la Superintendencia durante etapa de instalación, configuración y pruebas del software ofertado.

4.4 CAPACITACIÓN

Capacitación en configuración, administración, monitoreo, auditoria, dashboard, generación de alertas y reportes del Software para la Gestión de DNS, DHCP e IPAM (DDI), el curso deberá realizarse en la modalidad virtual, tendrá una duración mínima de seis (06) horas cronológicas, asimismo deberá ser impartido a cuatro (04) profesionales de la Gerencia de Tecnologías de Información,

El capacitador deberá contar con mínimo dos (2) años de experiencia en en instalación y/o configuración y/o soporte en el Software DDI ofertado. Los documentos que acreditan la experiencia del capacitador deberán presentarse para la suscripción del contrato.

La capacitación deberá ser impartida como máximo dentro de los treinta (30) días calendario de perfeccionado el contrato.

V. PERSONAL CLAVE

El postor deberá contar con el siguiente personal:

V1. PERSONAL CLAVE

a) Un (01) Jefe del Proyecto para las coordinaciones referidas a la implementación del servicio.

Formación académica: ~~Mínimamente~~ Bachiller en Ingeniería: Electrónica o de Telecomunicaciones o de Redes y Comunicaciones, o de Sistemas, o de Industrial

Experiencia: Experiencia mínima de dos (2) años en implementación de proyectos de telecomunicaciones y/o de tecnologías de información, realizando labores de administración, y/o de gestión y/o de supervisión y/o de planificación y/o de coordinación

b) Un (01) técnico especializado en el software DDI ofertado, encargado de la instalación, configuración y soporte.

Formación académica: ~~Mínimamente~~ Bachiller en Ingeniería: Electrónica o de Telecomunicaciones o de Redes y Comunicaciones, o de Sistemas.

Experiencia: Experiencia mínima de dos (2) años en instalación y/o configuración y/o soporte en el Software DDI ofertado.

Certificación: Certificación Profesional vigente del software DDI del fabricante ofertado. Adjuntar copia de la certificación vigente para la firma del contrato.

VI. OTRAS CONSIDERACIONES PARA LA EJECUCIÓN DE LA PRESTACIÓN

6.1 REQUISITOS DEL POSTOR

El postor debe ser un representante autorizado en el Perú para la comercialización del Servicio de Suscripción del Software para la Gestión de DNS, DHCP e IPAM (DDI) ofertado y para brindar el servicio de soporte técnico ofertado. En tal sentido, el postor debe acreditar lo antes señalado mediante:

- Carta del fabricante, que acredite que el postor es representante autorizado por aquel en el Perú para comercializar, brindar soporte y brindar el Servicio de Suscripción del Software para la Gestión de DNS, DHCP e IPAM (DDI) ofertado o;

- Carta del distribuidor oficial que acredite que el postor es representante autorizado para comercializar, brindar soporte y brindar el Servicio de Suscripción del Software para la Gestión de DNS, DHCP e IPAM (DDI). .El postor deberá presentar este documento como requisito para el perfeccionamiento del contrato

6.2 SEGURIDAD DE LA INFORMACIÓN Y CONFIDENCIALIDAD

El contratista, con motivo de la prestación, recibirá de la Superintendencia información de carácter estrictamente confidencial que debe ser utilizada sólo para los fines de ejecución, por ello, será obligación del proveedor mantener total secrecía y confidencialidad respecto a los datos e información de cualquier clase, que la Superintendencia le proporcione, o bien, a la que tenga acceso, con motivo de la prestación y desarrollo de su ejecución.

Adicionalmente, el contratista está obligado a instruir a sus funcionarios o personal que será parte conformante del recurso humano que ejecutará la prestación respecto a la obligación de mantener total secrecía y confidencialidad.

Como parte de la prestación y con relación a la SEGURIDAD DE LA INFORMACION, se adjunta el Anexo N° A.

6.3 CONFORMIDAD DE LA PRESTACIÓN

El área que brindará la conformidad del servicio de suscripción del software DDI mediante un acta de conformidad es el Departamento de Soporte Técnico de la Gerencia de Tecnologías de la Información (GTI).

