CHRISTIAN CHACON RODRIGUEZ (FIRMA)
Digitally signed by CHRISTIAN CHACON RODRIGUEZ (FIRMA)
Date: 2020.06.29 19:23:44 -06'00'

OBJETO: Solución para el fortalecimiento de la Infraestructura Redundante para el Centro de Procesamiento Primario (CPP) y el Centro Procesamiento Alterno (CPA).

Capítulo 1: Condiciones Técnico – Específicas

Nº Ítem	Unidad	Cantidad	Descripción del bien o servicio
Único	**Ud**	**1**	**Solución para el fortalecimiento de la Infraestructura Redundante de Procesamiento de Información para el Centro de Procesamiento Primario (CPP) y el Centro Procesamiento Alterno (CPA).**
Subítem 1.1	Unidad	1	Servicios de alojamiento para la habilitación de un Centro de Procesamiento Alterno (CPA), enlaces de comunicación e internet.
Subítem 1.2	Unidad	1	Infraestructura como servicio (IaaS) y servicios para el rediseño y Actualización de la Infraestructura de Comunicaciones para el Centro de Procesamiento Primario y Alterno.
Subítem 1.3	Unidad	1	Servicios de Implementación para la Replicación y Recuperación de Desastres para servicios TIC on-Premise.
Subítem 1.4	Unidad	1	Transferencia de Conocimientos de la Solución adquirida.

N°	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
1	***PRESENTACION DE LA OFERTA.***			
1.1	El propósito de este documento es establecer la lista de requerimientos técnicos del servicio que se proveerá a la Caja Costarricense del Seguro Social en adelante referido como CCSS, como parte del proyecto denominado "Solución complementaria para el Fortalecimiento de la Infraestructura Redundante de Procesamiento de Información para el Centro de Datos Primario (CPP) y el Sitio Alterno (CPA)." Con el propósito de facilitar el análisis de las ofertas, la presentación de estas debe hacerse estrictamente como se indica en el presente documento.			
1.2	Cualquier alternativa que se desee proponer debe hacerse clara y totalmente separada de la oferta base y se considerará solo si cumple la base con las características solicitadas y resulta ganadora del método de evaluación. La cotización de una alternativa no debe hacer alusión a lo ofrecido en la oferta base u otras alternativas, sino que debe detallarse cada una en forma independiente.			
1.3	La información adjunta debe tener claramente identificado el desglose de los productos ofrecidos.			
1.4	**Para el subítem 1.1:** Se debe presentar el monto mensual y el total durante el periodo de 48 meses estipulado en el presente cartel.			
1.5	**Para el subítem 1.2:** Para este subitem, se debe presentar una oferta como servicio, es decir en modo de monto mensual y el total durante el periodo de 48 meses estipulado en el presente cartel. Adicionalmente se debe una oferta totalmente separada, considerando para este subítem una propuesta en modalidad de venta. Esta oferta debe presentarse desglosada y totalmente separada de la oferta de pago mensual. Es decir, debe ser una oferta de pago único, en donde la CCSS adquiere este subítem en modo de compra.			
1.6	**Para el subítem 1.3:** Se debe presentar un único monto para los servicios seleccionados.			
1.7	**Para el subítem 1.4:** Se debe presentar el monto correspondiente para cada una de las transferencias de conocimientos solicitadas.			
2	**REQUISITOS DE LOS OFERENTES:** Para que la oferta sea válida, el oferente debe acatar en forma obligatoria las siguientes condiciones técnico-específicas.			

2.1	El oferente o subcontratista debe ser distribuidor autorizado del fabricante para la comercialización de todos los productos y componentes ofrecidos, para lo cual debe presentar documentación actualizada que lo certifique, en caso de documentos emitidos en el extranjero debe aportarse debidamente legalizado vía consular o apostillado. Todas las cartas deben ser originales o bien certificadas por un notario público en el caso de ser copias. El oferente debe ser Gold Partner de CISCO y con especialización Advanced Data Center. Para el Subítem 1.2, el oferente debe presentar confirmación escrita que los servicios de diseño, planeación de implementación, planeación de migración, pruebas de aceptación y optimización serán ejecutados en conjunto entre el fabricante y el oferente.			

2.2	**Experiencia** El oferente debe cumplir y comprobar los siguientes requisitos mínimos respecto a su experiencia: o Debe contar con al menos 3 años de experiencia en el desarrollo de proyectos similares (al menos dos proyectos) al indicado en el presente cartel, donde haya instalado, configurado e implementado diseños de red de comunicaciones TIC "Enterprise", entre dos sitios geográficamente separados, según lo solicitado en el Subítem 1.2 (Federación de Centros de Datos). Adicionalmente, el oferente o subcontratista debe contar con experiencia en replicación de Bases de Datos Oracle que se detalla en el Subítem 1.3. o Para lo anterior, el oferente debe aportar al menos una carta de referencia de cliente que certifique la experiencia solicitada anteriormente y que la solución fue recibida a satisfacción por el cliente. En la carta se debe detallar el nombre completo de la empresa o institución, el nombre del contacto por parte del cliente, puesto dentro de la organización, número telefónico, correo electrónico, cantidad, modelo del equipo y fechas de las implementaciones. o Debe contar con una certificación de representación vigente de las casas fabricantes de los equipos que estaría poniendo a disposición de la CCSS por su parte o de sus alianzas, para lo que debe aportar la carta del fabricante que así lo confirme y no debe tener más de tres meses de emitida. o El oferente o subcontratista debe ser Partner Oracle Platinum certificado para lo cual debe aportar las copias de la certificación. En caso de consorcios, alguno de sus miembros debe contar con dicha certificación. o El oferente o subcontratista debe contar como mínimo con las siguientes especializaciones: • Oracle Platinum Partner Specialized Database 11g. • Oracle Platinum Partner Specialized Database 11g Performance Tuning. • Oracle Platinum Partner Data Integration 11g. • Oracle Platinum Partner Linux 6. o La CCSS se reserva el derecho de verificar los datos consignados en la lista de certificaciones presentada, y en caso de no ser correctos, no se tomarán como referencia. Igualmente, la CCSS se reserva el derecho de solicitar al oferente la constancia del cliente que cumpla con los requisitos indicados anteriormente.			
3	**PERSONAL DEL OFERENTE**			
3.1	En los siguientes puntos se solicitan por cada uno de los componentes de dicha contratación los requerimientos mínimos del personal con el que el oferente debe cumplir para hacer frente al proyecto.			
3.2	El oferente debe brindar un cuadro estilo **matriz** en el cual se pueda apreciar en forma clara y ordenada los nombres de todos los especialistas aportados y la especialización que cubre y el tipo de certificación que tiene.			

3.3	Se debe contar con al menos cinco profesionales certificados por el fabricante Cisco. Se requiere que los recursos cuenten con las siguientes certificaciones: o Al menos un CCIE Data Center. o Al menos un CCIE Switching and Routing. o Al menos un CCIE en Seguridad. o Al menos un especialista con grado de bachiller en informática o carrera a fin certificado en seguridad de redes de nivel profesional (igual o superior a la certificación CCNP Security de Cisco). o Al menos un técnico certificado en enrutamiento y conmutación de nivel profesional (igual o superior a la certificación CCNP de Cisco). Dichas certificaciones deben pertenecer a distintos recursos, es decir, deben ser diferentes personas en donde cada uno por separado cuente con alguna de las certificaciones anteriormente descritas.			
3.4	Se debe contar con al menos cuatro profesionales certificados por el fabricante Oracle. Se requiere que los recursos cuenten con las siguientes certificaciones: o Al menos dos (2) de los especialistas deben ser certificados en Oracle Database 12c Administrator Certified Professional (OCP) o superior, aportar las copias de la certificación(es) debidamente avaladas por un notario público. Al menos uno de los OCP, debe ser directamente del fabricante Oracle. o Al menos de dos (2) especialistas, deben tener la certificación OCA WebLogic (Oracle Certified Associate) versión 11g o superior, aportar las copias de la certificación(es) debidamente avaladas por un notario público. o Debe aportar currículum Vitae, copia del certificado y referencias que demuestren su experiencia por parte de las empresas en las cuales ha laborado.			
3.5	El oferente por su parte debe asignar un administrador de proyectos que liderará y coordinará el proceso de instalación, será el encargado de atender reuniones de planificación con personal de la CCSS. Debe contar con los siguientes atestados: • Bachiller en Informática, Ingeniería Industrial o afines. • Maestría en administración o gerencia de proyectos. • Incorporado al colegio respectivo. • SCRUM Certified o Project Management Professional (PMP) vigente. • Certificación ITIL Foundation. • Cinco (5) años de experiencia profesional. • Haber dirigido un mínimo de 3 proyectos de tecnología de información, donde esté involucrado la replicación de Bases de Datos Oracle, o Federación de Centros de Datos, podría ser una combinación de los anteriores. Debe indicar en la oferta la persona que fungirá dicho rol y debe adjuntar la respectiva hoja de vida con la experiencia y copia de las certificaciones.			
4	**PLAZO DE ENTREGA**			

