



## SOLICITUD DE COTIZACIÓN (SDC)

### SDC-41-2022

#### **Adquisición e implementación de una solución de Control de Acceso a la Red (NAC) para el Tribunal Constitucional de la República Dominicana.**

Estimado señor/Estimada señora:

El Programa de las Naciones Unidas para el Desarrollo (PNUD) agradece su cotización para la provisión de bienes, obras y/servicios según se detalla en el Anexo 1 de esta SDC.

Esta Solicitud de Cotización comprende los siguientes documentos:

Sección 1: Esta carta de solicitud

Sección 2: Instrucciones y datos de SDC

Anexo 1: Especificaciones técnicas

Anexo 2: Formulario de presentación de cotizaciones

Anexo 3: Oferta técnica y financiera

Anexo 4: Términos y condiciones

En la preparación de su cotización, guíese por las Instrucciones y los Datos de la SDC. Tenga en cuenta que las cotizaciones deben enviarse utilizando el Anexo 2: Formulario de presentación de cotizaciones y el Anexo 3: Oferta técnica y financiera, por el método y en la fecha y hora indicadas en la Sección 2. Es su responsabilidad asegurarse que su cotización se envíe el día o antes la fecha límite. Las cotizaciones recibidas después de la fecha límite de presentación, por cualquier motivo, no serán consideradas para evaluación.

Gracias y quedamos a la espera de su cotización.

Atentamente le saluda,

**Unidad de Adquisiciones PNUD**

## SECCION 2: SDC INSTRUCCIONES PARA LOS OFERENTES

<b>Introducción</b>	<p>Los oferentes deberán cumplir con todos los requerimientos de esta SDC, incluyendo cualquier enmienda emitida por el PNUD. Esta SDC se lleva a cabo de acuerdo con <a href="#">las Políticas y Procedimientos de Operaciones y Programas (POPP) del PNUD sobre Contratos y Adquisiciones</a></p> <p>Toda oferta que se presente será considerada como un ofrecimiento del oferente y no constituye ni implica la aceptación de la misma por parte del PNUD. El PNUD no tiene ninguna obligación de adjudicar un contrato a ningún oferente como resultado de esta SDC.</p> <p>El PNUD se reserva el derecho de cancelar el proceso de adquisición en cualquier etapa sin responsabilidad de ningún tipo para el PNUD, previa notificación a los oferentes o publicación del aviso de cancelación en el sitio web del PNUD.</p>
<b>Fecha límite para la presentación de la cotización</b>	<p>14 de julio 2022 a las 2pm</p>
<b>Forma de envío</b>	<p>La cotización debe ser enviada de la siguiente forma:</p> <p><input checked="" type="checkbox"/> Correo electrónico específico <a href="mailto:Adquisiciones.do@undp.org">Adquisiciones.do@undp.org</a></p> <ul style="list-style-type: none"> <li>▪ Formato de archivo PDF</li> <li>▪ Los nombres de archive, no pueden exceder los 60 caracteres, ni otros caracteres por fuera del alfabeto latino. Haga clic o pulse aquí para escribir texto.</li> <li>▪ Todos los archivos deben estar libres de virus y sin daño.</li> <li>▪ Peso máximo de los archivos, por envío <b>15 MB</b></li> <li>▪ Asunto del correo (obligatorio): <b>SDC-41-2022 Adquisición e implementación de una solución de Control de Acceso a la Red (NAC) para el Tribunal Constitucional de la República Dominicana.</b></li> <li>▪ En caso de múltiples correos, deben ser claramente identificados indicando en el asunto "Correo X de Y" y finalmente "Correo Y de Y".</li> <li>▪ Se recomienda que la cotización se envíe, con el mayor número de archivos adjuntos, en la medida de lo posible.</li> </ul> <p>El oferente debe recibir un mensaje automático de acuse de recibo de su oferta.</p>
<b>Costo de preparación de la cotización</b>	<p>El PNUD no será responsable de los costos asociados con la preparación y presentación de la cotización de los oferentes, independientemente del resultado o la forma en que se lleve a cabo proceso de selección.</p>
<b>Código de Conducta para el Proveedor, Fraude, Corrupción</b>	<p>Todos los posibles proveedores deben dar lectura al Código de Conducta para Proveedores de las Naciones Unidas y reconocer que cumple con los estándares mínimos que se espera de los proveedores de las Naciones Unidas. El Código de Conducta, que <b>incluye principios sobre trabajo, derechos humanos, medio ambiente y conducta ética</b>, se encuentra en: <a href="https://www.un.org/Depts/ptd/about-us/un-supplier-code-conduct">https://www.un.org/Depts/ptd/about-us/un-supplier-code-conduct</a></p> <p>Además, el PNUd ejerce rigurosamente una política de tolerancia cero ante prácticas prohibidas, incluidos el fraude, la corrupción, la colusión, las prácticas contrarias a la ética en general y a la ética profesional y la obstrucción por parte de proveedores del PNUD y exige a los oferentes / proveedores respetar los más altos estándares de ética durante el proceso de adquisición y la ejecución del contrato. La Política Anti-Fraude del PNUD se puede encontrar en: <a href="http://www.undp.org/content/undp/en/home/operations/accountability/audit/office_of_audit_and_investigation.html#anti">http://www.undp.org/content/undp/en/home/operations/accountability/audit/office_of_audit_and_investigation.html#anti</a></p>
<b>Obsequios y atenciones</b>	<p>Los oferentes/proveedores no ofrecerán obsequios o atenciones de ningún tipo a los miembros del</p>

	<p>personal del PNUD, incluidos viajes recreativos a eventos deportivos o culturales o a parques temáticos, ofertas de vacaciones o transporte, invitaciones a almuerzos o cenas extravagantes o similares.</p> <p>En virtud de esta política, el PNUD procederá de la siguiente manera: (a) Rechazará una propuesta si determina que el proponente seleccionado ha participado en prácticas corruptas o fraudulentas al competir por el contrato en cuestión. (b) Declarará inelegible a un proveedor, ya sea de manera definitiva o por un plazo determinado, para la adjudicación de un contrato si en algún momento determina que dicho proveedor ha participado en prácticas corruptas o fraudulentas al competir por un contrato del PNUD o al ejecutarlo.</p>
<b>Conflicto de interés</b>	<p>El PNUD requiere que todo potencial proveedor evite y prevenga conflictos de intereses, al informar al PNUD si usted, o cualquiera de sus afiliados o personal, estuvo involucrado en la preparación de los requisitos, diseño, especificaciones, estimaciones de costos y otra información utilizada en este SDC . Los oferentes evitarán estrictamente los conflictos con otras asignaciones o sus propios intereses y actuarán sin tener en cuenta trabajos futuros. Los oferentes que tengan un conflicto de intereses serán descalificados.</p> <p>Los oferentes deberán revelar en su oferta su conocimiento de lo siguiente:</p> <p>a) si los propietarios, copropietarios, ejecutivos, directores, accionistas mayoritarios de la entidad que presenta la propuesta o personal clave, son familiares del personal del PNUD que participa en las funciones de adquisición y/o en el Gobierno del país, o de cualquier Asociado en la Ejecución que recibe los bienes y/o los servicios contemplados en esta SDC.</p> <p>La elegibilidad de los oferentes que sean total o parcialmente propiedad del Gobierno estará sujeta a la evaluación y revisión adicional del PNUD en varios factores, como estar registrados, operados y administrados como una entidad comercial independiente, el alcance de la propiedad / participación del Gobierno, la recepción de subsidios, mandato y acceso a la información en relación a esta SDC, entre otros. Las condiciones que pueden conducir a una ventaja indebida frente a otros Licitantes pueden resultar en el eventual rechazo de la Oferta.</p>
<b>Condiciones Generales del Control</b>	<p>Cualquier Orden de Compra o Contrato que se emita como resultado de esta SDC, estará sujeta a las Condiciones Generales del Contrato</p> <p>Condiciones Generales aplicables a esta SDC:  <a href="#">Términos y Condiciones Generales / Condiciones Especiales del contrato</a>  Los Términos y Condiciones aplicables y otras disposiciones están disponibles: <a href="#">UNDP/How-we-buy</a></p>
<b>Condiciones Especiales del Contrato</b>	<p>Cancelación de la Orden de Compra/Contrato, si la finalización o entrega se retrasan en más de <b>15 días calendario</b>.</p>
<b>Elegibilidad</b>	<p>Un proveedor no debe estar suspendido, excluido o de otro modo identificado como inelegible por cualquier Organización de las Naciones Unidas, el Grupo del Banco Mundial o cualquier otra organización internacional. Por lo tanto, los proveedores deben informar al PNUD si están sujetos a alguna sanción o suspensión temporal impuesta por estas organizaciones. El no hacerlo puede resultar en la rescisión de cualquier contrato u orden de compra emitida posteriormente al proveedor por el PNUD.</p> <p>Es responsabilidad del Licitante asegurarse de que sus empleados, miembros de empresas conjuntas, subcontratistas, proveedores de servicios, proveedores y / o sus empleados cumplan con los requisitos de elegibilidad establecidos por el PNUD.</p> <p>Los oferentes deben tener la capacidad legal para celebrar un contrato con el PNUD y realizar las entregas en el país, o través de un representante.</p> <p>Los oferentes deben poseer nombramiento oficial como representante local, si presentan una Oferta en nombre de una entidad ubicada fuera del país y deben estar debidamente autorizado para actuar como Agente en nombre del Fabricante, o Poder Notarial, si el licitante no es un fabricante.</p>