6.4 PRUEBAS DE PUESTA EN FUNCIONAMIENTO PARA LA CONFORMIDAD DEL SERVICIO

- El contratista, en coordinación con la Superintendencia una vez terminada la instalación, realizarán en forma conjunta los procedimientos de inspección y pruebas sobre el Servicio de Suscripción del Software para la Gestión de DNS, DHCP e IPAM (DDI), de tal forma que le permita establecer que los servicios serán brindados de conformidad con lo solicitado en los presentes términos de referencia y en la propuesta del postor adjudicado.
- Las pruebas deben incluir como mínimo lo siguiente:

  - Pruebas de integración con los Servidores DNS y DHCP.
  - Pruebas de visibilidad, monitoreo y auditoria.
  - Pruebas de Dashboard.
  - Pruebas de Gestión de direcciones IP.
- Cualquier defecto notificado al contratista durante la realización de las pruebas de conformidad, serán inmediatamente rectificadas por éste sin costo alguno, teniendo como plazo máximo cinco (05) días calendarios a partir del día siguiente de su notificación. Las pruebas deberán concluirse al menos tres (03) días calendarios antes de la suscripción del acta de conformidad e inicio del servicio.

VII. FORMA DE PAGO

La Superintendencia deberá realizar el pago a favor del proveedor en pago único y pagos parciales de acuerdo con el siguiente detalle:

-El monto correspondiente a los servicios relacionados a la instalación, configuración, puesta en funcionamiento y la capacitación del Servicio de Suscripción del Software

para la Gestión de DNS, DHCP e IPAM (DDI), se pagará en un solo pago, previa conformidad del Departamento de Soporte Técnico de la Gerencia de Tecnologías de la Información (GTI) mediante el acta de conformidad e inicio de servicio y la recepción de la documentación requerida.

-El monto correspondiente al servicio de Suscripción del Software para la Gestión de DNS, DHCP e IPAM (DDI) y el soporte técnico del local y fabricante, se pagará de manera mensual al culminar el servicio del mes en doce pagos iguales, previa conformidad del Departamento de Soporte Técnico de la Gerencia de Tecnologías de la Información (GTI) mediante el acta de conformidad e inicio de servicio y la recepción de la documentación requerida.

VIII. RESPONSABILIDAD POR VICIOS OCULTOS

El contratista será responsable por la calidad ofrecida y por los vicios ocultos del bien conforme a lo indicado en el artículo 69° de la Ley General de Contrataciones Públicas, por un plazo de un (01) año a partir de la última conformidad otorgada por parte de la Superintendencia.

IX. DEL COMPROMISO Y CUMPLIMIENTO DE LA SEGURIDAD Y DE LA SALUD EN EL TRABAJO

El contratista se compromete a cumplir con todos los alcances y disposiciones establecidos en Ley Nº 29783, Ley de Seguridad y Salud en el Trabajo, en su Reglamento (aprobado por D.S. Nº 005-2012-TR), y en las demás normas vigentes que regulen la Seguridad y Salud en el Trabajo; así como, cumplir y adecuarse con el Reglamento Interno de Seguridad y Salud en el Trabajo de LA SUPERINTENDENCIA y las cláusulas adjuntas en el Anexo B; siendo el incumplimiento de dichas obligaciones causal de resolución contractual, de conformidad con el artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas.

X. REQUISITOS DE CALIFICACIÓN

A. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Requisitos:
El postor debe acreditar un monto facturado acumulado equivalente a dos (2) veces la cuantía de la contratación, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los quince (15) años anteriores a la fecha de la presentación de ofertas que se computa desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de 25% DE LA CUANTÍA DE LA CONTRATACIÓN, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los quince (15) años anteriores a la fecha de la presentación de ofertas que se computa desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.

Se consideran servicios similares los siguientes: Servicios de DNS y DHCP gestionado y/o IPAM independiente y/o automatización y/o gestión de redes y/o servicio de monitoreo de redes.

Acreditación:

La experiencia del postor en la especialidad se acredita con un máximo de veinte (20) contrataciones, mediante 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[1], o comprobantes de retención electrónico emitido por SUNAT por la retención del IGV[2]. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados[3], 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 servicio con conformidad o constancia de prestación.

En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo Nº XX** referido a la Experiencia del Postor en la Especialidad.

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

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso de que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo N° XX.