4.1	**Para el Subítems 1.1**: El plazo máximo para la entrega de la sala dedicada exclusivamente para la CCSS será de 60 días naturales máximo, contados a partir del día siguiente a la notificación de disponibilidad de retiro del contrato.			
4.2	**Para el Subítem 1.2:** El plazo máximo para la entrega de los equipos y software debidamente instalado y configurado, será de 120 días naturales máximo, contados a partir del día siguiente a la notificación de disponibilidad de retiro del contrato.			
4.3	**Para el Subítem 1.3:** El plazo máximo para la entrega de los servicios de implementación para la replicación será de 60 días naturales contados a partir del día siguiente a la recepción definitiva del Subítem 1.2.			
4.4	**Para el Subítem 1.4:** El plazo máximo para la entrega de la Transferencia de Conocimiento es de 30 días naturales contados a partir del día siguiente a la recepción definitiva del Subítem 1.2			
5	**FORMA DE ENTREGA**			
5.1	Asimismo, dentro de los primeros 15 días hábiles a partir del día siguiente a la notificación de retiro del contrato, el contratista debe desarrollar al inicio de la ejecución contractual, al menos un taller que permitan al equipo de trabajo de la Caja Costarricense de Seguro Social CCSS conocer el plan de trabajo y la metodología a aplicar para la puesta en marcha del proyecto. Es responsabilidad del contratista suministrar el lugar, materiales, equipos e insumos necesarios para su realización y coordinar con la CCSS la fecha y hora de su realización, esto se debe coordinar con el encargado general del contrato.			
5.2	Una vez realizado el taller, 5 días hábiles posteriores, se realizará la reunión de "kick-off", la cual será programada por la CAJA, para dar inicio a las tareas del cronograma.			
5.3	El contratista debe presentar al inicio una fase de **Planificación del proyecto**: Esta fase tiene como objetivo orientar la ejecución del proyecto, facilitando el control y seguimiento, a lo largo de todo el plazo de implementación.			

5.3.1	**Plan de trabajo del Proyecto:** El contratista en la reunión de kick-off, debe entregar un plan detallado del proyecto que incorpore la metodología de trabajo en sus diferentes etapas y contener al menos los siguientes aspectos: • Plan del alcance (descripción de las etapas, entregables y metodología). • Plan de recursos (descripción de los recursos, matriz RACI, porcentaje de dedicación, disponibilidad, enlaces con el equipo de implementación). • Plan de riesgos (identificación, análisis y evaluación de los riesgos inherentes al proyecto, propuesta de planes de tratamiento y prevención). • Plan de comunicación (análisis de interesados, identificación de mensajes y canales para grupos de interés, programación y frecuencia de las comunicaciones). • Plan de calidad (criterios de aceptación, requisitos documentales) • Plan de seguimiento (frecuencia de seguimiento, formato de reportes de avance, indicadores de gestión). • Plan de tiempos (cronograma de trabajo que relacione la estructura de desglose de trabajo, los recursos y las actividades de comunicación, debe incluir agendas detalladas para todas las actividades de trabajo de campo requeridas en el proyecto con el fin de que la CAJA sea capaz de planificar la disponibilidad de los recursos).			
5.3.2	**Informes de seguimiento:** El contratista debe preparar informes (en formato digital) de seguimiento semanal, con el fin de reportar el estado del proyecto, considerando los siguientes aspectos: • Avance de las tareas planificadas para el período. • Descripción de los hallazgos y situaciones clave sucedidas en el periodo y que afecten la planificación del alcance o los tiempos. • Descripción de los cambios en la planificación sucedidos en el período. • Análisis de los riesgos e incidentes relacionados con el proyecto, detallando las acciones correctivas y preventivas necesarias. • Seguimiento de la ruta crítica del proyecto.			
5.4	Todas las actividades contempladas en este cartel deben ser consideradas en el Plan de Trabajo.			

5.4.1	**Al menos debe incluir las siguientes etapas:** • Etapa 1 Habilitación Servicios de alojamiento para la habilitación de un Centro de Procesamiento Alterno (CPA), enlaces de comunicación e internet. • Etapa 2 Reforzamiento y rediseño de Comunicaciones • Etapa 3 Federación de centros de datos • Etapa 4 Movimiento de equipamiento al CPA. • Etapa 5 Instalación y habilitación de servicios en el CPA capa de aplicaciones, bases de datos (EDUS, MISE, SICERE, MDI, SIGES, RRHH) y otros servicios que se encuentran en el apartado del Subítem 1.4. • Etapa 6 Capacitación/Transferencia de conocimientos y/o Adopción. • Etapa 7 Pruebas.			
5.4.2	El oferente debe aportar literatura técnica sobre cada uno de los componentes de la solución a cotizar, de manera que esta permita corroborar cada elemento técnico requerido.			
5.4.3	La documentación debe estar en idioma inglés o español.			
6	***LUGAR DE ENTREGA***			
6.1	Para el **subítem 1.1**, la sala exclusiva para la CCSS solicitada en este subítem, debe ser entregada en el Centro de Procesamiento Alterno, esto va ser en la ubicación que cumpla con los requerimientos técnicos solicitados ofrecido por el contratista.			
6.2	Para el **subítem 1.2**, los equipos y servicios deben ser instalados en el Oficentro Tecnológico en Llorente de Tibás contiguo a la escuela Anselmo Llorente y en el Centro de Procesamiento Alterno.			
6.3	Para el **subítem 1.3**, los Servicios deben ser entregados en el Oficentro Tecnológico CODISA en Llorente de Tibás contiguo a la escuela Anselmo Llorente y Centro de Procesamiento Alterno.			
6.4	Para el **subítem 1.4**, la transferencia de conocimiento debe ser entregada en el lugar que previamente coordinen el Contratista y el Encargado General del Contrato, en un área no mayor a 10 km de las Oficinas Centrales CCSS.			
7	**DESGLOSE DEL PRECIO**			
7.1	Debe presentarse un desglose de precios por Subítem con todos los componentes que conforman el objeto de la contratación.			
7.2	El precio se debe desglosar según lo dispuesto en los artículos 25, 26 y 27 del RLCA. Para lo cual, debe detallarlo de la siguiente manera: • Costo mensual y total del alojamiento. • Costo mensual y total de la infraestructura como servicio (IaaS). • Costo de implementación total. • Costo de cada transferencia de conocimiento unitario y total. • Precio total de la oferta.			