<b>Moneda de la cotización</b>	Moneda Local RD\$ pesos dominicanos o USD dólares para empresas extranjeras sin representación en el país. Para fines de evaluación de la propuesta se utilizará la moneda pesos dominicanos en su equivalente a la tasa de NNUU del día de la presentación de la oferta.
<b>Asociación en Participación (Joint Venture), Consorcio o Asociación</b>	Si el oferente es un grupo de entidades legales que formarán o han formado un Joint Venture (JV), Consorcio o Asociación para la oferta, deberán confirmar en su Oferta que: (i) han designado a una de las partes para actuar como líder entidad, debidamente autorizada para vincular legalmente a los miembros de la JV, Consorcio o Asociación de manera conjunta y solidaria, lo que deberá constar mediante Acuerdo debidamente notariado entre las personas jurídicas, y presentado con la Oferta; y (ii) si se les adjudica el contrato, el contrato será celebrado por y entre el PNUD y la entidad líder designada, quien actuará en nombre y representación de todas las entidades miembros que componen la empresa conjunta, Consorcio o Asociación.
<b>Única oferta</b>	<p>El oferente (incluida la Entidad Líder en nombre de los miembros individuales de cualquier Joint Venture, Consorcio o Asociación) deberá presentar sólo una Oferta, ya sea en su propio nombre o, si se trata de una Joint Venture, Consorcio o Asociación, como la entidad líder de tal Joint Venture, Consorcio o Asociación.</p> <p>Las ofertas presentadas por dos (2) o más oferentes deberán ser rechazadas si se determina que tienen alguno de los siguientes:</p> <p>a) tienen al menos un socio controlador, director o accionista en común; o b) cualquiera de ellos recibe o ha recibido algún subsidio directo o indirecto de los demás; o</p> <p>b) tienen el mismo representante legal para efectos de esta SDC; o</p> <p>c) tienen una relación entre ellos, directamente o a través de terceros comunes, que los coloca en posición para tener acceso a información o influencia sobre la Oferta de otro Oferente con respecto a este proceso de SDC;</p> <p>d) son subcontratistas de la Oferta del otro, o un subcontratista de una Oferta también presenta otra Oferta bajo su nombre como Oferente principal; o</p> <p>e) algún personal clave propuesto para formar parte del equipo de un Oferente participa en más de una Oferta recibida para este proceso de SDC. Esta condición relativa al personal, no se aplica a los subcontratistas incluidos en más de una Oferta.</p>
<b>Tasas e Impuestos</b>	<p>El artículo II, sección 7, de la Convención sobre Prerrogativas e Inmidades dispone, entre otras cosas, que las Naciones Unidas, incluido el PNUD como órgano subsidiario de la Asamblea General de las Naciones Unidas, están exentas de todos los impuestos directos, excepto los impuestos por servicios públicos, y está exento de restricciones aduaneras, derechos y cargas de naturaleza similar con respecto a los artículos importados o exportados para su uso oficial. Todas las cotizaciones se presentarán netas de impuestos directos y otros impuestos y aranceles, a menos que se especifique lo contrario a continuación:</p> <p>Todos los precios cotizados:</p> <p><input type="checkbox"/> No deberá incluir el ITBIS y otros impuestos indirectos aplicables</p>
<b>Idioma de la oferta</b>	<b>Español</b> Incluyendo documentación, catálogos, instrucciones y manuales de operación.
<b>Documentos a ser presentados</b>	<p><b>Los Oferentes incluirán la siguiente documentación en su oferta:</b></p> <p><input checked="" type="checkbox"/> Anexo 2: Formulario de Cotización debidamente completado y firmado</p> <p><input checked="" type="checkbox"/> Anexo 3: Oferta Técnica y Económica, debidamente completada y firmada, de acuerdo con los requerimientos establecidos en el Anexo 1.</p> <p><input checked="" type="checkbox"/> Perfil de la empresa que no deberá exceder 10 páginas incluidos folletos impresos y catálogos de productos relevantes para los bienes o los servicios adquiridos.</p> <p><input checked="" type="checkbox"/> Certificado de Registro Mercantil con al menos 3 años de registro.</p> <p><input checked="" type="checkbox"/> Certificado de impuestos internos de estar al día en sus obligaciones fiscales.</p> <p><input checked="" type="checkbox"/> Demostrar tener al menos 2 experiencias probada en el negocio de implementación de soluciones de control de acceso a la red (NAC) en los últimos dos años con Cartas de clientes en los cuales se hayan realizado implementaciones de este tipo de solución</p>

	<p><input checked="" type="checkbox"/> Evidencias en los últimos tres (3) años de al menos 3 implementaciones de soluciones de control de acceso a la red (NAC) en ambiente de Alta Disponibilidad (HA). Cartas de clientes en los cuales se hayan realizado implementaciones de este tipo de solución</p> <p><input checked="" type="checkbox"/> Autorización del fabricante para representar, instalar y configurar las soluciones de control de acceso a la red (NAC)</p> <p><input checked="" type="checkbox"/> Deberá presentar certificación en la que especifique poseer al menos un gerente de proyectos : mínimo 2 experiencias probada liderando proyectos en la implementación de soluciones de control de acceso a la red (NAC) nombre empresa, contacto, año de implementación en los últimos dos años</p> <p>Personal técnico clave del proyecto: mínimo 2 experiencias de experiencia probada participando en la implementación de control de acceso a la red (NAC). en los últimos dos años</p> <p><input checked="" type="checkbox"/> En caso de consorcio, se debe presentar copia simple de los poderes legales vigentes de los representantes de las empresas que integran la asociación o consorcio. La designación del Representante Legal común del Consorcio.</p> <p><input checked="" type="checkbox"/> Auto Declaración por escrito de que la empresa no está incluida en la Lista 1267/1989 del Consejo de Seguridad de la ONU, o en la lista de la División de Adquisiciones de la ONU o en cualquier otra lista suspensiva de la ONU.</p> <p><input checked="" type="checkbox"/> Cronograma</p> <p><b><u>Nota: El NO CUMPLIMIENTO CON LA TOTALIDAD de requisitos en este apartado conducirá al RECHAZO de la oferta.</u></b></p>				
<b>Validez de la oferta</b>	La oferta se mantendrá válida por <b>60 días</b> , contados a partir de la fecha límite establecida para presentación de ofertas.				
<b>Variación de precio</b>	No se aceptará ninguna variación de precio debido a escalada, inflación, fluctuación en los tipos de cambio o cualquier otro factor del mercado, en ningún momento durante la validez de la oferta una vez que se haya recibido la cotización.				
<b>Ofertas parciales</b>	<input checked="" type="checkbox"/> No permitidas				
<b>Ofertas alternativas</b>	<input checked="" type="checkbox"/> No permitidas				
<b>Forma de pago</b>	<table border="1"> <tr> <td data-bbox="349 1213 467 1367">60%</td> <td data-bbox="467 1213 1408 1367"> <ul style="list-style-type: none"> <li>• Instalación de la solución de control de acceso a la red (NAC).</li> <li>• Configuración de la solución de control de acceso a la red (NAC).</li> <li>• Integración de la solución de control de acceso a la red (NAC) con Active Directory, Domain Controller, Microsoft System Center Configuration Manager, Bitdefender e Infraestructura Fortinet.</li> </ul> </td> </tr> <tr> <td data-bbox="349 1367 467 1701">40%</td> <td data-bbox="467 1367 1408 1701"> <ul style="list-style-type: none"> <li>• Realización de las pruebas de failover en la premisa.</li> <li>• Demostración del correcto funcionamiento de la solución de control de acceso a la red (NAC) aún con un (1) appliance fuera de servicio.</li> <li>• Realización de pruebas de failover a Azure, y failback a la premisa, de dos (2) sistemas con sus correspondientes servidores virtuales, a definir durante ejecución del proyecto.</li> <li>• Capacitación de dos (2) personas en el uso de las herramientas administrativas provistas por la solución, y de acuerdo al diseño implementado.</li> <li>• Entrega de la documentación técnica y de uso del fabricante de las herramientas administrativas provistas por la solución.</li> <li>• Entrega de la documentación de la solución implementada.</li> </ul> </td> </tr> </table>	60%	<ul style="list-style-type: none"> <li>• Instalación de la solución de control de acceso a la red (NAC).</li> <li>• Configuración de la solución de control de acceso a la red (NAC).</li> <li>• Integración de la solución de control de acceso a la red (NAC) con Active Directory, Domain Controller, Microsoft System Center Configuration Manager, Bitdefender e Infraestructura Fortinet.</li> </ul>	40%	<ul style="list-style-type: none"> <li>• Realización de las pruebas de failover en la premisa.</li> <li>• Demostración del correcto funcionamiento de la solución de control de acceso a la red (NAC) aún con un (1) appliance fuera de servicio.</li> <li>• Realización de pruebas de failover a Azure, y failback a la premisa, de dos (2) sistemas con sus correspondientes servidores virtuales, a definir durante ejecución del proyecto.</li> <li>• Capacitación de dos (2) personas en el uso de las herramientas administrativas provistas por la solución, y de acuerdo al diseño implementado.</li> <li>• Entrega de la documentación técnica y de uso del fabricante de las herramientas administrativas provistas por la solución.</li> <li>• Entrega de la documentación de la solución implementada.</li> </ul>
60%	<ul style="list-style-type: none"> <li>• Instalación de la solución de control de acceso a la red (NAC).</li> <li>• Configuración de la solución de control de acceso a la red (NAC).</li> <li>• Integración de la solución de control de acceso a la red (NAC) con Active Directory, Domain Controller, Microsoft System Center Configuration Manager, Bitdefender e Infraestructura Fortinet.</li> </ul>				
40%	<ul style="list-style-type: none"> <li>• Realización de las pruebas de failover en la premisa.</li> <li>• Demostración del correcto funcionamiento de la solución de control de acceso a la red (NAC) aún con un (1) appliance fuera de servicio.</li> <li>• Realización de pruebas de failover a Azure, y failback a la premisa, de dos (2) sistemas con sus correspondientes servidores virtuales, a definir durante ejecución del proyecto.</li> <li>• Capacitación de dos (2) personas en el uso de las herramientas administrativas provistas por la solución, y de acuerdo al diseño implementado.</li> <li>• Entrega de la documentación técnica y de uso del fabricante de las herramientas administrativas provistas por la solución.</li> <li>• Entrega de la documentación de la solución implementada.</li> </ul>				
<b>Condiciones para liberar pagos</b>	<p><input checked="" type="checkbox"/> Solución debidamente instalada e integrada con toda la infraestructura, bajo las mejores prácticas recomendadas por el fabricante.</p> <p><input checked="" type="checkbox"/> Documentación de la instalación (configuraciones realizadas, etc.).</p> <p><input checked="" type="checkbox"/> Manuales de usuarios y técnicos.</p> <p><input checked="" type="checkbox"/> Planes de mantenimiento a la solución.</p> <p><input checked="" type="checkbox"/> Aceptación escrita de los bienes, basada en el pleno cumplimiento de los requisitos de la SDC.</p>				