Las personas jurídicas resultantes de un proceso de reorganización societaria no pueden acreditar como experiencia del postor en la especialidad aquella que le hubieran transmitido como parte de dicha reorganización las personas jurídicas sancionadas con inhabilitación vigente o definitiva.

Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicio o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo Nº XX referido a la Experiencia del Postor en la Especialidad.

Advertencia

En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que ejecutan conjuntamente el objeto del contrato.

[1] El solo sello de cancelado en el comprobante de pago, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación fehaciente de la cancelación. Es válido el sello colocado por el cliente del postor (sea utilizando el término “cancelado” o “pagado”).

[2] De acuerdo con el Régimen de Retenciones del Impuesto General a las Ventas (IGV).

[3] Se entiende “privados” como aquellos que no son entidades contratantes.

B. CAPACIDAD TÉCNICA Y PROFESIONAL

B.1 EXPERIENCIA DEL PERSONAL CLAVE

Requisitos:

01 Jefe de Proyecto

Mínimo dos (2) años de experiencia en implementación de proyectos de telecomunicaciones y/o de tecnologías de información, realizando labores de administración, y/o de gestión y/o de supervisión y/o de planificación y/o de coordinación, del personal clave requerido desempeñándose como jefe de proyecto

01 Técnico especializado

Mínimo dos (2) años de experiencia en instalación y/o configuración y/o soporte en el Software DDI ofertado del personal clave requerido desempeñándose como técnico especializado en Software DDI y/o Servicios de DNS y DHCP gestionado y/o IPAM independiente y/o automatización y/o gestión de redes y/o servicio de monitoreo de redes.

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) en el **Anexo N° XX**, 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.

B.2 CALIFICACIONES DEL PERSONAL CLAVE

B.2.1 Formación académica

01 Jefe de Proyecto

Requisitos:

Bachiller en Ingeniería: Electrónica y/o de Telecomunicaciones y/o de Redes y/o Comunicaciones, y/o de Sistemas y/o Industrial del personal clave requerido como jefe de proyecto.

01 Técnico especializado

Bachiller en ingeniería: Electrónica y/o de Telecomunicaciones y/o de Redes y Comunicaciones, y/o de Sistemas del personal clave requerido como técnico especializado.

Acreditación:

El postor debe señalar los nombres y apellidos, documento de identidad, el nombre de la universidad o institución educativa que expidió el grado de título profesional, y el grado o título profesional obtenido en el **Anexo N° XX**, adjuntando en su oferta copia del grado de bachiller o título profesional. En caso se acredite estudios en el extranjero del personal clave, debe presentarse, adicionalmente, copia simple de la revalidación o reconocimiento del grado o título ante la SUNEDU.

Los evaluadores o la DEC, según corresponda, verifican los grados o títulos profesionales en el Registro Nacional de Grados Académicos y Títulos Profesionales 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 del Ministerio de Educación, a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/ según corresponda.

ANEXO A:

CLÁUSULAS DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

1. SEGURIDAD DE LA INFORMACIÓN

1.1. CONFIDENCIALIDAD

Se califica como confidencial toda la información obtenida, así como los informes y toda clase de documentos que produzca o tenga a su alcance EL CONTRATISTA para la ejecución del presente contrato.

Se entenderá como tal toda información de tipo económica, financiera, legal, contable, técnica, comercial, estratégica o de otro tipo, así como la información proveniente de la función de supervisión, que sea revelada por LA SUPERINTENDENCIA a EL CONTRATISTA, en forma oral, escrita, o por cualquier otro medio o soporte para la realización de la prestación contratada; así como cualquier análisis, recopilación, estudio, resumen, extracto o documentación de todo tipo que elabore o formule EL CONTRATISTA a partir de la Información Confidencial o documentación revelada por LA SUPERINTENDENCIA.

EL CONTRATISTA se obliga a cumplir con el deber de reserva respecto de dicha información, no pudiendo por tanto divulgarla sin autorización expresa de LA SUPERINTENDENCIA. Esta obligación subsistirá aún después de concluida la vigencia del presente contrato por un plazo mínimo de cinco (5) años.

EL CONTRATISTA se compromete a limitar el acceso a la Información Confidencial de forma tal que solo sea accesible a aquellas personas que necesariamente deban involucrarse en las conversaciones, tratativas y/o acuerdos mantenidos con LA SUPERINTENDENCIA.