7.3	El contratista debe presentar en su oferta el desglose de la estructura del precio para el ítem único. Entre ellos: Mano Obra, Gastos Administrativos, Insumos y Utilidad.			
8	**GARANTIA DEL FABRICANTE.**			
8.1	Para los Subítems 1.2 el respaldo de la garantía del fabricante al contratista debe ser de al menos 36 meses			
8.2	Debe cubrir los repuestos originales necesarios para reparar el equipo, los gastos de envío o de desplazamiento y la mano de obra.			
8.3	Cada componente de hardware o software; deben ser aptos para el correcto funcionamiento de la solución indicada en este cartel.			
8.4	Debe garantizar el correcto ensamblado de cada uno de los componentes de hardware y software de los equipos para la solución indicada en este cartel.			
8.5	Cada equipo, componente de hardware o software; deben ser la versión más reciente que cumpla con el objeto de la solución y compatibilidad indicada en este cartel.			
8.6	Permitir actualizaciones y parchados liberados por el fabricante para el hardware y software de sistema operativo.			
8.7	Ante la eventual falla de alguno de los componentes de hardware que forman la solución, la misma deber ser reemplazada por otra idéntica.			
8.8	Después del cambio del componente dañado, el contratista debe brindar un reporte que contenga al menos la siguiente información: • Número de parte y serie del componente dañado y del nuevo. • Descripción del componente dañado y del nuevo. • Fecha del reemplazo.			
8.9	Si se determina que alguno de los equipos o componente presenta alguna anomalía en su empaque o estructura física normal que lo convierta en un elemento de futura funcionalidad sospechosa o de alto riesgo, debe ser inmediatamente reemplazado antes de ser configurado. La CCSS revisará en este proceso de entrega todos los productos y le indicará al oferente cuáles de ellos requieren de ser reemplazados sin ningún costo adicional para la Institución.			
9	**GARANTÍA DE CUMPLIMIENTO**			
9.1	El adjudicatario debe presentar una garantía de cumplimiento equivalente al **5%** del monto total adjudicado.			
9.2	La garantía de cumplimiento debe tener una vigencia de al menos **54 meses** a partir de la adjudicación en firme de la oferta.			
9.3	El adjudicatario cuenta con un plazo de 3 días hábiles para presentar la garantía de cumplimiento y demás documentos de requisitos de legalidad, contados a partir de la solicitud de estos documentos por parte de la CCSS.			
10	**DERECHOS Y CONFIDENCIALIDAD.**			

10.1	**Cláusula de confidencialidad:** En virtud de lo dispuesto por la Junta Directiva en el ARTICULO 25 de la sesión No. 7918, celebrada el 16 de diciembre del año 2004, la o las empresas que resulten adjudicadas que entregarán o desarrollarán productos que tengan que ver con Tecnologías de Información y Comunicación, se deben comprometer a mantener la mayor, reserva, discreción y secreto, respecto a todos los datos, diagramas, documentación, procesos y esquemas de cualquier índole (independiente del medio o formato por el que le hayan sido facilitadas) respecto de los cuales tuviere conocimiento o información en virtud de los servicios que le suministra a la CAJA o bien a sus alianzas estratégicas. La empresa contratista debe asegurarse que su personal cumpla con esta normativa dado que será la responsable del uso de dicha información tanto por parte de su personal, como del uso o divulgación que le den terceras personas sin el consentimiento previo por parte de la CAJA. Queda prohibido a la contratista y consecuentemente a su personal, revelar a cualquier tercero sin el previo y expreso consentimiento de la CAJA, cualquier dato o información al que haya tenido acceso con ocasión de la presente contratación o por el desempeño de su personal en las labores contratadas, o bien utilizar la información o conocimientos adquiridos con ocasión de la prestación de servicios a la CAJA, para cualquier otro fin que no sea el estipulado en el contrato, todo lo anterior bajo pena de tener por incumplido el contrato sin responsabilidad alguna por parte de la CAJA, pudiendo ésta ante un eventual incumplimiento reclamar los daños y perjuicios que el incumplimiento pudiere irrogarle, ya sea en sede administrativa o en sede judicial. Cualquier producto que se genere durante el periodo de la contratación será propiedad de la CAJA, por lo que los contratistas no pueden disponer de estos para cualquier otro fin, sin previa autorización de la CAJA. La violación de tal prohibición tendrá las mismas consecuencias previstas en el párrafo anterior. La presente cláusula tendrá validez hasta cinco (5) años después de finalizado o entregado el producto o programa objeto de la contratación.			
11	***FORMA DE PAGO***			
11.1	Todo pago se realizará sobre servicios o productos recibidos y contra acta de recepción definitiva por parte de la Comisión Técnica de la contratación.			
11.2	Una vez recibida la factura del contratista el trámite de pago será la forma usual de pago de la CCSS, 30 días naturales contados a partir del recibido del subítem correspondiente mediante el acta de recepción definitiva y de la correcta presentación de la factura digital por parte del contratista para su trámite de pago. A partir del recibo del Acta de Recepción Definitiva el contratista procede con la confección de la factura y su envío mediante el sitio WEB Institucional para la recepción de facturas electrónicas.			
11.3	**Para el subítem 1.1:** Se iniciarán los pagos mensuales a partir de la recepción definitiva del subítem 1.2 hasta que se cumpla el periodo estipulado de dicha contratación que será de 48 meses, para lo cual se levantará acta de recepción definitiva y de la correcta presentación de la factura digital por parte del contratista para su trámite de pago.			
11.4	**Para el subítem 1.2:** Se iniciarán los pagos mensuales a partir de la recepción definitiva hasta que se cumpla el periodo estipulado de dicha contratación que será de 48 meses, para lo cual se levantará acta de recepción definitiva y de la correcta presentación de la factura digital por parte del contratista para su trámite de pago.			

11.5	**Para el subítem 1.3:** Se hará un único pago por concepto de implementación de la Replicación y Recuperación de desastres para Servicios TIC on-premise, contados a partir de la recepción definitiva, para lo cual se levantará acta de recepción definitiva y de la correcta presentación de la factura digital por parte del contratista para su trámite de pago.			
11.6	**Para el subítem 1.4:** Se harán pagos únicos por concepto de cada Transferencia de Conocimiento que se brinde y se reciba a satisfacción de la Administración, contados a partir de la recepción definitiva de cada transferencia de conocimiento, para lo cual se levantará acta de recepción definitiva y de la correcta presentación de la factura digital por parte del contratista para su trámite de pago. • Transferencia de conocimiento del servicio de migración a nivel de comunicaciones. • Transferencia de conocimiento del producto Oracle Data Guard.			
11.7	Cada factura digital debe indicar mínimo lo siguiente: • Número de Licitación. • Número de Contrato. • Item y descripción. • Subítem y descripción. • Precio unitario. • Monto total de la factura. • Periodo en el cual se brindó el servicio (para los Servicios de Mantenimiento y Optimización).			
12	***VIGENCIA DE LA CONTRATACIÓN***			
12.1	El contrato estará vigente durante todo el plazo necesario para que el contratista cumpla con sus obligaciones.			
12.2	El contrato entrará a regir a partir del día siguiente a la notificación de la disponibilidad de retiro de la orden de compra o contrato por parte de la administración.			
12.3	La vigencia del contrato tendrá un plazo de 48 meses, por cada subtiem recibido a satisfacción (entiéndase satisfacción con cumpliendo del alcance estipulado en el requerimiento) de la CCSS.			
13	***CLAUSULAS VERDES***			
13.1	El oferente debe contar con un programa para el manejo y reciclaje de residuos electrónicos. El cual debe ser especificado dentro de la oferta.			
13.2	El oferente debe aportar documentación de los acuerdos que posee con empresas dedicadas al manejo de residuos electrónicos. La CCSS se reserva el derecho de contactar a la empresa para verificar el acuerdo.			
13.3	El oferente se debe comprometer a recibir para su debido tratamiento de reciclaje, los residuos electrónicos de los componentes a instalar en los equipos.			
13.4	El oferente debe aportar copia de la oferta en formato digital, en dispositivo de almacenamiento USB o CD ROM. No se aceptarán copias de la oferta en formato físico.			
14	***MULTAS***			