<b>Contacto para correspondencia, notificaciones y aclaraciones</b>	<p>Correo electrónico : <a href="mailto:adquisiciones.do@undp.org">adquisiciones.do@undp.org</a>  Publicada directamente en página web</p> <p>Cualquier retraso en la respuesta del PNUD no se utilizará como motivo para extender el plazo para la presentación, a menos que el PNUD determine que tal extensión es necesaria y comunique un nuevo plazo a los Proponentes.</p>
<b>Reunión previa a la presentación de ofertas</b>	No se llevará a cabo
<b>Aclaraciones</b>	<p>Se estarán recibiendo preguntas hasta <b>las 11:00 am del día 07 de julio del 2022</b> a través del correo <a href="mailto:adquisiciones.do@undp.org">adquisiciones.do@undp.org</a> y se responderán a través del página web a través de documentos de aclaraciones hasta <b>el día 08 de julio del 2022</b></p> <p>Nota: Es responsabilidad de todos los oferentes estar pendientes de la fecha y hora del cierre de las aclaraciones.</p>
<b>Método de evaluación</b>	<input checked="" type="checkbox"/> La Orden de Compra / Contrato será otorgado a la oferta que se ajuste a lo requerido y ofrezca el menor precio
<b>Criterio de evaluación</b>	<input checked="" type="checkbox"/> Cumplimiento total de todos los requisitos especificados en el Anexo 1 <input checked="" type="checkbox"/> Plena aceptación de las Condiciones Generales de Contratación y precio más bajo
<b>Derecho a aceptar o a rechazar cualquiera o todas las Propuestas</b>	<b>PNUD</b> no está obligado a aceptar cotizaciones, ni adjudicar un Contrato / Orden de Compra.
<b>Derecho a modificar el requisito en el momento de la adjudicación</b>	En el momento de la adjudicación del Contrato / Orden de Compra, El PNUD se reserva el derecho de variar (aumentar o disminuir) la cantidad de servicios y/ o bienes, hasta un máximo del veinticinco (25%) del total de la oferta, sin ningún cambio en el precio unitario u otros términos y condiciones.
<b>Tipo de Contrato a adjudicar</b>	<input checked="" type="checkbox"/> Orden de Compra
<b>Fecha prevista para adjudicar el contrato</b>	Julio del 2022
<b>Publicación de la adjudicación del contrato</b>	PNUD publicará las adjudicaciones de contratos valoradas en USD 100.000 o más, en los sitios web de la Oficina de País y el sitio web corporativo del PNUD.
<b>Políticas y procedimientos</b>	Esta SDC se lleva a cabo de acuerdo a <a href="#">Políticas y Procedimientos de Operaciones y Programas (POPP) del PNUD</a>
<b>UNGM registration</b>	Cualquier Contrato resultante de este ejercicio de SDC estará sujeto a que el proveedor se registre en el nivel apropiado en el sitio web del Mercado Global de las Naciones Unidas (UNGM) <a href="http://www.ungm.org">www.ungm.org</a> . El oferente aún puede presentar una cotización incluso si no está registrado en la UNGM, sin embargo, si es seleccionado para la adjudicación del Contrato, el Proveedor debe registrarse en la UNGM antes de la firma del contrato

## ANEXO 1: ESPECIFICACIONES TECNICAS:

### **Adquisición e implementación de una solución de Control de Acceso a la Red (NAC) para el Tribunal Constitucional de la República Dominicana.**

#### **1. Información sobre el proyecto**

El Tribunal Constitucional de la República Dominicana (TCRD), no posee en su infraestructura de ciberseguridad una solución que permita de manera automática, identificar los equipos que se conectan a la red de datos, y a la vez proveer accesos que no comprometan la seguridad. Con la proliferación de dispositivos que permiten las iniciativas de transformación digital y mejorar la eficiencia, la flexibilidad y la optimización, se necesita de una herramienta de apoyo a la gestión que realiza un CISO (Chief Information Security Officer) o Director de Seguridad de la Información.

Una solución tecnológica de control de acceso a la red (NAC) proporcionará al TCRD la importante visibilidad de la red para controlar granularmente todo lo que se conecta a ella, incluyendo la implementación de respuestas y acciones dinámicas y automatizadas.

#### **2. Contexto del proyecto**

##### Solución actual

Actualmente el TCRD cuenta con los siguientes componentes de seguridad de la información:

- Dos (2) Firewall físicos Fortigate 200E configurados en Alta Disponibilidad (HA) en la localidad de Luperón y un Fortigate 90D en la localidad de Mirador Norte.
- Una (1) solución de Antivirus virtualizada, Bitdefender GravityZone Advanced Business Security, sin alta disponibilidad.
- Dos (2) servidores de Windows Server Update Services (WSUS) para almacenamiento de actualizaciones de sistema operativo.
- Un (1) servidor de Microsoft System Center Configuration Manager para realizar el despliegue de actualizaciones del sistema operativo, Windows 10, a las estaciones de trabajo.
- Dieciséis (16) Wireless Access Point Fortinet FortiAP FP221E desplegados en la localidad de Luperón.
- Dos (2) localidades interconectadas entre sí por dos (2) enlaces VPN simultáneos, para permitir balanceo y brindar estabilidad de conexión.
- Cuatro (4) switches Cisco de acceso de 24 puertos en la localidad de Mirador Norte.
- Dos (2) switches Cisco Core de 24 puertos en la localidad de Mirador Norte.
- Dos (2) switches (Cisco y Fortinet) de 24 puertos en la localidad de Luperón.
- Dos (2) switches Fortinet Core de 24 puertos en la localidad de Luperón.
- Dos (2) switches Cisco Core de 48 puertos en la localidad de Luperón.
- Cuatro (4) switches Cisco de acceso de 48 puertos en el DataCenter.
- Diez (10) switches Fortinet de acceso de 48 puertos en la localidad de Luperón.

- 713 dispositivos conectados a la red alámbrica entre ambas localidades, clasificados en:
  - 35 impresoras
  - 318 teléfonos IP (según reporte Infraestructura del 26-FEB-2022)
  - 2 centrales telefónicas
  - 12 servidores físicos
  - 100 laptops
  - 347 desktops (278 localidad principal + 69 localidad secundaria)
- Puntos de red por sede:
  - Sede Plaza de la Bandera (principal) 864
  - Sede Mirador Norte (secundaria) 144
- Contamos con Una (1) Suscripción Microsoft Azure:
  - A esta localidad se replican los servidores virtuales (48) en la premisa, sirviendo esta como espacio de recuperación de desastres del site principal (premisa).
  - Servicios adicionales:
    - Tres (3) máquinas virtuales, las cuales operan desde Microsoft Azure
    - App Services para el manejo de aplicaciones
    - Cuentas de almacenamiento (storage account) para el almacenamiento de data
    - Redes virtuales, Firewall, Gateway en la nube
    - Discos duros en la nube
    - Y otros servicios

### 3. **Objetivo general**

Dotar al TCRD de una solución tecnológica de control de acceso a la red (NAC) que permita controlar de forma granular qué dispositivos pueden acceder a la red de datos, permitiendo establecer políticas de gestión de los dispositivos, tanto fijos como móviles, e integrar estas políticas con la facilidad de permitir a los usuarios traer su propio dispositivo, para de este modo evitar, la propagación de malware y otras amenazas que pueden poner en riesgo la infraestructura, dejando al TCRD vulnerable ante ataques y pérdidas de datos.

### 4. **Objetivos específicos**

1. Adquisición e implementación de una solución tecnológica de control de acceso a la red (NAC), como un appliance virtual en la premisa y en el Azure Site Recovery (ASR).
2. Integración de la solución tecnológica de control de acceso a la red (NAC) con Active Directory, Domain Controller, Microsoft System Center Configuration Manager, Bitdefender e Infraestructura Fortinet.
3. Aplicar políticas para cada situación operativa sin requerir productos separados o módulos adicionales.
4. Reconocer y elaborar los perfiles de los usuarios y sus dispositivos antes de que un código malicioso pueda causar daños.
5. Administrar los usuarios temporales mediante un portal de autoservicio personalizable que incluye el registro, la autenticación y un portal de administración de los usuarios temporales.
6. Evaluar el cumplimiento de la política de seguridad por tipo de usuario, tipo de dispositivo y sistema operativo.
7. Mitigación de las amenazas a la red mediante la aplicación de políticas de seguridad que bloquean, aíslan y reparan las maquinas no conformes sin la atención del administrador.
8. Integración con otras soluciones de red y seguridad a través de una API de RESTful/abierta.
9. Contar con una solución que permita un ambiente de Alta Disponibilidad (HA) de los servicios.

10. Realización de diseño de la solución según los objetivos específicos descritos.
11. Documentación exhaustiva de la solución implementada.
12. Capacitación a dos (2) personas en el uso de las herramientas administrativas provistas por la solución, y de acuerdo al diseño implementado.
13. Contar con un acuerdo anual de soporte del fabricante para implementaciones de misión crítica 24x7 y tiempo de respuesta no mayor a seis (6) horas, por un período inicial de tres (3) años, que incluya servicio técnico remoto y en sitios.
14. Contar con un modelo de licenciamiento anual para el software requerido por la solución de control de acceso a la red (NAC), con una vigencia inicial a tres (3) años.

## 5. Actividades requeridas al contratista

1. Proveer e implementar la solución control de acceso a la red (NAC) según los términos de referencia.
2. Integrar la solución control de acceso a la red (NAC) con Active Directory, Domain Controller, Microsoft System Center Configuration Manager, Bitdefender e Infraestructura Fortinet.
3. Establecer e implementar las políticas de respuesta y acciones automatizadas.
4. Proveer todas las licencias requeridas por la solución, exceptuando los sistemas operativos Windows Server que serán provistos por el TCRD.
5. Establecer los contratos de soporte del fabricante.
6. Configurar la Alta Disponibilidad (HA) entre el appliance virtual en la premisa y el Azure Site Recovery (ASR) de la institución.
7. Realizar el diseño de la solución según los objetivos específicos descritos.
8. Documentar exhaustivamente la solución implementada.
9. Suplir la documentación técnica y de uso del fabricante de las herramientas administrativas provistas por la solución.
10. Capacitar dos (2) personas en el uso de las herramientas administrativas y operativas provistas por la solución, y de acuerdo al diseño implementado.
11. Realizar pruebas de funcionamiento de las políticas establecidas, así como las situaciones de failover.
12. Realizar las demostraciones de correcto funcionamiento de la solución control de acceso a la red (NAC) aún con un (1) appliance fuera de servicio.
13. Realizar las pruebas de failover a Azure, y failback a la premisa, de la solución control de acceso a la red (NAC), a definir durante ejecución del proyecto.