EL CONTRATISTA responderá legalmente por los daños y perjuicios causados por el incumplimiento al deber de reserva al que se refiere esta cláusula y, para este efecto, suscribe este documento.

1.2. INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN

EL CONTRATISTA se compromete a respetar y aplicar en la prestación que brinde, según correspondan, las políticas, principios, procedimientos, manuales y controles de los sistemas de gestión, metodologías, estándares y otros, referidos a seguridad de la información, establecidos por LA SUPERINTENDENCIA y que declara conocer y aceptar. Asimismo, se compromete a cumplir con la sección “Obligaciones del Contratista”.

Previa evaluación y conformidad de las áreas competentes, LA SUPERINTENDENCIA autorizará los accesos a recursos o herramientas propias de la institución y que sean requeridos por EL CONTRATISTA para la ejecución de la prestación materia del presente contrato. Una vez finalizado el contrato, todos los accesos serán retirados.

EL CONTRATISTA debe tomar medidas de protección de la información de LA SUPERINTENDENCIA que se encuentre almacenada en los equipos y/o dispositivos que requieran mantenimiento fuera o dentro de las instalaciones de LA SUPERINTENDENCIA.

EL CONTRATISTA adoptará las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de la información involucrada. Las medidas de seguridad deben ser apropiadas y acordes con la naturaleza y envergadura de tal información, a fin de evitar cualquier manejo contrario a la prestación contratada, incluyéndose, entre otros, a la adulteración, la alteración, la pérdida, las desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

EL CONTRATISTA deberá reportar a LA SUPERINTENDECIA dentro de las cuarenta y ocho (48) horas siguientes a su ocurrencia, cualquier incidente de seguridad de la información, hallazgo o situaciones sospechosas que puedan poner en riesgo la citada información, relacionada con vulneraciones a la Confidencialidad, Disponibilidad, Integridad o Privacidad de la información de LA SUPERINTENDENCIA, a fin de adoptar, de ser el caso, las coordinaciones y acciones necesarias que correspondan.

EL CONTRATISTA al inicio de la prestación deberá proporcionar al área usuaria la información de los canales de contactos respectivos (números de teléfonos y correos electrónicos) y un procedimiento para el reporte de incidentes de seguridad de la información y ciberseguridad que incluya un cuadro de escalamiento comercial, de post-venta y atención de averías y/o asistencia de soporte técnico.

El CONTRATISTA exime de toda responsabilidad a LA SUPERINTENDENCIA, sus empleados y funcionarios, por cualquier litigio, acción legal o procedimiento administrativo, reclamación o demanda que pudiera derivarse de cualquier trasgresión o supuesta trasgresión de cualquier patente, uso de modelo, diseño registrado, marca registrada, derechos de autor o cualquier otro derecho de propiedad intelectual que estuviese registrado o de alguna otra forma existente a la fecha del contrato debido a la ejecución de la prestación por parte de EL CONTRATISTA o el uso de la misma por parte de LA SUPERINTENDENCIA.

El incumplimiento de lo dispuesto en la presente cláusula de Seguridad de la Información por parte de EL CONTRATISTA constituye causal de resolución del presente contrato[4], y asimismo, dará lugar a la indemnización por daños y perjuicios que le corresponda a LA SUPERINTENDENCIA conforme a ley.

2. PROTECCIÓN DE DATOS PERSONALES

2.1. DEL CUMPLIMIENTO DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES

EL CONTRATISTA declara que se somete a las disposiciones previstas por la Ley de Protección de Datos Personales, su reglamento, directiva y demás normas conexas, complementarias, modificatorias y/o sustitutorias; por lo que los datos personales que se proporcionen, así como aquellos generados o recopilados en el marco del presente contrato serán tratados en forma confidencial y estarán sujetos a estrictas medidas de seguridad, conforme lo dispone la referida normativa.

EL CONTRATISTA en caso corresponda, acepta y reconoce la responsabilidad de sus trabajadores y cualquier personal a su cargo, de mantener permanentemente una absoluta y total reserva y confidencialidad respecto de los datos personales a que tengan acceso en el marco del presente contrato, la que subsistirá en forma permanente e indefinida.