14.1	**Para los Subítem 1.2:** Si por mal funcionamiento de los equipos entregados, ocurre algún daño sobre la plataforma institucional de manera que causen interrupción de los servicios críticos que se brindan desde el centro de datos institucional, la Caja aplicará una multa de $1.000 por cada hora que el servicio que no se pudo brindar hasta un máximo del 25% del monto total adjudicado. La multa se rebajará de las facturas de pago, en caso de no existir facturas pendientes el contratista contará con tres días hábiles para realizar el pago a la cuenta que la Caja le indique.			
14.2	Para el Subítem 1.2: Si se presenta una interrupción en la prestación de servicios que brinda la institución debido a causas atribuibles al contratista por una mala práctica a la hora de realizar el mantenimiento preventivo y/o correctivo. Se aplicará una multa de $500.00 (quinientos dólares) por hora natural de tiempo fuera de línea del servicio que soporta la plataforma tecnológica institucional, hasta un máximo de 25% del monto correspondiente a ese semestre. Dichas multas se deducirán de las facturas pendientes de pago.			
14.3	**Para el subítem 1.3:** Si se presenta una interrupción en la prestación de servicios que brinda la institución debido a causas atribuibles al contratista por una mala práctica a la hora de realizar la implementación de la replicación. Se aplicará una multa de $500.00 (quinientos dólares) por hora natural de tiempo fuera de línea del servicio que soporta la plataforma tecnológica institucional, hasta un máximo de 25% del monto total adjudicado. La multa se rebajará de las facturas de pago, en caso de no existir facturas pendientes el contratista contará con tres días hábiles para realizar el pago a la cuenta que la Caja le indique.			
15	***CLÁUSULAS PENALES***			
15.1	De conformidad con el artículo 50 del RLCA, todo atraso en la entrega del **subítem 1.1** por concepto de Servicios de alojamiento para la habilitación de un Centro de Procesamiento Alterno (CPA), enlaces de comunicación e internet, se le aplicará una sanción de 1.0% por cada día natural de atraso, hasta completar el 25% del monto total adjudicado para el subítem 1.1. Esta cláusula penal se rebajará de las facturas pendientes de pago.			
15.2	De conformidad con el artículo 50 del RLCA, todo atraso en la entrega del **subítem 1.2** por concepto de Infraestructura como servicio (IaaS) y servicios para el rediseño y Actualización de la Infraestructura de Comunicaciones para el Centro de Procesamiento Primario y Alterno, se le aplicará una sanción de 1.0% por cada día natural de atraso, hasta completar el 25% del monto total adjudicado para el subítem 1.2. Esta cláusula penal se rebajará de las facturas pendientes de pago.			
15.3	De conformidad con el artículo 50 del RLCA, todo atraso en la entrega del **subítem 1.3** por Servicios de Implementación para la Replicación y Recuperación de Desastres para servicios TIC on-Premise, se le aplicará una sanción de 1.0% por cada día natural de atraso, hasta completar el 25% del monto total adjudicado para el subítem 1.3. Esta cláusula penal se rebajará de las facturas pendientes de pago.			
15.4	De conformidad con el artículo 50 del RLCA, todo atraso en la entrega del **subítem 1.4** por concepto de Transferencia de Conocimientos de la Solución adquirida, se le aplicará una sanción de 1.0% por cada día natural de atraso, hasta completar el 25% del monto total adjudicado para el subítem 1.4. Esta cláusula penal se rebajará de las facturas pendientes de pago.			
15.5	Si la visita de mantenimiento correctivo del subítem 1.2, se realiza posterior al tiempo de respuesta, solución o reparación, se aplicará una multa de $50.00 (cincuenta dólares) por hora de atraso, del monto correspondiente a ese semestre. Esta sanción se rebajará de la factura pendiente de pago hasta alcanzar un 25% de la factura del subítem correspondiente 1.2.			

15.6	Si el Informe del mantenimiento preventivo del **subítem 1.2,** se entrega posterior a los 5 días hábiles disponibles para la entrega de este, se aplicará una multa de $25.00 (veinticinco dólares) por día de atraso en la entrega de este, del monto correspondiente a ese semestre. Esta sanción se rebajará de la factura pendiente de pago hasta alcanzar un 25% de la factura del subítem correspondiente (1.2).			

Capítulo 2: Especificaciones Técnicas

Nº Ítem	Unidad	Cantidad	Descripción del bien o servicio
Único	**Ud**	**1**	**Solución para el fortalecimiento de la Infraestructura Redundante de Procesamiento de Información para el Centro de Procesamiento Primario (CPP) y el Centro Procesamiento Alterno (CPA).**
Subítem 1.1	Unidad	1	Servicios de alojamiento para la habilitación de un Centro de Procesamiento Alterno (CPA), enlaces de comunicación e internet.
Subítem 1.2	Unidad	1	Infraestructura como servicio (IaaS) y servicios para el rediseño y Actualización de la Infraestructura de Comunicaciones para el Centro de Procesamiento Primario y Alterno.
Subítem 1.3	Unidad	1	Servicios de Implementación para la Replicación y Recuperación de Desastres para servicios TIC on-Premise.
Subítem 1.4	Unidad	1	Transferencia de Conocimientos de la Solución adquirida.

Solución para el fortalecimiento de la Infraestructura Redundante de Procesamiento de Información para el Centro de Procesamiento Primario (CPP) y el Centro Procesamiento Alterno (CPA).

El objetivo de dicha contratación es seleccionar a un oferente que tenga la capacidad de poder fortalecer la red institucional actual entregando los componentes necesarios que se puedan integrar con los equipos que se encuentran en operación en el Centro de Procesamiento Primario (CODISA) y proveer todo el equipo complementario en el Centro de Procesamiento Alterno. Se busca habilitar a nivel de comunicaciones un esquema de recuperación de desastres reutilizando la infraestructura actual con que cuenta la CCSS en su centro de datos principal de manera tal que se habiliten los servicios de un Centro de Procesamiento Alterno CPA, mediante la integración de elementos complementarios que permitan cumplir con los objetivos internos de la institución.

Esta contratación es el primer paso dentro del roadmap institucional para proveer posteriormente al 100% de una arquitectura que le permita la continuidad de las operaciones de los servicios que se prestan a nivel nacional para toda la CCSS.

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
1.	**Subítem 1.1 Servicios de alojamiento para la habilitación de un Centro de Procesamiento Alterno (CPA), enlaces de comunicación e Internet.** Los servicios institucionales deben ser albergados en una suite privada exclusiva para la CCSS, no debe compartir racks con otros clientes. (Debe tener la capacidad de albergar al menos 10 racks).			
1.1.	Diseñado y construido bajo los lineamientos solicitados para edificios clase A (Edificaciones e instalaciones Esenciales), según definición “Clasificación de edificaciones según importancia” del			

Nº	***Descripción del Cartel***	***Cumple***		***Descrip-ción del oferente***
		Sí	***No***	
	Código Sísmico de Costa Rica vigente al momento de la construcción. Se deberá presentar una certificación firmada por un profesional con especialidad en Ingeniería Estructural, autorizado por el Colegio de Ingenieros y Arquitectos de Costa Rica donde se garantice que el Centro de Datos cumple con el Código Sísmico de Costa Rica.			
1.2.	Deberá ser un sitio con una ubicación física ideal tomando como referencia la ubicación del CPP (Centro de Procesamiento Principal) de la CCSS, debe existir al menos una distancia de 30 Km entre ambos sitios, esto con el propósito de minimizar la posible afectación de los mismos ante una eventualidad focalizada en sus alrededores y conforme a las buenas prácticas.			
1.3.	El CPA debe estar ubicado en un sitio que no se encuentre expuesto al alto tránsito vehicular del GAM, distante de aeropuertos, de la alta proliferación de industria así como lejos de sitios de almacenamiento de combustibles y procesamiento de químicos.			
1.4.	El edificio donde estará la (s) sala (s) de procesamiento de datos deberá ser de una sola planta, diseñado y construido con el único objetivo de brindar servicios de Data Center.			
1.5.	El edificio donde estará la (s) sala (s) de procesamiento de datos deberá con paredes que retarden la propagación del fuego como mínimo 2 horas.			
1.6.	El edificio donde estará la (s) sala (s) de procesamiento de datos deberá contar con la distribución de espacios separados, para hospedar los sistemas de soporte eléctrico, mecánico, de conectividad, de monitoreo y gestión, así como zonas para el almacenaje y des almacenaje de los equipos, de seguridad y vigilancia, debe contar con un recinto de pruebas de plataformas nuevas (cuarto de cuarentena), de resguardo de información sensible (sala cofre).			
1.7.	El edificio donde estará la (s) sala (s) de procesamiento de datos deberá contar con los espacios suficientes y necesarios para realizar labores de mantenimiento preventivo y correctivo a toda la infraestructura electromecánica de soporte.			
1.8.	El edificio deberá contar con muros exteriores completamente cerrados, construidos de manera sólida y robusta.			
1.9.	El Proveedor del centro de datos deberá instalar, operar y dar mantenimiento a los Sistemas de Suministro de Energía, Climatización, Gestión de Elementos Electromecánicos, Seguridad e Incendio, conformados por: acometidas eléctricas, transformadores, equipos de medición, líneas secundarias, cuadros o tableros de distribución, interruptores automático de transferencia, grupos electrógenos, unidades interrumpibles de energía, plantas de energía de corriente directa, bancos de batería de respaldo, unidades de climatización, sistema de detección, anunciación y supresión de incendio, control de acceso y seguridad, sistema de gestión de elementos electromecánicos, sistema de cableado estructurado, obras eléctricas misceláneas (iluminación, tomacorrientes y otros), sistemas de protección y puesta a tierra, y cualquier otro elemento necesario para			