## 6. Características requeridas de la solución de control de acceso a la red (NAC) (solución requerida)

- Permitir una arquitectura centralizada que permita la administración y visualización de localidades remotas.
- Encontrarse dentro del primer cuarto de la vida útil establecida por el fabricante.
- Debe contar con la posibilidad de expandir la solución, permitiendo VM's con un procesamiento distinto a los instalados originalmente y/o que estas VM's puedan ser únicamente utilizadas de forma pasiva.
- La solución propuesta debe soportar duplicación o replicación automática en tiempo real entre las unidades en ambiente de alta disponibilidad.

## 7. Especificaciones técnicas de la solución requerida

<b>SOLUCIÓN CONTROL DE ACCESO A LA RED (NAC)</b>	
<b>Arquitectura</b>	<ul style="list-style-type: none"> <li>• Solución de Control de Acceso a la Red (NAC) basada en máquinas virtuales (VMs), desplegadas sobre arquitecturas Microsoft Hyper-V o Azure.</li> <li>• La solución debe soportar, al menos 800 dispositivos conectados simultáneamente desde un único appliance, y deberá poder escalar a más dispositivos con la adición de licenciamiento o suscripción a la arquitectura o VM/Appliance adicional.</li> <li>• La Arquitectura de la solución debe ser escalable, permitiendo instalaciones de múltiples dispositivos físicos o virtuales coordinados para dar servicio de acceso a instalaciones de miles de dispositivos.</li> <li>• En caso de requerirse múltiples VMs para la implementación de la solución, esta deberá permitir la administración centralizada del conjunto desde un Appliance o VM de administración.</li> <li>• La solución debe ser licenciable por dispositivo concurrente. Estas licencias deben ser suscripciones anuales y deben permitir distintos niveles de operación (visibilidad, control, cumplimiento).</li> </ul>
<b>Visibilidad - Red</b>	<ul style="list-style-type: none"> <li>• La solución debe permitir un despliegue centralizado, en una arquitectura fuera de banda, y brindar control de acceso en Capa 2 y 3 sobre una infraestructura cableada e inalámbrica.</li> <li>• Debe permitir crear una estructura jerárquica que permita ordenar los dispositivos de infraestructura de la red de manera lógica y/o geográfica.</li> <li>• Debe permitir crear, modificar y borrar dispositivos y sus características.</li> <li>• Debe permitir el registro manual de dispositivos no SNMP.</li> <li>• Debe contar con un proceso continuo de detección y categorización de dispositivos de infraestructura de red, que permita detectar y controlar los switches, routers y otros dispositivos de la red.</li> <li>• Debe permitir mover fácilmente los dispositivos dentro de la estructura jerárquica generada.</li> <li>• Debe permitir realizar consulta a nivel Capa 2 y 3 (polling) de los dispositivos que se encuentren conectados a los equipos de red controlados, para poder utilizar esta información en la fase de control de acceso.</li> <li>• La solución debe poder ser registrada como un dispositivo independiente dentro de la topología física en la consola de gestión unificada del firewall del mismo fabricante de la solución de control de acceso a la red (NAC) ofertada.</li> </ul>
<b>Visibilidad - Endpoint</b>	<ul style="list-style-type: none"> <li>• Debe permitir determinar el perfil de los hosts descubiertos mediante métodos que no requieran la instalación de agentes incluyendo, al menos, los siguientes: <ul style="list-style-type: none"> <li>– DHCP Fingerprinting</li> <li>– HTTP/HTTPS</li> <li>– Ubicación</li> <li>– Rangos IP</li> <li>– SNMP</li> <li>– SSH</li> <li>– Telnet</li> <li>– TCP</li> <li>– UDP</li> <li>– OUI</li> <li>– WMI</li> <li>– WinRM</li> <li>– Activo con NMAP</li> </ul> </li> </ul>

<b>SOLUCIÓN CONTROL DE ACCESO A LA RED (NAC)</b>	
	<ul style="list-style-type: none"> <li>- Pasivo con POF</li> <li>- Agente</li> <li>- ONVIF</li> <li>- Trafico de red (Network traffic)</li> <li>- Script usando Perl</li> <li>- Debe permitir la detección de hosts desconocidos (rogue).</li> <li>- Debe permitir la identificación de hosts mediante Portal Cautivo.</li> <li>- Debe permitir la categorización automática de hosts y dispositivos IoT.</li> <li>- Debe permitir la recategorización periódica de los hosts desconocidos.</li> <li>- Debe recordar el perfil asignado a cada host, y verificar que sigue siendo válido en cada nueva conexión del host. Si el perfil variara, deberá impedir su conexión y notificar inmediatamente sobre el evento.</li> </ul>
<b>Visibilidad - Endpoint</b>	<ul style="list-style-type: none"> <li>- La solución debe poder reconocer los siguientes sistemas operativos sin necesidad de agentes:</li> <li>- Android</li> <li>- Apple iOS for iPhone/iPad7/iPod</li> <li>- Blackberry OS/Blackberry 10 OS</li> <li>- Chrome OS</li> <li>- Free BSD</li> <li>- Kindle/Kindle Fire</li> <li>- Linux</li> <li>- Mac OS X</li> <li>- Open BSD</li> <li>- Solaris</li> <li>- Symbian</li> <li>- Web OS</li> <li>- Windows</li> <li>- Windows Phone/CE/RT</li> <li>- La solución no debe requerir el uso de 802.1x para permitir el descubrimiento de hosts o usuarios, o brindar control de acceso a nivel de Puerto en la infraestructura cableada.</li> <li>- Debe permitir la integración con plataformas MDM.</li> <li>- Debe permitir la integración con las siguientes plataformas de MDM:</li> <li>- Air Watch</li> <li>- Google GSuite</li> <li>- MaaS360</li> <li>- Mobile Iron</li> <li>- XenMobile</li> <li>- Fortinet EMS</li> <li>- Nozomi</li> <li>- JAMF</li> <li>- Debe permitir la fijación de períodos en los que el host está autorizado a conectarse, y evaluarlos periódicamente.</li> </ul>
<b>Visibilidad - Endpoint</b>	<ul style="list-style-type: none"> <li>- Debe permitir la importación de un archivo .CSV conteniendo información sobre los hosts a registrar.</li> <li>- Debe permitir determinar el perfil de los dispositivos IoT mediante una URL hacia una base de datos de Servicios de IoT del mismo fabricante de la solución de control de acceso a la red (NAC) ofertada.</li> <li>- Debe permitir determinar el perfil de los dispositivos descubiertos mediante sesiones de firewall del mismo fabricante de la solución de control de acceso a la red (NAC) ofertada.</li> </ul>
<b>Visibilidad - Usuarios</b>	<ul style="list-style-type: none"> <li>- Debe permitir el uso de Agentes Persistentes para el perfilamiento de hosts.</li> <li>- Debe permitir la identificación de usuarios mediante Active Directory.</li> </ul>

<b>SOLUCIÓN CONTROL DE ACCESO A LA RED (NAC)</b>	
	<ul style="list-style-type: none"> <li>- Debe permitir la identificación de usuarios mediante Portal Cautivo.</li> <li>- La solución debe incluir opciones de análisis flexibles para plataformas Windows, MacOS y Linux. La tecnología de agentes desvanecientes (vanishable) no debe requerir la instalación de software de terceros, tales como Java.</li> <li>- Debe permitir la designación de un Patrocinador (Sponsor) que autorice el acceso de un invitado.</li> <li>- Debe permitir la designación de un Patrocinador (Sponsor) que autorice la categorización de un host.</li> </ul>
<b>Automatización y Control</b>	<ul style="list-style-type: none"> <li>- Debe permitir el ingreso de credenciales mediante 802.1x o Portal Cautivo.</li> <li>- Debe soportar la validación de credenciales con: <ul style="list-style-type: none"> <li>- Google Account</li> <li>- Servidor RADIUS externo</li> <li>- Servidor LDAP</li> </ul> </li> <li>- Debe soportar como postura de seguridad la restricción de conexiones inalámbricas a SSIDs específicos.</li> <li>- Debe soportar como postura de seguridad la detección de Multilocalización (Multihoming).</li> <li>- Debe permitir la autenticación de usuarios mediante las siguientes redes sociales: Facebook, Google, LinkedIn, Outlook, Twitter y Yahoo.</li> <li>- Debe actuar como servidor de RADIUS local embebido dentro de la misma solución de control de acceso a la red.</li> <li>- Debe permitir modo de autenticación de Radius Local con los siguientes modos de EAP 802.1X: <ul style="list-style-type: none"> <li>- TTLS/PAP</li> <li>- TTLS/MSCHAPv2</li> <li>- PEAP/MSCHAPv2</li> <li>- TLS</li> </ul> </li> <li>- Debe soportar la validación automática de credenciales mediante agentes persistentes o volátiles</li> <li>- La solución debe tener la capacidad de aprovechar la combinación de informaciones sobre la identidad del usuario y el tipo de dispositivo para aprovisionar dinámicamente permisos de acceso basados en roles y distintos niveles de acceso.</li> <li>- Debe permitir la generación de políticas de control, agrupadas jerárquicamente, y determinar la política a aplicar a cada dispositivo en función de una serie de reglas de asignación.</li> <li>- La solución debe incluir funcionalidades de Gestión de Invitados (Guest Management), permitiendo la creación de perfiles de Invitados y Contratistas.</li> </ul>
<b>Automatización y Control</b>	<ul style="list-style-type: none"> <li>- Debe soportar, al menos, los siguientes tipos de información para determinar la política a aplicar: <ul style="list-style-type: none"> <li>- Ubicación</li> <li>- Grupo de Pertenencia</li> <li>- Atributo</li> <li>- Fecha y Hora</li> </ul> </li> <li>- Debe permitir la creación de plantillas que agrupen a los invitados o contratistas en grupos que tengan distintos permisos de acceso, o períodos de acceso permitido.</li> <li>- Debe contar con herramientas que permitan la generación y mantenimiento de este tipo de usuarios y sus claves de acceso.</li> <li>- Debe permitir la creación de Portales de Auto-Registro.</li> <li>- Debe soportar el envío de claves de acceso y mensajes personalizables mediante correo electrónico y SMS.</li> </ul>