2.2. DEL ENCARGO DEL TRATAMIENTO

[4] *Artículo 164.1° literal a) del Reglamento de la Ley de Contrataciones del Estado.*

En caso EL CONTRATISTA deba proporcionar datos personales de sus colaboradores o terceros para el tratamiento de los datos personales, así como en caso deban generarlos o recopilarlos cuando estos resulten necesarios en el marco del cumplimiento del presente contrato, ello no implicará de modo alguno la transferencia de los mismos, debiendo EL CONTRATISTA asumir en dichos casos, la condición de encargados del tratamiento en el marco de la Ley de Protección de Datos Personales, y de su Reglamento, directiva y demás normas conexas, complementarias, modificatorias y/o sustitutorias.

EL CONTRATISTA declara conocer que asume la condición de encargado del tratamiento cuando corresponda y por tanto se compromete a no utilizar o tratar los datos personales proporcionados, generados o recopilados con una finalidad distinta a aquella por la que le fueron entregados o por la que son generados o recopilados así como a no transferirlos o divulgarlos a terceros, con excepción de entidades públicas, cuando estas lo soliciten en el marco del cumplimiento de sus funciones debidamente sustentadas o el poder judicial cuando sea solicitado mediante la orden judicial correspondiente, debiendo notificar de ello a la otra parte, según corresponda, dentro de las 24 horas de recibido el requerimiento.

En caso EL CONTRATISTA asuma la condición de encargado del tratamiento de los datos personales que se pudieran proporcionar, se comprometen a conservarlos por el plazo de dos (2) años contados desde la culminación de la finalidad del presente contrato.

EL CONTRATISTA en caso corresponda, reconoce y acepta que podrá en cualquier momento, ser auditado por LA SUPERINTENDENCIA sobre las medidas aplicadas, en cumplimiento de la Ley de Protección de Datos Personales, su reglamento, y demás normas conexas. De comprobar LA SUPERINTENDENCIA el incumplimiento de esta cláusula podrá resolver el presente contrato e interponer las acciones legales a que hubiera lugar.

3. OBLIGACIONES DEL CONTRATISTA:

3.1. RESERVA Y USO DE LA INFORMACIÓN

EL CONTRATISTA acepta la obligación de guardar reserva sobre cualquier información de LA SUPERINTENDENCIA a la que haya tenido acceso con ocasión de la ejecución del presente contrato; a no revelar ni permitir la revelación de cualquier detalle a los medios de prensa o a terceros; a no utilizar la información vinculada al contrato con LA SUPERINTENDENCIA o el nombre, logo o cualquier medio que identifique a LA SUPERINTENDENCIA en cualquier promoción, publicidad o anuncio, sin previa autorización escrita de LA SUPERINTENDENCIA, a excepción de aquella información que LA SUPERINTENDENCIA o una autoridad judicial o arbitral autorice o disponga, o cuando se trate de información de dominio público, circunscrito para el uso que LA SUPERINTENDENCIA, autoridad respectiva o las normas vigentes permitan de manera expresa. El incumplimiento de esta obligación puede ser causal de resolución del presente contrato. Asimismo, esta obligación permanecerá vigente no obstante el vencimiento o la terminación del presente contrato, y su incumplimiento podrá conllevar a efectuar las acciones legales que correspondan.

La confidencialidad de la información, a que se refiere el párrafo precedente, alcanza a todo el personal y subcontratistas de EL CONTRATISTA, debiendo así constar en los correspondientes contratos que con estos se celebren.

3.2. FACILIDADES PARA LA INSPECCIÓN O VERIFICACIÓN

EL CONTRATISTA acepta y autoriza a LA SUPERINTENDENCIA para efectuar inspección o verificación en sitio, según la dirección indicada en su propuesta y/o contrato.

EL CONTRATISTA debe facilitar a LA SUPERINTENDENCIA, su(s) representante(s) y/u organismos reguladores o de fiscalización, el acceso a las instalaciones para la provisión de la prestación, en casos de auditorías, investigaciones e inspecciones de verificación de cumplimiento de las condiciones de la prestación. Estos accesos serán informados, autorizados y acordados con LA SUPERINTENDENCIA.