Nº	Descripción del Cartel	Cumple		Descripción del oferente
		Sí	No	
	garantizar la confiabilidad y disponibilidad de la infraestructura electromecánica del Data Center.			
1.10.	El proveedor del centro de datos además de cumplir con todas las normas, estándares y/o reglamentaciones debe cumplir las listadas a continuación para la instalación y puesta en operación de los Sistemas de Suministro de Energía, Climatización, Gestión de Elementos Electromecánicos y Seguridad a suministrar: • NFPA 70, 72,100, 101, 110, 2001, 2010. • Ley N° 7593 “Instalación y Equipamiento de Acometidas Eléctricas” • IEEE STD 11-88-1996 para descargas de baterías. • ANSI/TIA/EIA 568, 569, 570, 606, 607,608, 942 últimas versiones y adendas. • ANSI IEEE estándar C-62.41-1991, para protecciones de voltajes transitorios. • IEC 555-2 Distorsión Armónica. • Norma UL 142 para tanques de combustibles. • Norma UL 2127. • Normas UL para uso en general. • ANSI C-62.91, y para uso general. • ASTM para uso en general. • Código Sísmico de Costa Rica. • Código de Seguridad e Higiene Ocupacional. • Norma Oficial para la utilización de colores de seguridad y su simbología. • Normas y regulaciones del MINAE para el almacenamiento de combustible. • Normas NEMA. • Normas ASA. • Norma MIL -1-24092. • Reglamento a la Ley de Igualdad de Oportunidades para Personas con Discapacidad. • Reglamento para el Tramite de los Planos y Conexión de los Servicios Eléctricos, Telecomunicaciones y de Otros en Edificios – CFIA. • Normas ISO 9001. • Ley No. 8228, “Ley del Cuerpo de Bomberos del Instituto Nacional de Seguros”. • Manual para redes de distribución eléctrica subterránea. 19.9/34.5 KV. CFIA. . ICE. CIEMI. CNFL. Julio 2006. • Norma de protección de Equipos e Instalaciones Eléctricas del Sistema Nacional de Telecomunicaciones. • ISO/IEC 27001 e ISO/IEC 17799. Estándar para la seguridad de la información. • NFPA 2001 Standard on Clean Agent Fire Extinguishing Systems_Edicion2000. • NFPA 72_National Fire Alarm Code_Edicion1999. • NFPA 75_Standard for the Protection of Electronic Com-puter-Data Processing Equipment			

Nº	***Descripción del Cartel***	***Cumple***		***Descrip-ción del oferente***
		Sí	***No***	
	• Estándar Uptime Institute, última versión			
1.11.	Para el cumplimiento de las normas, estándares y/o reglamentaciones se deberá emitir una declaración jurada que certifique el cumplimiento de las mismas.			
1.12.	El Centro de Datos debe cumplir con la certificación TIER III o superior por parte del UpTime Institute, esta certificación debe ser la de tipo "design".			
1.13.	El Edificio donde se encuentre ubicado el Centro de Datos debe estar en territorio costarricense en el Gran Área Metropolitana y estar al día en todos los permisos municipales y nacionales de funcionamiento necesarios para dar el servicio.			
1.14.	El Edificio donde se encuentre ubicado el Centro de Datos no debe estar en zonas que sean susceptibles a inundaciones o derrumbes. Para esto debe presentar un análisis de riesgo, tomando como base los estudios y/o información que sobre el particular genera la Comisión Nacional de Emergencias (CNE).			
1.15.	Debe contar con racks de uso exclusivo para la CCSS, de al menos 42U (unidades de altura para gabinetes).			
1.16.	El piso de la (s) sala (s) de procesamiento de datos debe soportar como mínimo 1,250 kilogramos por metro cuadrado. Se aceptarán ofertas de salas que posean tanto con piso de loza o piso falso de uso exclusivo para este centro de procesamiento de datos.			
1.17.	El interior de la (s) sala (s) de procesamiento de datos debe tener un espacio de 1 metro como mínimo entre el piso y la loza superior.			
1.18.	La (s) sala(s) de procesamiento de datos deberá estar ubicada en un edificio de un piso que evite inestabilidad estructural producida por fuerzas laterales mayores como: huracanes, vientos y sismos.			
1.19.	Todas las líneas de agua, aspersores, ductos, líneas de gas, etc. que sirvan a otras áreas del centro de datos, no deben pasar a través de la sala (s) de datos donde se ubiquen los servicios de la CCSS.			
1.20.	El Centro de Datos debe contar con un área para desalmacenaje de al menos 2 x 3 metros, así como un área de armado de al menos 2 x 3 metros.			
1.21.	Las paredes de la (s) sala (s), deben tener una resistencia al fuego de 1 hora como mínimo, por ende debe demostrar el cumplimiento con algunas de las normas: UPTIME, ICREA O BICSI, el oferente debe aportar una declaración de juramento o el informe de auditorio que compruebe lo solicitado.			
1.22.	Las puertas de la (s) sala (s) de datos deben tener como mínimo 120 centímetros de ancho por 210 centímetros de alto			
1.23.	La entrada de la (s) sala (s) de procesamiento de datos no debe tener poste central.			
1.24.	Las puertas de la (s) sala (s) de datos deben ser de un material sólido, preferiblemente metal, con un grosor mínimo de 4.5 centímetros.			
1.25.	El edificio del centro de datos debe contar con sistemas adicionales como luces de emergencia, sistema contra incendios, salidas de emergencia, señalización y extintores entre otros que minimicen el riesgo de accidentes y por ende la vida de sus			

Nº	***Descripción del Cartel***	***Cumple***		***Descrip-ción del oferente***
		Sí	***No***	
	ocupantes. Los sistemas contra incendios deben asegurar en todo momento que los equipos dispuestos en dichas salas no se vean afectados.			
1.26.	La (s) sala (s) para el procesamiento de datos debe contar con sensores para la detección de derrames.			
1.27.	La (s) sala (s) para el procesamiento de datos debe contar con sensores para la detección de incendios (humo).			
1.28.	La (s) sala (s) para el procesamiento de datos debe contar con sistemas para la detección temprana de incendios que complementen la acción de los sistemas de detección de humo.			
1.29.	El oferente debe proveer la interconexión a la red pública telefónica (ICE).			
1.30.	La (s) sala (s) para el procesamiento de datos debe contar con dos rutas independientes de conectividad.			
1.31.	Se debe asegurar que la temperatura de dicha sala asegure el óptimo funcionamiento de los equipos ahí instalados y que no exista condensación. Todo esto de acuerdo a los estándares y óptimos definidos por los fabricantes de la solución ofrecida.			
1.32.	El sitio debe contar con dos acometidas eléctricas, las cuales deben pertenecer a circuitos de distribución eléctrica independiente. (Dos subestaciones independientes)			
1.33.	Es imprescindible que al menos una acometida eléctrica sea subterránea desde la subestación eléctrica, esto minimiza al máximo las perturbaciones que las redes eléctricas aéreas sufren.			
1.34.	Todo lo relacionado con potencia deberá ingresar de manera subterránea al edificio. Esto se refiere a las acometidas eléctricas subterraneas.			
1.35.	El edificio donde se encuentre la (s) sala (s) de datos debe tener los dispositivos de transferencia eléctrica automatizados que se encargue de alimentar la sala de procesamiento de datos con los generadores eléctricos en caso de fallas en el fluido eléctrico de la red pública.			
1.36.	La (s) sala (s) de procesamiento de datos debe contar con respaldo de emergencia de generadores eléctricos, con capacidad de soportar la carga eléctrica total ofrecida como mínimo 8 horas continuas de operación.			
1.37.	Los Generadores deberán ser del tipo continuos, sin restricción de horas de uso a 100% de capacidad del centro de datos.			
1.38.	Los grupos electrógenos deberán estar dimensionados para soportar el 100% de la carga del Data Center.			
1.39.	Debe existir un esquema de configuración redundante N+1 o superior en los grupos electrógenos con equipos de igual potencia, de modo que permita operar el Centro de Datos bajo el concepto de concurrentemente mantenible.			
1.40.	El sistema de almacenamiento de combustible en el sitio deberá permitir una autonomía de operación de cómo mínimo 48 horas a plena carga en caso de una eventualidad de orden superior.			
1.41.	El sitio debe contar con múltiples bombas y tuberías de suministro de combustible.			
1.42.	El sitio debe contar con un sistema que permita la contención de posibles derrames de combustible (pileta anti derrames).			