<b>SOLUCIÓN CONTROL DE ACCESO A LA RED (NAC)</b>	
	<ul style="list-style-type: none"> <li>- Debe permitir la existencia de Patrocinadores (Sponsors) que aprueben el ingreso de Invitados o Contratistas a la red, o que eleven los permisos de acceso de ciertos individuos.</li> <li>- La solución debe incluir funcionalidades de Inducción de Internet de las Cosas (IoT Onboarding) con autorización de Patrocinadores (Sponsors).</li> <li>- La solución debe incluir funcionalidades de detección y contención de dispositivos desconocidos (rogues)</li> <li>- La solución debe incluir funcionalidades de Cumplimiento de Dispositivos. Antes de permitir el acceso de los dispositivos a la red, debe asegurarse de que estos cumplen con una serie de requisitos de seguridad, integridad y configuración, que hagan seguro su acceso a la red.</li> <li>- Debe permitir el uso de agentes persistentes, desvanecientes (desaparecen luego de realizado en análisis) o pasivos.</li> <li>- Debe permitir el control de acceso a la red (NAC) basado en políticas de acceso que determinen el tipo de segmentación de red para los dispositivos y usuarios registrados. Estas políticas deben asignar una etiqueta (tag) de cortafuego (firewall) que será recibido automáticamente por el cortafuego (firewall) del mismo fabricante de la solución ofertada.</li> </ul>
<b>Automatización y Control</b>	<ul style="list-style-type: none"> <li>- Si un dispositivo no pasa las pruebas de cumplimiento, debe ser posible: <ul style="list-style-type: none"> <li>- No forzar la remediación.</li> <li>- Forzar la remediación inmediatamente, enviando al dispositivo a una red de cuarentena.</li> <li>- Permitir la remediación retardada, dando un período de tiempo desde la detección inicial de problemas, para la solución de estos. Pasado el período de tolerancia, de persistir los problemas, el dispositivo debe ser puesto en cuarentena inmediatamente.</li> <li>- Debe permitir el control de acceso a la red de los usuarios remotos autenticados a través de VPN IPsec y/o SSL utilizando como terminador VPN el mismo fabricante de la solución de control de acceso a la red (NAC) ofertada.</li> </ul> </li> <li>• Debe permitir determinar la postura de Seguridad de los usuarios conectados remotamente a través de VPN IPsec y/o SSL utilizando agente disolvente descargado a través de un portal para las redes de contratistas y agente persistente para la red corporativa.</li> </ul>
<b>Respuesta ante Incidentes de Seguridad</b>	<ul style="list-style-type: none"> <li>• Debe permitir la creación, modificación y borrado de acciones que puedan ser asociadas a una alarma.</li> <li>• Las acciones a ejecutar deben incluir, al menos: <ul style="list-style-type: none"> <li>- Ejecución de un script de comandos</li> <li>- Enviar una alarma a un log externo</li> <li>- Enviar un mensaje de correo electrónico al usuario o a los administradores</li> <li>- Enviar un SMS</li> <li>- Cambiar el rol del host involucrado</li> <li>- Deshabilitar el host</li> <li>- Deshabilitar el puerto de conexión</li> <li>- Revalidar el estado de cumplimiento del host</li> <li>- Marcar el host como En Riesgo</li> <li>- Marcar el host como Seguro</li> </ul> </li> </ul>
<b>Respuesta ante Incidentes de Seguridad</b>	<ul style="list-style-type: none"> <li>• Debe permitir la construcción de reglas de seguridad que se activen ante eventos de seguridad definidos por el administrador, para generar alarmas de seguridad.</li> </ul>

<b>SOLUCIÓN CONTROL DE ACCESO A LA RED (NAC)</b>	
	<ul style="list-style-type: none"> <li>• Ante una alarma de seguridad debe permitir el bloqueo o aislamiento automático de los hosts comprometidos.</li> <li>• Debe permitir homogeneizar los niveles de severidad de los mensajes de Syslog de múltiples dispositivos externos.</li> </ul>
<b>Integraciones</b>	<ul style="list-style-type: none"> <li>• La solución debe permitir el control de usuarios conectados por VPN, con el fin de validar su postura antes que éstos ingresen a los recursos de Red. Esta funcionalidad debe estar integrada como mínimo a plataformas Fortigate y Cisco.</li> <li>• La solución debe poder interoperar con dispositivos de conexión cableada e inalámbrica de los principales fabricantes, incluyendo, como mínimo: <ul style="list-style-type: none"> <li>– Adtran NetVanta</li> <li>– Alcatel-Lucent</li> <li>– Allied Telesis</li> <li>– Arista Networks</li> <li>– Cisco/Meraki</li> <li>– Dell</li> <li>– D-Link</li> <li>– Extreme Networks/Enterasys/Motorola/Avaya/Foundry Networks</li> <li>– Fortinet/Meru</li> <li>– HPE/HP Procurve/3Com/H3C/Aruba</li> <li>– Hirschmann</li> <li>– Huawei</li> <li>– Juniper</li> <li>– Linksys</li> <li>– Mist</li> <li>– Riverbed/Xirrus</li> <li>– Ruckus/Brocade</li> <li>– Ubiquity Unifi</li> <li>– Brocade</li> </ul> </li> </ul>
<b>Integraciones</b>	<ul style="list-style-type: none"> <li>• La solución debe permitir la integración de dispositivos de infraestructura de seguridad de terceras partes, incluyendo: <ul style="list-style-type: none"> <li>– CheckPoint</li> <li>– Cyphort</li> <li>– Cisco/SourceFire</li> <li>– FireEye</li> <li>– Fortinet</li> <li>– Juniper/Netscreen</li> <li>– Palo Alto</li> <li>– Qualys</li> <li>– SonicWall</li> <li>– Sophos</li> <li>– Tenable</li> <li>– AirWatch</li> <li>– MobileIron</li> <li>– MaaS360</li> <li>– Citrix XenMobile</li> <li>– Adtran/BlueSocket</li> </ul> </li> <li>• La solución debe incluir una REST API que permita: <ul style="list-style-type: none"> <li>– Obtener información detallada sobre un elemento en particular, tal como un usuario o un host.</li> <li>– Interrogar a la base de datos para obtener información sobre un conjunto de dispositivos.</li> <li>– Actualizar los registros de usuarios o dispositivos</li> <li>– Bloquear o desbloquear el acceso de un usuario o dispositivo a la red</li> </ul> </li> </ul>

<b>SOLUCIÓN CONTROL DE ACCESO A LA RED (NAC)</b>	
	<ul style="list-style-type: none"> <li>• La solución debe integrarse con la plataforma actual de seguridad perimetral que tiene la institución permitiendo alcanzar un control de acceso granular y respuesta automatizada ante cualquier evento de seguridad presentado, utilizando Etiquetas (Tags) de cortafuego (firewall) y conectores; para aplicar segmentación de acceso a la red La solución debe contar con un método genérico de integración de dispositivos, mediante la recepción, análisis e interpretación de mensajes de Syslog.</li> </ul>
<b>Integraciones</b>	<ul style="list-style-type: none"> <li>• La solución debe permitir la integración de Aplicaciones de Seguridad de Dispositivos (Endpoints), incluyendo: <ul style="list-style-type: none"> <li>– Bitdefender</li> <li>– ESET</li> <li>– Kaspersky</li> <li>– McAfee</li> <li>– Microsoft</li> <li>– Norton</li> <li>– Panda</li> <li>– Sophos</li> <li>– Symantec</li> <li>– Trend Micro</li> </ul> </li> <li>• La solución debe permitir la integración de Servicios de Directorios y Sistemas Operativos, incluyendo: <ul style="list-style-type: none"> <li>– RADIUS: Microsoft IAS, Cisco ACS, FreeRADIUS</li> <li>– LDAP: Microsoft Active Directory, OpenLDAP, Google SSO, CheckPoint</li> <li>– Microsoft Windows</li> <li>– Apple Mac OS X e IOS</li> <li>– Linux</li> <li>– Android</li> </ul> </li> <li>• La información enviada por la solución de control de acceso a la red a la plataforma de seguridad perimetral que tiene la institución debe contener IP, usuario, Grupo o TAGs personalizados que permiten ser asignados de manera automática a grupos de usuarios de firewall utilizados en políticas de IPV4.</li> </ul>
<b>Administración</b>	<ul style="list-style-type: none"> <li>• La solución debe permitir distintos roles administrativos, incluyendo la capacidad de limitar y controlar la cantidad de acceso permitido a las funcionalidades disponibles, dependiendo del grupo administrativo de la organización al que pertenezca el usuario. Por ej., Help Desk, Operaciones de Red, Operaciones de Seguridad.</li> <li>• La solución debe proveer información de auditoría de todas las conexiones de la red, tanto cableadas como inalámbricas. Esto debe incluir una interfaz amigable, que permita buscar y generar consultas en la información almacenada.</li> <li>• La solución debe incluir información de auditoría de todas las acciones y cambios realizados al sistema por los usuarios administradores, incluyendo qué se cambió, cuándo se cambió y quién lo cambió.</li> </ul>
<b>Reportes</b>	<ul style="list-style-type: none"> <li>• Debe contar con reportes predefinidos que incluyan resultados sobre: <ul style="list-style-type: none"> <li>– Registro de Invitados</li> <li>– Registro de dispositivos</li> <li>– Escaneo de Dispositivos</li> </ul> </li> <li>• Debe permitir la generación de reportes a medida sobre: <ul style="list-style-type: none"> <li>– Registro de usuarios y Dispositivos</li> <li>– Falla en los Registros</li> <li>– Logs de Conexión</li> </ul> </li> </ul>