3.3. DEVOLUCIÓN Y ELIMINACIÓN DE LA INFORMACIÓN

Al vencimiento del presente contrato y mientras no se incumpla las condiciones de la prestación5, EL CONTRATISTA debe devolver y eliminar toda la información que le haya sido proporcionada para el cumplimiento de las prestaciones materia del contrato, independientemente del soporte o formato en el que se encuentre almacenada; y, a mantener el compromiso de confidencialidad en forma indefinida, incluso luego de concluido el presente contrato.

EL CONTRATISTA está obligado a proveer evidencia de que dicha eliminación ha sido realizada, de acuerdo con las condiciones de la prestación a satisfacción de LA SUPERINTENDENCIA, en un plazo no mayor a cinco (5) días hábiles contados a partir de la fecha de culminación de contrato.

3.4. DE LA NORMATIVIDAD:

Hasta donde sea aplicable, el contratista deberá considerar las normas, reglamentos y documentación, de acuerdo con las condiciones de la prestación:
Normas Técnicas Peruanas (NTP).
Estándares Internacionales y buenas prácticas.
Recomendaciones del fabricante de los equipos para su normal funcionamiento.
Otros documentos normativos internos dispuestos por la Superintendencia.

3.5. CANALES DE COMUNICACIÓN DE LA SUPERINTENDENCIA PARA RECIBIR REPORTES DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

EL CONTRATISTA deberá reportar a la brevedad posible a LA SUPERINTENDENCIA cualquier incidente de seguridad de la información, hallazgo o situaciones sospechosas que pusieran en riesgo la citada información, relacionada con vulneraciones a la Confidencialidad, Disponibilidad, Integridad o Privacidad de la información de LA SUPERINTENDENCIA, a fin de adoptar, de ser el caso, las coordinaciones y acciones necesarias en el marco de la Gestión de Incidentes de Seguridad de la Información; así como las acciones legales que correspondan.

A través de los canales establecidos para tal fin:

- Incidente de Seguridad Digital: A través del correo mesa-ayuda@sbs.gob.pe o en su defecto al número +51 1 630 9300.
- Incidentes relacionados a Seguridad Física: A través de la cuenta AA-seguridad@sbs.gob.pe o a través de una llamada telefónica al Departamento de Seguridad al +51 1 6309000 anexo 1424 o 1425.

[5] P.e. En caso la prestación sea una capacitación, curso o taller en el cual se requiera mantener los registros de los participantes para mantener la trazabilidad de los certificados emitidos, la eliminación no sería aplicable.

4. FIRMA

El que suscribe, ……, con DNI N° ....., representante legal de la empresa …… (EL CONTRATISTA), con RUC N° ……, y con domicilio legal en ……, provincia y departamento de ……; acepta estas cláusulas.

Lima, …. de ……. de 20XX.

……..……..
XXX
D.N.I. N° XXX
Representante legal de la empresa XXX

ANEXO B

CLAUSULAS CONTRACTUALES REFERIDAS AL COMPROMISO Y CUMPLIMIENTO DE LA SEGURIDAD Y LA SALUD EN EL TRABAJO

1. POLÍTICA DE SEGURIDAD

Es política de la Superintendencia, garantizar la seguridad y la salud en el trabajo de sus trabajadores, contratistas y de terceras personas que se encuentren dentro de los locales de la institución.

La Superintendencia fomenta una cultura de prevención y mitigación de riesgos, a través de un adecuado sistema de gestión de la seguridad y salud en el trabajo, en concordancia con la normatividad pertinente, compromiso que debe asumir el Contratista, como responsable de la prevención de accidentes y enfermedades profesionales en cada una de las áreas donde ejecuten sus prestaciones.

2. OBLIGACIONES DEL CONTRATISTA

Por medio del presente, el contratista se obliga a lo siguiente:

2.1. Asignar a la SBS personal que posea las habilidades y los conocimientos suficientes, adquiridos a través de los programas de capacitación y la propia experiencia acumulada a través de los años.

2.2. Capacitar adecuadamente a su personal respecto de los riesgos a los que está expuesto en función a las características de las labores o actividades que desarrolla y el cargo que ocupa.

2.3. Evaluación de los riesgos de las actividades que efectuará su personal, adoptando las medidas necesarias de control antes del inicio de las actividades.