Nº	***Descripción del Cartel***	***Cumple***		***Descrip-ción del oferente***
		Sí	***No***	
1.43.	El sitio debe contar con un sistema para asegurar el adecuado tratamiento de las aguas oleaginosas en caso de que se produzca un incidente relacionado a un derrame de combustible.			
1.44.	El oferente debe presentar en su oferta una declaración jurada donde se indique que tiene planes de abastecimiento de combustible que aseguren el relleno del (los) tanque (s) en caso de cortes eléctricos prolongados, tomado en cuenta días feriados, fines de semana y otras situaciones especiales como embotellamientos, bloqueos, derrumbes etc., que afecten el transporte terrestre, que permitan la operación continua de los servicios en el Centro de Datos.			
1.45.	El oferente debe adoptar las medidas correspondientes para asegurar que las emisiones y el ruido de los generador (es) eléctricos no interrumpan la operación diaria.			
1.46.	El oferente debe asegurar que en caso de corte de fluido eléctrico comercial, la operación de la sala de procesamiento de datos no salga de operación por alta temperatura mientras los sistemas de enfriamiento se reestablecen.			
1.47.	El oferente debe adoptar las medidas correspondientes, para que el (los) generador (es) eléctricos, aseguren el correcto enfriamiento durante el tiempo que sea necesario mantenerlo funcionando en caso de cortes en el fluido eléctrico.			
1.48.	Los generadores eléctricos deben estar colocados sobre una estructura que desvíe derrames y que además prevenga la vibración.			
1.49.	Los generadores eléctricos deben tener controles de operación que permitan: a. Asumir automáticamente la carga en caso de fallas en el fluido eléctrico. (Esto en conjunto con los dispositivos de transferencia eléctrica) b. Transferir a la alimentación eléctrica del servicio público una vez reestablecido el servicio después de un corte. (Esto en conjunto con los dispositivos de transferencia eléctrica)			
1.50.	La (s) sala (s) de procesamiento de datos debe contar con los sistemas ininterrumpido de poder (UPS) necesarios en configuración N+1 que sea capaz de abastecer la totalidad de consumo eléctrico de la sala mientras entra en operación el generador de emergencia en caso de cortes eléctricos de la red pública.			
1.51.	El sistema de potencia interrumpida (UPS) deberá contemplar el 100% de las cargas críticas del Data Center.			
1.52.	El sistema de potencia interrumpida (UPS) deberá considerar un sistema de baterías redundante que brinde una autonomía de cómo mínimo 15 minutos a la totalidad de la carga crítica del centro de datos.			
1.53.	El sistema de potencia interrumpida (UPS) deberá ser de doble conversión y en línea.			

Nº	***Descripción del Cartel***	***Cumple***		***Descripción del oferente***
		Sí	***No***	
1.54.	El lugar donde se ubiquen las UPS deben contar con el espacio necesario (al menos un metro libre entre equipos) para labores de mantenimiento, reparación, movimiento o retiro de equipos.			
1.55.	Se requiere que la ubicación del recinto donde se instalen las UPS quede prácticamente adyacente a la (s) sala (s) de procesamiento de datos.			
1.56.	Se deberá proveerse un bypass externo para el sistema de UPS, que debe ser parte integral del UPS, es decir deberá venir incorporado en un gabinete de fábrica.			
1.57.	Cada rack debe ser alimentado por al menos dos circuitos eléctricos por rutas diferentes (de 110v, 220v y 208v dependiendo de las necesidades de la CCSS) para poder conectar las fuentes de poder. La carga máxima requerida por cada uno de los racks es de 5KW o en su defecto una carga total de la (s) sala (s) completa (s) de hasta 200 KW para uso exclusivo de equipo electrónico ubicado en los racks, permitiendo un crecimiento de acuerdo a las necesidades de la CCSS.			
1.58.	El Proveedor debe suministrar los circuitos eléctricos que la CCSS requiera para la conexión en los racks.			
1.59.	El espacio (s) sala (s) a arrendar debe contar con sistemas de distribución eléctrica mediante soluciones de ducto-barra en alta disponibilidad para energizar los racks.			
1.60.	El oferente debe proporcionar todos los conectores de ducto-barra necesarios para iniciar la operación así como todos los conectores requeridos para la operación durante el tiempo de vigencia de la contratación.			
1.61.	Cada rack deberá contar con al menos dos PDU o regletas (una por cada brazo de alimentación), éstas deben ser administrables remotamente y con la capacidad suficiente en potencia y salidas para conectar los equipos del cliente.			
1.62.	Debe contar con personal de operación y mantenimiento disponible para los sistemas electromecánicos y estructurales, durante las 24 horas del día los 7 días a la semana, de manera que cualquier problema que se presente en estos elementos sea atendido de acuerdo a los tiempos de respuesta establecidos en este cartel.			
1.63.	El Centro de Procesamiento de Datos debe contar con sistemas de protección para equipo electrónico, tales como sistema de mallas y barras de tierras, descargadores de sobre voltaje, etc., todo según lo dispuesto por el Código Eléctrico Nacional vigente.			
1.64.	Se requiere dos circuitos independientes de alimentación eléctrica (de diferentes subestaciones). Estos circuitos deben estar desde el punto de entrega de la empresa distribuidora de energía eléctrica, usando cables de un solo tramo, sin empalmes o conexiones intermedias. Para el cálculo de la línea se debe tomar un factor de seguridad de 100% en la sección de los conductores para una caída máxima de voltaje de 2% para asegurar el correcto funcionamiento de los equipos informáticos.			
1.65.	Se debe conectar a la tierra física, la cual se conectará a través de un cable con cubierta aislante al centro de carga del área de cómputo.			

Nº	*Descripción del Cartel*	*Cumple*		*Descrip-ción del oferente*
		Sí	*No*	
1.66.	Todos los componentes del sistema eléctrico deben estar debidamente rotulados, marcados e identificados para su rápida operación por parte del personal autorizado.			
1.67.	La instalación eléctrica de los equipos informáticos y de telecomunicaciones del Data Center, deberá ser independiente de la de iluminación, de la de climatización y de la de los tomacorrientes para servicios generales y deberá estar correctamente identificada			
1.68.	Deberá contar en un lugar próximo a la puerta con un control para cortar la energía a todo el equipo de cómputo en cualquier situación de emergencia, y deberá estar debidamente señalizado			
1.69.	Se debe desinstalar y remover todo el cableado existente (eléctrico, lógico, telefónico, y de seguridad) que se encuentre en desuso dentro del área especificada, sin que esto afecte la operación de otras áreas dentro del edificio en forma parcial o permanente			
1.70.	La distribución eléctrica se hará por un ducto paralelo al que conduce la red de comunicaciones, y separado de éste por una distancia no menor a 25cm, excepto en el caso de que se utilicen ductos metálicos conectados a tierra para su conducción, caso en el que la distancia podrá ser menor.			
1.71.	La ocupación de los ductos utilizados para la potencia no deberá superar el 70% de su capacidad máxima.			
1.72.	El sistema de enfriamiento deberá contemplar el 100% de las cargas existentes en el Data Center.			
1.73.	Debe contar con sistemas de climatización que funcionen ininterrumpidamente y que mantenga la temperatura en 23°C con una fluctuación máxima de ± 2°C, y la humedad relativa entre el 40% y 60%.			
1.74.	En el caso de ofrecer sistemas de enfriamiento con agua helada, toda tubería de agua debe estar ubicada bajo piso falso y contar con sensores para la detección de derrames en esta zona.			
1.75.	El oferente deberá asegurar que en caso de que ocurra ruptura de alguna tubería de agua helada dentro de la sala de procesamiento de datos, el agua sea evacuada inmediatamente mediante un sistema de drenaje construido para ese propósito.			
1.76.	El sistema de enfriamiento por agua helada deberá contar con doble circuito de distribución que permita labores de mantenimiento o atención de fallas sin afectar el funcionamiento normal de la sala de procesamiento de datos.			
1.77.	La configuración de todo el sistema de enfriamiento debe ser N+1, esto aplica para Chiller, tuberías, bombas, manejadoras, torres de enfriamiento, válvulas.			
1.78.	Los racks deben estar alineados de forma contigua, de manera que se creen pasillos calientes y pasillos fríos para mejorar el enfriamiento de los equipos de cómputo que se ubicarán en ellos.			
1.79.	La ubicación de los componentes dentro de la sala de procesamientos debe evitar la recirculación de aire caliente o la mezcla de aire frio con aire caliente de retorno.			
1.80.	Con el propósito de un manejo eficiente de la carga térmica y para evitar puntos calientes o mezclas de aire frio y caliente El proveedor debe ser responsable por el aislamiento de pasillos			