<b>SOLUCIÓN CONTROL DE ACCESO A LA RED (NAC)</b>	
	<ul style="list-style-type: none"> <li>• Debe contar con un Tablero de Control que presente información relevante de manera resumida.</li> <li>• El Tablero de Control debe poder ser modificable para permitir el despliegue de la información que el Administrador considere más relevante.</li> <li>• Debe permitir la generación y archivado de reportes periódicos.</li> <li>• Debe permitir el envío automatizado de reportes mediante correo electrónico.</li> <li>• El log de alarmas debe poder ser ordenado por severidad.</li> <li>• Debe permitir la aceptación y eliminación de alarmas del log de forma manual.</li> <li>• Debe permitir la aceptación y eliminación de alarmas del log de forma automática.</li> <li>• Debe permitir la definición de alarmas en función de la ocurrencia de determinados eventos.</li> </ul>
<b>Servicios</b>	<ul style="list-style-type: none"> <li>• El fabricante debe entregar el soporte directo sobre la plataforma en español.</li> <li>• Entrenamiento (Virtual o Presencial) sobre la administración y operación de la solución de control de acceso a la red (NAC)</li> </ul>
<b>Mantenimiento y Soporte</b>	<ul style="list-style-type: none"> <li>• Incluir tres (3) años de soporte del fabricante para implementaciones de misión crítica, 24 x 7, en donde se cuente con: <ul style="list-style-type: none"> <li>– Tiempo de respuesta no mayor a seis (6) horas o menos de tiempo de respuesta que incluya servicio técnico remoto y en sitio, así como el reemplazo de piezas.</li> <li>– Actualizaciones de parches y nuevas versiones de software.</li> </ul> </li> </ul>

## 8. Competencias requeridas del oferente.

1. Años de experiencia probada en el negocio de implementación de soluciones de control de acceso a la red (NAC).

Cinco (5) o más	100% de los puntos dispuestos.
Entre dos (2) y cuatro (4)	50% de los puntos dispuestos.
Menos de dos (2)	0% de los puntos dispuestos.

2. Evidencias en los últimos tres (3) años de implementaciones de soluciones de control de acceso a la red (NAC) en ambiente de Alta Disponibilidad (HA).

Diez (10) o más	100% de los puntos dispuestos.
Entre nueve (9) y cinco (5)	50% de los puntos dispuestos.
Menos de cinco (5)	0% de los puntos dispuestos.

3. Autorización del fabricante para representar, instalar y configurar las soluciones de control de acceso a la red (NAC) que presente.

Sí	100% de los puntos dispuestos.
----	--------------------------------

No	0% de los puntos dispuestos.
----	------------------------------

4. Gerente del proyecto: Años de experiencia probada liderando proyectos en la implementación de soluciones de control de acceso a la red (NAC).

Cuatro (4) o más	100% de los puntos dispuestos.
Entre dos (2) y tres (3)	50% de los puntos dispuestos.
Menos de dos (2)	0% de los puntos dispuestos.

5. Personal técnico clave del proyecto: Años de experiencia probada participando en la implementación de control de acceso a la red (NAC).

Cinco (5) o más	100% de los puntos dispuestos.
Entre tres (3) y cuatro (4)	50% de los puntos dispuestos.
Menos de tres (3)	0% de los puntos dispuestos.

**9. Fuera de alcance:**

No se requiere que el oferente:

- Crear las VM's necesarias para instalar y/o configurar la solución de control de acceso a la red (NAC).

**10. Metodología, plan de acción y cronograma**

El oferente, después de estudiar detalladamente los trabajos a realizar y las condiciones que rodean al proyecto, deberá presentar en su propuesta la metodología y plan de acción que utilizará para ejecutar el proyecto, tomando en cuenta los recursos disponibles y lo especificado en la presente licitación.

Debe incluir un cronograma del proyecto que indique las etapas que agotará. Este cronograma debe completar mínimamente lo siguiente:

- Diseño.
- Suministro.
- Instalación e integración.
- Configuración.
- Pruebas de aceptación.
- Capacitación.
- Ajustes finales y puesta en marcha.

Deberá utilizar una metodología de carácter participativa con el equipo contraparte designado por el Tribunal Constitucional de la República Dominicana.

**Requisitos de entrega de los bienes**

<b>Requisitos de entrega</b>	
<b>Plazo de entrega</b>	El Proveedor entregará los bienes a más tardar 60 días luego de firmado el Contrato/Orden de Compra.
<b>Términos de entrega (INCOTERMS 2020)</b>	DAP
<b>Despacho de Aduana (debe estar asociado al INCOTERM)</b>	<input checked="" type="checkbox"/> Proveedor/Contratista
<b>Dirección/es exacta/s de entrega</b>	Dirección de la sede principal. Ave 27 de Febrero Esq Gregorio Luperón
<b>Requisitos de servicio posventa y asistencia técnica local</b>	Incluir tres (3) años de soporte del fabricante para implementaciones de misión crítica, 24 x 7, en donde se cuente con: Tiempo de respuesta no mayor a seis (6) horas o menos de tiempo de respuesta que incluya servicio técnico remoto y en sitio, así como el reemplazo de piezas. Actualizaciones de parches y nuevas versiones de software.

## ANEXO 2: FORMULARIO DE PRESENTACION DE OFERTA

Se solicita a los Oferentes que completen este formulario, incluyendo el Perfil de la Compañía y la Declaración del Oferente, lo firmen y entreguen como parte de su cotización junto con el Anexo 3: Oferta Técnica y Financiera. El Oferente completará este formulario de acuerdo con las instrucciones indicadas. No se permitirán alteraciones en su formato ni se aceptarán sustituciones.

Nombre del Oferente:		
SDC Referencia:	Click or tap here to enter text.	Fecha: Haga clic aquí o pulse para escribir una fecha.

### Perfil de la empresa

Descripcion	Detalle de la información	
Nombre legal del Oferente o entidad principal de las empresas asociadas	Haga clic o pulse aquí para escribir texto.	
Dirección legal completa	Haga clic o pulse aquí para escribir texto.	
Sitio web	Haga clic o pulse aquí para escribir texto.	
Año de Constitución/Registro	Haga clic o pulse aquí para escribir texto.	
Estructura Legal	Elija un elemento.	
¿Es una empresa registrada en UNGM como Proveedor?	<input type="checkbox"/> Si <input type="checkbox"/> No en UNGM	En caso afirmativo, Inserte su número de Proveedor
Certificación de Calidad (Ej: ISO 9000 o equivalente) (en caso afirmativo, proporcione una copia del certificado válido)	<input type="checkbox"/> Si <input type="checkbox"/> No	
Dispone de alguna acreditación como ISO 14001 o ISO 14064 o equivalente relacionada con el medio ambiente? (En caso afirmativo, proporcione una copia del certificado válido)	<input type="checkbox"/> Si <input type="checkbox"/> No	
¿Demuestra su empresa un compromiso significativo con la sostenibilidad a través de otros medios, por ejemplo, documentos de política interna de la empresa sobre el empoderamiento de la mujer, energías renovables o membresía en instituciones comerciales que promueven estos temas? (En caso afirmativo, proporcione una copia)	<input type="checkbox"/> Si <input type="checkbox"/> No	
¿Su empresa es miembro del Pacto Mundial de las Naciones Unidas?	<input type="checkbox"/> Si <input type="checkbox"/> No	

Información bancaria	Nombre del banco: Haga clic o pulse aquí para escribir texto. Dirección del banco: Haga clic o pulse aquí para escribir texto. IBAN: Haga clic o pulse aquí para escribir texto. SWIFT/BIC: Haga clic o pulse aquí para escribir texto. Moneda de la Cuenta: Haga clic o pulse aquí para escribir texto. Número de la Cuenta: Haga clic o pulse aquí para escribir texto.			
<b>Experiencia previa relevante: 5 contratos</b>				
Nombre de contrato previo	Detalles de contacto del cliente y de referencia, incluido el correo electrónico	Monto del contrato	Período de actividad	Tipo de actividades realizadas

#### Declaración del Oferente

Sí	No	
<input type="checkbox"/>	<input type="checkbox"/>	<b>Requisitos y Términos y Condiciones:</b> Yo/Nosotros he/hemos leído y entendido completamente la SDC, incluida la Información y los Datos de la SDC, los requerimientos, las Condiciones Generales del Contrato y las Condiciones Especiales del Contrato. Confirmando/confirmamos que el Oferente acepta registrarse por ellos.
<input type="checkbox"/>	<input type="checkbox"/>	Yo/Nosotros confirmamos que el Oferente tiene la capacidad, y las licencias necesarias para cumplir o superar en su totalidad los requerimientos y que se estará disponible para entregar durante el período del Contrato correspondiente.
<input type="checkbox"/>	<input type="checkbox"/>	<b>Ética:</b> al presentar esta Cotización, garantizo/garantizamos que el Oferente: no ha celebrado ningún arreglo inadecuado, ilegal, colusorio o anticompetitivo con ningún Competidor; no se ha acercado directa o indirectamente a ningún representante del Comprador (que no sea el Punto de Contacto) para presionar o solicitar información en relación con la SDC; no ha intentado influir o proporcionar ninguna forma de incentivo, recompensa o beneficio personal a ningún representante del Comprador.
<input type="checkbox"/>	<input type="checkbox"/>	Confirmando/confirmamos que me comprometo a no participar en prácticas prohibidas, o cualquier otra práctica no ética, con las Naciones Unidas o cualquier otra Parte, y a realizar negocios de una manera que evite cualquier riesgo financiero, operativo, reputacional u otro riesgo indebido para las Naciones Unidas y hemos leído el Código de Conducta para proveedores de las Naciones Unidas <a href="https://www.un.org/Depts/ptd/about-us/un-supplier-code-conduct">https://www.un.org/Depts/ptd/about-us/un-supplier-code-conduct</a> y reconocer que proporcionamos los estándares mínimos que se esperan de los proveedores de las Naciones Unidas.
<input type="checkbox"/>	<input type="checkbox"/>	<b>Conflicto de interés:</b> Yo/nosotros garantizamos que el Oferente no tiene ningún conflicto de intereses real, potencial o percibido al presentar esta cotización o al celebrar un contrato para cumplir con los requisitos. Cuando surja un conflicto de interés durante el proceso de solicitud de cotización, el Oferente lo informará inmediatamente al punto de contacto del contratante.
<input type="checkbox"/>	<input type="checkbox"/>	<b>Prohibiciones, sanciones:</b> Yo/Nosotros declaramos que nuestra empresa, sus afiliadas o subsidiarias o empleados, incluidos los miembros de JV/Consortio o subcontratistas o proveedores de cualquier parte del contrato, no están sujetos a la prohibición de adquisiciones de las Naciones Unidas, incluidos, entre otros, a prohibiciones derivadas de Listas de Sanciones del Consejo de Seguridad de las Naciones Unidas y no han sido suspendidas, inhabilitadas, sancionadas o identificadas de otra manera como no elegibles