2.4. Contar con las licencias y/o las certificaciones nacionales y/o extranjeras que sean requeridas y/o necesarias de acuerdo con la normativa vigente, según sea el trabajo o actividad a realizar.

2.5. Prevenir el impacto que sobre el medio ambiente tenga el manejo y la manipulación de residuos, materiales, insumos o sustancias químicas que sean utilizados y/o desechados en las actividades que son materia del presente contrato.

2.6. Cumplir con las reglas de conducta y de seguridad interna que disponga la Superintendencia.

2.7. Dar cumplimiento a la normatividad vigente sobre Seguridad y Salud en el trabajo, que a modo de referencia se mencionan las siguientes:

- Ley N° 29783 y sus modificatorias, Ley de Seguridad y Salud en el Trabajo.
- Decreto Supremo N° 005-2012-TR y sus modificatorias, Reglamento de la Ley N° 29783.
- Ley N° 28048. Ley de protección de la mujer gestante.
- Ley N° 27626, De las empresas especiales de servicios y cooperativas de trabajadores.
- Decreto Supremo N° 009-2004-TR, Reglamento de la Ley N° 28048.
- Resolución Ministerial N° 374-2008-TR, De protección de la mujer gestante.
- Decreto Supremo N° 042-F, Reglamento de Seguridad Industrial.
- Resolución Ministerial N° 480-2008/MINSA, que aprueba la NTS N° 068-MINSA/DGSP-V.1.
- Decreto Supremo N° 003-98-SA, Norma Técnica del Seguro Complementario de Trabajo de Riesgo.
- Decreto Supremo N° 015-2005-SA, Valores permisibles para agentes químicos en el ambiente de trabajo.

- Decreto Supremo N° 022-2001-SA, Reglamento sanitario para las actividades de saneamiento ambiental.
- Decreto Supremo N° 011-2006-Vivienda y sus modificaciones. Reglamento Nacional de Edificaciones.
- Resolución Ministerial N° 449-2001-SA-DM, Norma Sanitaria para trabajos de desinfección, desinsectación, desratización, limpieza de ambientes, de tanques sépticos, etc.
- Resolución Ministerial N° 037-2006-MEM, Código Nacional de Electricidad.
- Resolución Ministerial N° 111- 2013 Reglamento de Seguridad y Salud en el Trabajo de las Actividades Eléctricas
- NTP 400.034, Andamios. Requisitos.
- Norma G.050, Seguridad durante la Construcción.

La relación de normas nacionales descritas anteriormente, es solo referencial y no exime al contratista del cumplimiento de toda la normatividad que le sea aplicable en materia de seguridad y salud, así como todas aquellas normas y lineamientos internos que la Superintendencia ponga en su conocimiento.

2.8. Conocer y difundir a su personal, el Reglamento Interno de Seguridad y Salud en el Trabajo de la Superintendencia, así como todas las medidas para el cuidado de la seguridad y salud en el trabajo dispuestas por esta.

2.9. Contar con los implementos de seguridad adecuados para el tipo de trabajo que se va a realizar.

2.10. Proporcionará a su personal, los equipos de protección y la ropa de trabajo que sea la adecuada para resguardarlo de los potenciales daños por efectos mecánicos, contaminantes, químicos y biológicos, ambientales y/o meteorológicos. De igual forma, deberá controlar el correcto uso de estos elementos así como su calidad.

2.11. Suministrar todo los equipos y herramientas que su personal requiera para el desarrollo y ejecución adecuada de los trabajos o actividades contratados. Los mismos que deberán ser de óptima calidad, de características para su uso y encontrarse en buen estado. Cualquier situación que afecte el funcionamiento y la calidad de estos, deberá ser reemplazado y debe ser puesto en conocimiento inmediato del personal de la Superintendencia.

3. FACULTADES DE LA SUPERINTENDENCIA

La Superintendencia se reserva el derecho de supervisar en cualquier momento los equipos, elementos, sitios de trabajo, personal y documentos que sean necesarios para evaluar el cumplimiento y aplicación de las normas de Seguridad y Salud en el trabajo.