Nº	*Descripción del Cartel*	*Cumple*		*Descrip-ción del oferente*
		Sí	*No*	
	calientes, fríos o cualquier otra área, utilizando materiales especializados retardantes a fuego.			
1.81.	El cableado de la sala o salas de datos no debe interferir con la circulación necesaria de aire para mantener la temperatura recomendada de los equipos de cómputo.			
1.82.	En el caso de ofrecer salas de datos con piso falso, las unidades de aire acondicionado deben estar ancladas de manera independiente, de manera que no transmitan vibraciones al piso falso.			
1.83.	La potencia eléctrica de los equipos críticos de aire acondicionado debe estar soportada por los generadores eléctricos. El aire acondicionado de la sala (s) de datos debe ser del tipo “continuous cooling”, de manera que siga operando en forma ininterrumpida junto a los demás equipos (servidores, almacenamiento, librerías de respaldo, equipos de comunicación, etc.) aun cuando haya fallas en el suministro eléctrico de la red pública.			
1.84.	Los sistemas de climatización para las salas del Data Center deberán contar con unidades de climatización de precisión, especialmente diseñadas para ser utilizadas en salas que alojan equipo electrónico sensitivo con alta generación de calor sensible y bajo condiciones de operación continua (24 horas al día, los 365 días del año) para mantener condiciones de temperatura y humedad en los ámbitos de control de los valores de ajustes de operación fijados para dichos parámetros respectivamente. En estas salas la configuración de los sistemas de climatización será tal, que se suministren la cantidad de unidades de climatización para mantener una configuración redundante del tipo n+1, tanto en capacidad de refrigeración como en alimentación eléctrica a las unidades.			
1.85.	Estos sistemas deben tener la capacidad de detectar automáticamente el fallo de una de las unidades y proceder a enviar la señal a la unidad más cercana a la que falló para que aumente su rendimiento supliendo la necesidad temporal.			
1.86.	Los sistemas de climatización para las salas en las que convivirá personal en forma permanente con equipos de tecnología de información u otros equipos que lo requieran deberán contar con unidades de climatización de confort, bajo condiciones de operación continua (24 horas al día, los 365 días del año) para mantener condiciones de temperatura y humedad en los ámbitos de control de los valores de ajustes de operación fijados para dichos parámetros respectivamente.			
1.87.	En caso de utilizar sistemas de climatización en base a agua en los cuartos eléctricos, el proveedor deberá tomar las precauciones para que en caso de fuga, los equipos eléctricos no se vean afectados, esto incluye sensores de líquido a nivel de piso y equipos elevados al menos 5 cm del nivel de piso terminado.			
1.88.	Se debe garantizar la seguridad física y perimetral de las instalaciones del centro de datos a través de personal de seguridad 24 horas al día por 7 días a la semana. Para lo cual el			

Nº	*Descripción del Cartel*	*Cumple*		*Descrip-ción del oferente*
		Sí	*No*	
	oferente debe presentar una declaración jurada en la cual se compromete a realizar esta actividad.			
1.89.	Todas las paredes de concreto del edificio donde se encuentre la (s) sala (s) de datos deben estar reforzadas desde su construcción con estructuras de varilla de hierro. Entregando la certificación correspondiente para validar el cumplimiento de la misma.			
1.90.	El edificio donde se encuentre la solución debe estar rodeada por una tapia o malla perimetral que impida el acceso de personas no autorizadas a las cercanías del edificio.			
1.91.	El espacio destinado para la sala de datos no debe tener ventanas.			
1.92.	La sala de procesamiento de datos debe tener como mínimo 3 niveles de seguridad o controles de ingreso: 1. Control de acceso a las instalaciones donde está el Centro de Procesamiento de Datos. 2. Control de acceso al edificio específico donde están ubicadas la (s) sala (s) de procesamiento de datos. 3. Control de acceso a la (s) sala (s) de procesamiento de datos donde se encuentre instalada la solución.			
1.93.	Las puertas de los gabinetes (racks) como niveles de seguridad o control de acceso, no se consideran dentro de los 3 niveles de seguridad solicitados.			
1.94.	El espacio de la (s) sala (s) de procesamiento de datos debe tener control de acceso biométrico para las personas autorizadas, que funcione en combinación ya sea con una tarjeta de acceso o una clave.			
1.95.	Todo acceso y cualquier movimiento generado en las instalaciones deben ser filmados por cámaras de vigilancia y grabado para su posterior análisis. Los videos deberán ser conservados y estar disponibles en el momento como mínimo 3 meses para su consulta posterior. Para la (s) sala (s) de Procesamiento de Datos se requiere un monitoreo de cámaras 7*24*365 en cada una sala. Condiciones de este monitoreo. i. Cámaras por movimiento de alta resolución. ii. Se deben cubrir todos los ángulos y pasillos entre cada rack. vi. La CCSS se reserva el derecho de solicitar los vídeos, cuando sea requerido.			
1.96.	Se debe garantizar que únicamente el personal autorizado por la CCSS o el oferente podrá acceder a la (s) sala (s) de procesamiento donde se encuentre instalada la solución, como por ejemplo terceros como partner que forman parte de la solución.			

Nº	*Descripción del Cartel*	*Cumple*		*Descrip-ción del oferente*
		Sí	*No*	
1.97.	Las puertas ubicadas en la (s) sala (s) y espacio (s) donde se encuentre la solución deben tener un bloqueo eléctrico, que impida su apertura.			
1.98.	Las puertas que dan acceso a la (s) sala (s) y espacio (s) donde se encuentre la solución deben tener un sistema de apertura interna que permita salir fácilmente, en caso de emergencia.			
1.99.	El edificio debe tener iluminación exterior como mínimo en las siguientes áreas: perímetro del edificio, puertas de acceso (vehicular, peatonal), puertas del edificio, lobbies, casetas de seguridad, todas las áreas públicas, aceras y escaleras.			
1.100.	El proveedor debe tener implementados planes y políticas de seguridad que incluyan como mínimo: políticas de control de acceso (peatones y vehículos), políticas de alarmas (incendios, acceso no autorizado), políticas de vigilancia, políticas de control de ingreso y salida de equipo. Cada oferente debe presentar declaración jurada del cumplimiento de este requisito.			
1.101.	Los visitantes del Data Center deben estar acompañados, en todo momento, por personal del oferente.			
1.102.	Una visita de emergencia será considerada como tal, solo ante un incidente de indisponibilidad de servicio.			
1.103.	Los visitantes deben guardar en todo momento las reglas de uso aceptable del Data Center que incluye: a. No se deben tomar fotografías b. No se deben abrir Racks o tocar equipos c. No se realizan trabajos físicos de equipos con personal que no sea del oferente o un proveedor certificado en el mismo d. No se abre falso piso o techo con personal que no sea del oferente en sitio por norma de seguridad de los visitantes e. Toda visita debe firmar su ingreso a las instalaciones.			
1.104.	La sala de procesamiento de datos debe tener un sistema de protección contra incendios de agente limpio que tenga como mínimo los siguientes elementos: • Un elemento de detección de incendios, como sensores de humo o calor. • Un elemento de protección, como materiales de construcción resistentes al fuego. • Un elemento de supresión, como por ejemplo gas Ecaro 25 u otro.			
1.105.	La sala de procesamiento de datos debe tener un sistema de detección temprana de incendios, que tome muestras del aire para determinar presencia de humo, mediante tuberías que tomen muestras de aire en lugares críticos de la sala.			
1.106.	Las áreas que tengan equipos electromecánicos como transferencias o tableros eléctricos deben contar con un sistema de detección de incendios.			