Si	No	
		por ninguna Organización de las Naciones Unidas o el Grupo del Banco Mundial o cualquier otra organización internacional.
<input type="checkbox"/>	<input type="checkbox"/>	<b>Quiebra:</b> Yo/Nosotros no nos hemos declarado en quiebra, no estamos involucrados en procedimientos de quiebra o administración judicial, y no hay sentencia o acción legal pendiente en nuestra contra que pueda perjudicar las operaciones en un futuro previsible.
<input type="checkbox"/>	<input type="checkbox"/>	<b>Período de validez de la oferta:</b> Confirmando/Confirmamos que esta cotización, incluido el precio, permanece vigente para la aceptación durante la validez de la oferta.
<input type="checkbox"/>	<input type="checkbox"/>	Yo/Nosotros entendemos y reconocemos que ustedes no están obligados a aceptar ninguna Cotización que reciban, y certificamos que los productos ofrecidos en nuestra Cotización son nuevos y sin uso.
<input type="checkbox"/>	<input type="checkbox"/>	Al firmar esta declaración, el signatario a continuación representa, garantiza y acepta que ha sido autorizado por la empresa Oferente para realizar esta declaración en su nombre.

Firma: \_\_\_\_\_

Nombre: Haga clic o pulse aquí para escribir texto.

Cargo: Haga clic o pulse aquí para escribir texto.

Fecha: Haga clic aquí o pulse para escribir una fecha.

**ASEGURARSE DE FIRMAR Y SELLAR FORMULARIOS**

### ANEXO 3: OFERTA TECNICA Y ECONOMICA - BIENES

Se solicita a los Oferentes que completen este formulario, lo firmen y entreguen como parte de su cotización junto con el Anexo 2: Formulario de Oferta. El Oferente completará este formulario de acuerdo con las instrucciones indicadas. No se permitirán alteraciones en su formato ni se aceptarán sustituciones.

Nombre del Oferente:		
SDC Referencia:	Click or tap here to enter text.	Fecha: Haga clic aquí o pulse para escribir una fecha.

<b>Moneda de la oferta</b> Haga clic o pulse aquí para escribir texto.					
<b>INCOTERMS: DAP</b>					
Ítem No	Descripción	Unidad de medida	Cantidad	Precio unitario	Precio total
1.	<b>SOLUCIÓN CONTROL DE ACCESO A LA RED (NAC)</b> según especificaciones técnicas	UD	1		
2.	<b>Incluir tres (3) años de soporte del fabricante para implementaciones de misión crítica, 24 x 7, en donde se cuente con:</b>  <ul style="list-style-type: none"> <li>▪ <b>Tiempo de respuesta no mayor a seis (6) horas o menos de tiempo de respuesta que incluya servicio técnico remoto y en sitio, así como el reemplazo de piezas.</b></li> <li>▪ <b>Actualizaciones de parches y nuevas versiones de software</b></li> </ul>	ud	3		
Precio total bienes					
<b>PRECIO TOTAL ENTREGA DAP (Delivery at Place, Incoterms 2020)</b>					
Otros cargos (especificar)					
<b>PRECIO TOTAL TODO INCLUIDO</b>					

### Cumplimiento de los requisitos

	Su respuesta		
	Si, se cumple	No, no se cumple	Si no puede cumplir, indicar contraoferta
Especificaciones técnicas mínimas requeridas	<input type="checkbox"/>	<input type="checkbox"/>	Haga clic o pulse aquí para escribir texto.
Términos de entrega (INCOTERMS)	<input type="checkbox"/>	<input type="checkbox"/>	Haga clic o pulse aquí para escribir texto.
Plazo de entrega	<input type="checkbox"/>	<input type="checkbox"/>	Haga clic o pulse aquí para escribir texto.
Garantía y requerimientos postventa	<input type="checkbox"/>	<input type="checkbox"/>	Haga clic o pulse aquí para escribir texto.
Validez de la oferta	<input type="checkbox"/>	<input type="checkbox"/>	Haga clic o pulse aquí para escribir texto.
Términos y condiciones de pago	<input type="checkbox"/>	<input type="checkbox"/>	Haga clic o pulse aquí para escribir texto.
Contrato de Soporte del fabricante	<input type="checkbox"/>	<input type="checkbox"/>	Haga clic o pulse aquí para escribir texto.
Solución instalada y configurada por el personal técnico certificado en la solución	<input type="checkbox"/>	<input type="checkbox"/>	Haga clic o pulse aquí para escribir texto.
tres (3) años de soporte del fabricante para implementaciones de misión crítica, 24 x 7, en donde se cuente con:- Tiempo de respuesta no mayor a seis (6) horas o menos de tiempo de respuesta que incluya servicio técnico remoto y en sitio, así como el reemplazo de piezas.  -Actualizaciones de parches y nuevas versiones de software	<input type="checkbox"/>	<input type="checkbox"/>	Haga clic o pulse aquí para escribir texto.

Yo, el abajo firmante, certifico que estoy debidamente autorizado para firmar esta oferta y vincular a la empresa a continuación en caso de que la oferta sea aceptada.	
<b>Nombre y datos exactos de la empresa:</b> Nombre de la empresa Haga clic o pulse aquí para escribir texto. Dirección Haga clic o pulse aquí para escribir texto. Haga clic o pulse aquí para escribir texto. Teléfono Haga clic o pulse aquí para escribir texto. Correo electrónico Haga clic o pulse aquí para escribir texto.	<b>Firma autorizada:</b> Fecha Haga clic o pulse aquí para escribir texto. Nombre Haga clic o pulse aquí para escribir texto. Cargo: Haga clic o pulse aquí para escribir texto. Correo electrónico Haga clic o pulse aquí para escribir texto.

**ASEGURARSE DE FIRMAR Y SELLAR FORMULARIOS**

## **ANEXO 4: Términos y Condiciones Generales para Órdenes de Compra**

### **1. ACEPTACIÓN DE LA ORDEN DE COMPRA**

Esta Orden de Compra sólo podrá ser aceptada una vez que el Proveedor haya firmado y devuelto una copia como acuse de recibo, o tras la entrega oportuna de las mercancías de conformidad con los términos de esta Orden de Compra, según se especifica aquí. La aceptación de esta Orden de Compra constituirá un contrato entre las Partes en virtud del cual los derechos y obligaciones de las Partes se regirán exclusivamente por los términos y condiciones de la presente Orden de Compra, incluyendo las presentes Condiciones Generales. Ninguna cláusula adicional o incompatible que propusiere el Proveedor obligará al PNUD, salvo que dé su acuerdo por escrito un funcionario debidamente autorizado del PNUD.

### **2. PAGO**

- 2.1 El PNUD deberá, en cumplimiento de las condiciones de entrega y salvo disposición en contra en la presente Orden de Compra, efectuar el pago en los 30 días siguientes a la recepción de la factura del Proveedor por los bienes y copias de los documentos de embarque especificados en la presente Orden de Compra.
- 2.2 El pago de la factura mencionada supra reflejará cualquier descuento indicado en las condiciones de pago de la presente Orden de Compra, siempre y cuando el pago se efectúe en el plazo estipulado en dichas condiciones.
- 2.3 Salvo que fuera autorizado por el PNUD, el Proveedor deberá presentar una factura en relación con la presente Orden de Compra y en dicha factura se consignará el número de identificación de la citada Orden.
- 2.4 Los precios indicados en esta Orden de Compra no podrán aumentarse, salvo acuerdo expreso y por escrito del PNUD.

### **3. EXENCION TRIBUTARIA**

- 3.1 El Artículo 7 de la Convención sobre Privilegios e Inmunidades de las Naciones Unidas dispone, entre otras cosas, que las Naciones Unidas, incluidos sus órganos subsidiarios, quedarán exentas del pago de todo tipo de impuestos directos, salvo las tasas por servicios públicos; además, se exime a las Naciones Unidas de pagar derechos aduaneros e impuestos similares en relación con los artículos importados o exportados de uso oficial. Si alguna autoridad gubernamental se negase a reconocer la exención impositiva de las Naciones Unidas en relación con dichos impuestos, derechos o gravámenes, el Proveedor consultará de inmediato al PNUD a fin de determinar un procedimiento que resulte aceptable para ambas partes.
- 3.2. De igual modo, el Proveedor autoriza al PNUD a deducir de la facturación del Proveedor cualquier monto en concepto de dichos impuestos, derechos o gravámenes, salvo que el Proveedor haya consultado al PNUD antes de abonarlos y que el PNUD, en cada caso, haya autorizado específicamente al Proveedor el pago de los impuestos, derechos o gravámenes en cuestión, bajo protesta. En este caso, el Proveedor entregará al PNUD los comprobantes por escrito de que el pago de los impuestos, derechos o gravámenes se haya realizado y haya sido debidamente autorizado.

### **4. RIESGO DE PÉRDIDA**

El riesgo de pérdida, daño o destrucción de los bienes se regirá de conformidad con Incoterms 2010, a menos que haya sido acordado lo contrario por las Partes en la parte frontal de esta Orden de Compra.

## **5. LICENCIAS DE EXPORTACIÓN**

Con independencia del Incoterm 2010 que se utilice en esta Orden de Compra, el Proveedor obtendrá todas las licencias de exportación que requieran los bienes.

## **6. BUEN ESTADO DE LOS BIENES Y SU EMBALAJE**

El Proveedor garantizará que los bienes, incluido su embalaje, cumplen con las especificaciones establecidas en la presente Orden de Compra y que aptos para los fines a que suelen destinarse dichos bienes y para los fines que el PNUD comunicó expresamente al Proveedor, y que están libres de defectos de materiales y fabricación. El Proveedor garantizará también que las mercancías estén envasadas o embaladas adecuadamente para proteger los bienes.