La Superintendencia se reserva el derecho de impedir las labores o actividades del personal del contratista que incumpla los citados procedimientos y normas. En caso esta situación se torne persistente y/o generalizada, la Superintendencia queda facultada a paralizar los trabajos y resolver el contrato sin lugar a reclamo por parte del contratista.

La Superintendencia se reserva el derecho de comunicar a la Autoridad de Trabajo cualquier incumplimiento por parte del contratista relacionado con las Normas de Seguridad y Salud en el Trabajo materia del presente contrato.

El contratista tiene el deber de dar estricto cumplimiento de las normas y disposiciones sobre seguridad y salud en el trabajo.

El incumplimiento de estas obligaciones es causal de resolución de contrato. La SBS se reserva el derecho de solicitar la acreditación sobre el cumplimiento de dichas obligaciones durante la ejecución contractual.

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

ANEXO C:

<table>
<tr><th colspan="7">Formato para identificar, evaluar y asignar riesgos</th></tr>
<tr><td rowspan="3">1</td><td colspan="6">IDENTIFICACIÓN DE LOS RIESGOS</td></tr>
<tr><td colspan="2">RIESGOS EN EL PROCESO DE CONTRATACIÓN (*)</td><td colspan="4">- Falta de proveedores en la interacción con el mercado
- Demora en la respuesta del mercado</td></tr>
<tr><td colspan="2">RIESGOS EN LA EJECUCIÓN DE LA PRESTACIÓN (**)</td><td colspan="4">- Incumplimiento, retrasos en los plazos de entrega y ejecución.
- Deficiencias en la supervisión de la ejecución, falta de seguimiento al contrato, cambio de personal sin autorización.</td></tr>
<tr><td rowspan="14">2</td><td colspan="6">EVALUACIÓN DE LOS RIESGOS</td></tr>
<tr><td colspan="2" rowspan="2">RIESGO IDENTIFICADO</td><td colspan="2" rowspan="2">PROBABILIDAD DE OCURRENCIA</td><td colspan="2" rowspan="2">IMPACTO EN LA EJECUCIÓN DE LA PRESTACIÓN</td></tr>
<tr></tr>
<tr><td colspan="2" rowspan="3">Falta de proveedores en la interacción con el mercado</td><td>Baja</td><td>X</td><td>Baja</td><td>X</td></tr>
<tr><td>Media</td><td></td><td>Media</td><td></td></tr>
<tr><td>Alta</td><td></td><td>Alta</td><td></td></tr>
<tr><td colspan="2" rowspan="3">Demora en la respuesta del mercado</td><td>Baja</td><td></td><td>Baja</td><td></td></tr>
<tr><td>Media</td><td>X</td><td>Media</td><td>X</td></tr>
<tr><td>Alta</td><td></td><td>Alta</td><td></td></tr>
<tr><td colspan="2" rowspan="3">Incumplimiento, retrasos en los plazos de entrega y ejecución</td><td>Baja</td><td></td><td>Baja</td><td></td></tr>
<tr><td>Media</td><td>X</td><td>Media</td><td>X</td></tr>
<tr><td>Alta</td><td></td><td>Alta</td><td></td></tr>
<tr><td colspan="2" rowspan="3">Deficiencias en la supervisión de la ejecución, falta de seguimiento al contrato, cambio de personal sin autorización.</td><td>Baja</td><td></td><td>Baja</td><td></td></tr>
<tr><td>Media</td><td>X</td><td>Media</td><td>X</td></tr>
<tr><td>Alta</td><td></td><td>Alta</td><td></td></tr>
<tr><td rowspan="5">3</td><td colspan="6">ASIGNACIÓN DE LOS RIESGOS</td></tr>
<tr><td colspan="3">Falta de proveedores en la interacción con el mercado</td><td colspan="3">Subgerencia de Logística</td></tr>
<tr><td colspan="3">Demora en la respuesta del mercado</td><td colspan="3">Subgerencia de Logística</td></tr>
<tr><td colspan="3">Incumplimiento, retrasos en los plazos de entrega y ejecución</td><td colspan="3">Contratista.</td></tr>
<tr><td colspan="3">Deficiencias en la supervisión de la ejecución, falta de seguimiento al contrato, cambio de personal sin autorización.</td><td colspan="3">Contratista.</td></tr>
</table>

(*) A identificar por parte de la SL

(**) A identificar por parte del Área usuaria