## **7. INSPECCIÓN**

7.1 El PNUD dispondrá de un plazo razonable después de la entrega de la mercancía para inspeccionarla y rechazar y rehusar su aceptación si no cumplen con lo indicado en la presente Orden de Compra, el pago de los bienes de conformidad con la presente Orden de Compra no se considerará una aceptación de la mercancía.

7.2 La inspección anterior al embarque no exonerará al Proveedor de ninguna de sus obligaciones contractuales.

## **8. VIOLACIÓN DE DERECHOS DE PROPIEDAD INTELECTUAL**

El Proveedor garantiza que el uso o suministro por el PNUD de la mercancía vendida en virtud de la presente orden de compra no viola ninguna patente, diseño, nombre comercial o marca registrada. Además, el Proveedor, de conformidad con esta garantía, indemnizará, defenderá y mantendrá al PNUD y a las Naciones Unidas a salvo de cualquier acción o reclamo interpuesto contra el PNUD o las Naciones Unidas relativa a una supuesta infracción de patente, diseño, nombre comercial o marca en relación con los productos vendidos bajo esta Orden de Compra.

## **9. DERECHOS DEL PNUD**

En caso de incumplimiento por parte del proveedor de sus obligaciones en virtud de los términos y condiciones de esta Orden de Compra, incluyendo pero no limitado a la imposibilidad de obtener las licencias de exportación necesarias o de hacer entrega de todo o parte de los bienes en la fecha o fechas de entrega acordada, el PNUD podrá, después de dar al Proveedor un aviso razonable para que cumpla su obligación y sin perjuicio de cualesquiera otros derechos o recursos, ejercer uno o más de los siguientes derechos:

9.1 Adquirir la totalidad o parte de los productos de otros proveedores, en cuyo caso el PNUD podrá exigir al proveedor la responsabilidad por cualquier aumento de los costos en que hubiese incurrido.

9.2 Negarse a aceptar la entrega de todos o parte de los bienes.

- 9.3 Rescindir la presente Orden de Compra sin responsabilidad alguna por los gastos de rescisión u otra responsabilidad de cualquier tipo del PNUD.

#### **10. RETRASO EN LA ENTREGA**

Sin perjuicio de cualesquiera otros derechos u obligaciones de las partes que constan en el presente, si el Proveedor no pudiera entregar los bienes en la(s) fecha(s) de entrega(s) prevista(s) en esta Orden de Compra, el Proveedor, (i) consultará inmediatamente al PNUD para establecer los medios más rápidos para suministrar la mercancía, y (ii) utilizará un medio rápido de entrega, a su costa (a menos que el retraso se deba a un caso de fuerza mayor), si así lo solicita razonablemente el PNUD.

#### **11. CESION Y QUIEBRA**

- 11.1 El Proveedor no podrá, excepto después de haber obtenido el consentimiento por escrito del PNUD, ceder, transferir, dar en prenda o disponer de otro modo de la presente Orden de Compra, o parte de ella, o cualquiera de los derechos u obligaciones del Proveedor en virtud de la presente Orden de Compra.
- 11.2 Si el Proveedor cayera en insolvencia o perdiera el control de la empresa por causa de insolvencia, el PNUD podrá, sin perjuicio de cualesquiera otros derechos o recursos, rescindir inmediatamente la presente Orden de Compra emplazando al Proveedor mediante aviso escrito de terminación.

#### **12. UTILIZACIÓN DEL NOMBRE O, EMBLEMA DEL PNUD O DE LAS NACIONES UNIDAS**

El Contratista no utilizará en modo alguno el nombre, el emblema o el sello oficial del PNUD o de las Naciones Unidas con ninguna finalidad.

#### **13. PROHIBICIÓN DE PUBLICIDAD**

El Proveedor no anunciará ni hará público el hecho de que es un proveedor del PNUD, sin contar antes con la autorización específica del PNUD en cada caso.

#### **14. TRABAJO INFANTIL**

El Proveedor declara y garantiza que ni él mismo ni ninguno de sus filiales realiza prácticas que violen los derechos establecidos en la Convención sobre los Derechos del Niño, en particular el Artículo 32 de la misma que, entre otras cosas, requiere que se proteja a los menores del desempeño de trabajos peligrosos que entorpezcan su educación o sean nocivos para su salud o para su desarrollo físico, mental, espiritual, moral o social.

Cualquier violación de esta declaración y estas garantías autorizará al PNUD a rescindir la presente Orden de Compra de inmediato, mediante la debida notificación al proveedor y sin responsabilidad alguna para el PNUD por costos de rescisión u otro tipo de responsabilidad.

#### **15. MINAS**

El Proveedor declara y garantiza que ni él mismo ni ninguna de sus filiales se encuentran activa y directamente comprometidos en actividades de patente, desarrollo, ensamblado, producción, comercialización o fabricación de minas, o en actividades conexas relacionadas con los componentes utilizados en la fabricación de minas. El término "minas" se refiere a aquellos dispositivos definidos en

el Artículo 2, Párrafos 1, 4 y 5 del Protocolo II anexo a la Convención de 1980 sobre Armas Convencionales Excesivamente Nocivas o de Efectos Indiscriminados.

Cualquier violación de esta declaración o garantías autorizará al PNUD a rescindir el presente Contrato en forma inmediata, mediante la debida notificación al Proveedor, sin que esto implique responsabilidad alguna por los gastos de rescisión o cualquier otra responsabilidad para el PNUD.

## **16.0RESOLUCION DE CONFLICTOS**

**16.1 Resolución de mutuo acuerdo :** Las Partes realizarán todos los esfuerzos posibles para resolver de mutuo acuerdo cualquier conflicto, controversia o reclamo que surgiese en relación con la presente Orden de Compra o con algún incumplimiento, rescisión o invalidez relacionados con éste. En caso de que las Partes desearan buscar una solución de mutuo acuerdo mediante un proceso de conciliación, éste tendrá lugar con arreglo a las Reglas de Conciliación de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) vigentes en ese momento, o con arreglo a cualquier otro procedimiento que puedan acordar las Partes.

**16.2 Arbitraje: Si el conflicto,** controversia o reclamo que pudiera surgir entre las Partes en relación con esta Orden de Compra, o con su incumplimiento, rescisión o invalidez no, se resolviera de mutuo acuerdo con arreglo a lo estipulado en el Artículo 16.1 supra dentro de los sesenta (60) días a partir de la recepción por una de las Partes de la solicitud de resolución de mutuo acuerdo de la otra Parte , dicha disputa, controversia o reclamo podrá ser sometida por cualquiera de las Partes a un proceso de arbitraje según el Reglamento de Arbitraje de la CNUDMI vigente en ese momento, incluidas sus disposiciones sobre las leyes aplicables. El tribunal arbitral no tendrá autoridad para imponer sanciones punitivas. Las Partes estarán vinculadas por el fallo del tribunal arbitral resultante del citado proceso de arbitraje, a modo de resolución final de toda controversia, reclamo o disputa.

## **17.PRIVILEGIOS E INMUNIDADES**

Nada de lo estipulado en estos Términos y Condiciones Generales o en esta Orden de Compra se considerará como renuncia a los privilegios e inmunidades de las Naciones Unidas, incluidos sus órganos subsidiarios.

## **18.EXPLORACIÓN SEXUAL**

**18.1** El Contratista deberá tomar todas las medidas necesarias para impedir la explotación o el abuso sexual de cualquier persona por parte del Contratista, de sus empleados o de cualquier otra persona que pueda ser contratada por el Contratista para prestar cualquier servicio en virtud del presente Contrato. Para estos efectos, todo intercambio sexual con cualquier persona menor de dieciocho años, con independencia de cualesquiera leyes relativas al consentimiento, constituirá un caso de explotación y abuso sexual de dicha persona. Además, el Contratista se abstendrá, y tomará todas las medidas adecuadas para prohibir que lo hagan sus empleados u otras personas contratadas por él, intercambien dinero, bienes, servicios, ofertas de empleo u otros artículos de valor por favores o actividades sexuales, o entablar relaciones sexuales que constituyan una explotación o degradación de cualquier persona. El Contratista reconoce y acuerda que estas disposiciones del presente Contrato constituyen una condición esencial del mismo, y que cualquier incumplimiento de esta representación y garantía autorizará al PNUD a

rescindir el Contrato de inmediato mediante notificación al Contratista, sin obligación alguna relativa a gastos de rescisión o responsabilidad de ningún otro tipo.

- 18.2 El PNUD no aplicará la norma que antecede relativa a la edad en ningún caso en que el personal del Contratista o cualquier otra persona contratada por éste para prestar cualquier servicio en virtud del presente Contrato esté casado(a) con la persona menor de dieciocho años con quien haya mantenido dicho intercambio sexual y cuyo matrimonio sea reconocido como válido ante la ley del país de ciudadanía de las personas involucradas contratadas por el Contratista o de cualquier otra persona que pueda contratar el Contratista para realizar alguno de los servicios que incluye este Contrato.

#### **19. LOS FUNCIONARIOS NO SE BENEFICIARÁN**

El Contratista garantizará que ningún funcionario del PNUD o de las Naciones Unidas haya recibido o vaya a recibir beneficio alguno, directo o indirecto, como resultado del presente Contrato o de su adjudicación. El Contratista tendrá presente que la violación de esta disposición constituye un incumplimiento de una cláusula esencial del presente Contrato.

#### **20. FACULTAD PARA INTRODUCIR MODIFICACIONES**

Con arreglo al Reglamento Financiero y a las normas del PNUD, únicamente el Funcionario Autorizado del PNUD posee la autoridad para aceptar en nombre del PNUD cualquier modificación o cambio del presente Contrato, o renunciar a cualquiera de sus disposiciones o a cualquier relación contractual adicional de cualquier tipo con el Contratista. Del mismo modo, ninguna modificación o cambio introducidos en el presente Contrato tendrá validez y será aplicable contra el PNUD, a menos que se incluya en una enmienda al presente Contrato debidamente firmada por el Funcionario Autoriza