Nº	*Descripción del Cartel*	*Cumple*		*Descrip-ción del oferente*
		Sí	*No*	
1.107.	El elemento de protección debe contener la propagación de un fuego ya iniciado en cualquiera de las áreas de edificio donde esté ubicada la sala de procesamiento de datos: • Las paredes que dividan la (s) sala (s) de procesamiento de datos de cualquier cuarto eléctrico, mecánico o de comunicaciones deben tener una resistencia al fuego de mínimo 1 hora. • Las puertas de esas divisiones deben tener una resistencia al fuego de mínimo 1 hora. • El piso de la (s) sala (s) de procesamiento de datos y su loza superior deben tener una resistencia al fuego de mínimo 2 horas. • Cualquier mueble ubicado en la sala de procesamiento de datos debe ser retardante al fuego.			
1.108.	La sala de procesamiento de datos debe contar con un sistema limpio de supresión de incendios a base de gas, similar al ECARO 25, que sea inofensivo para la vida humana y que no produzca daños en equipos electrónicos. • El gas o agente limpio debe estar almacenado en un tanque dentro de la sala de procesamiento de datos. • En caso de activarse el sistema, el gas debe descargarse y crear una concentración suficiente para extinguir fuego y durar lo suficiente de manera que se prevengan re-igniciones. • Para descargar el gas deben existir al menos dos detectores activados, esto para minimizar falsos positivos.			
1.109.	La sala de procesamiento de datos no debe tener ningún recipiente para basura.			
1.110.	En caso de contar con piso falso, el área bajo el mismo debe contar con detectores de incendios.			
1.111.	El oferente debe tener políticas sobre tipo, ubicación y operación del sistema de detección y supresión de incendios.			
1.112.	El proveedor debe tener políticas sobre almacenamiento de combustible químicos y materiales.			
1.113.	La (s) sala (s) de procesamiento de datos debe contar con personal de monitoreo con capacidad de respuesta en caso de incendios.			
1.114.	Se proveerá para todas las áreas del Data Center un sistema de detección temprana, anunciación y supresión de incendio a base de agentes limpios			
1.115.	Se proveerá un sistema de detección temprana, anunciación y supresión a base de CO2 para las áreas de equipos electromecánicos			
1.116.	Los gabinetes deben ser de tipo estándar de al menos 42 U de altura con 19 pulgadas entre. En caso de equipo o equipos muy especializados, se debe trabajar el requerimiento en conjunto con			

Nº	*Descripción del Cartel*	*Cumple*		*Descrip-ción del oferente*
		Sí	*No*	
	el contratista para albergar los misos, ya sea en rack propietarios de la solución, o bien adapatar algún rack en la suite.			
1.117.	Los rieles de montaje vertical deberán ser ajustables ante cualquier requisito de montaje para el equipo de TI. Las posiciones U están numeradas por delante y por detrás para una rápida instalación del equipo.			
1.118.	Los gabinetes deben contar con puertas trasera y delantera del tipo ventilada.			
1.119.	Las puertas (delantera y trasera) de cada gabinete deben contar con un sistema de seguridad a base de combinación de números para su cierre y apertura.			
1.120.	Todos los racks deben estar provistos con puertas delanteras y traseras, con cerraduras y con paneles laterales.			
1.121.	Todos los racks deben tener mecanismos de administración de cableado tanto verticales como horizontales, tanto de red como eléctricos, cada cableado por separado.			
1.122.	En caso de existir piso falso, cualquier abertura para la entrada o salida de cables debe estar directamente bajo los mecanismos de administración de cableado.			
1.123.	Las aberturas para cableado en el piso falso no deben ser más grandes de lo necesario. Además deben tener dispositivos para evitar filtraciones de aire frio.			
1.124.	Todos los racks deben estar eléctricamente aterrizados.			
1.125.	Los racks deben permitir aterrizar eléctricamente todos los equipos que se instalen en ellos.			
1.126.	Todos los racks deben estar anclados al piso incluyendo una estructura sismo resistente que garanticen la estabilidad de los gabinetes.			
1.127.	Todos los racks deben estar nivelados por fila.			
1.128.	Los racks adyacentes deben estar unidos mediante tornillos, siempre que sea posible.			
1.129.	El proveedor debe proveer e instalar paneles en todas las aberturas que pudieran quedar entre los equipos de cómputo, como resultado de los requisitos de instalación particulares de cada equipo.			
1.130.	Las puertas de los racks deben permitir su desmontaje sin necesidad de herramientas.			
1.131.	Los paneles laterales deben ser removibles y deben tener cerradura para impedir su desmontaje.			
1.132.	Las unidades de distribución de potencia (PDU) que el proveedor suministre e instale en el Data Center, para alimentar los sistemas, equipos, cargas o gabinetes, deberán estar conectadas a circuitos eléctricos conectados a las ducto barras que permiten energizar cada gabinete. Debe suministrar redundancia (N+1) de los PDU. Se suministraran, instalaran y dejaran debidamente funcionando todos los PDU requeridos.			
1.133.	Se deben proveer líneas de comunicación mediante fibra óptica de tipo monomodo o multimodo desde los cuartos de comunicación de los proveedores de comunicaciones hasta la (s) sala (s) o espacio (s) donde se encuentre ubicada la solución.			

<table>
<tr><th rowspan="2">Nº</th><th rowspan="2">Descripción del Cartel</th><th colspan="2">Cumple</th><th rowspan="2">Descrip-ción del oferente</th></tr>
<tr><th>Sí</th><th>No</th></tr>
<tr><td>1.134.</td><td>La (s) sala (s) de procesamiento de datos debe incluir todo el cableado estructurado y patch panels necesarios para la activación del servicio, así como cualquier otro requerimiento de cableado y patch panels que resulte de nuevos servicios, durante todo el período de la contratación. Todo cableado deberá ser mínimo Categoría 6A o superior.</td><td></td><td></td><td></td></tr>
<tr><td>1.135.</td><td>Debe poseer una canastilla aérea de al menos 30 centímetros de ancho, interconectando todos los racks, para ubicar el cableado de datos, se deben de incluir ductos plásticos especialmente diseñados para la ubicación de cableados de fibra óptica.</td><td></td><td></td><td></td></tr>
<tr><td>1.136.</td><td>En el caso de cableado de datos bajo el piso falso, el cableado deberá estar ubicado en el pasillo caliente, en una canasta de al menos 30 centímetros de ancho.</td><td></td><td></td><td></td></tr>
<tr><td>1.137.</td><td>Para asegurar la capacidad de brindar el servicio durante el tiempo contratado el oferente deberá demostrar que es el propietario o tiene los derechos necesarios invariables sobre el inmueble donde se encuentra el área del Data Center.</td><td></td><td></td><td></td></tr>
<tr><td>1.138.</td><td>La disponibilidad del Centro de Procesamiento Alterno debe ser de al menos un 99.95%.</td><td></td><td></td><td></td></tr>
<tr><td>1.139.</td><td>La oferta debe contener las siguientes declaraciones juradas del oferente en original y con la firma respectiva (no copias):
Certificación por parte Comisión Nacional de Emergencia en la cual se indique que el lugar donde está edificio el CPD no está en una zona que sea susceptible a inundaciones o derrumbes. Al menos presentar alguna certificación de la entidad indicada anteriormente, no tiene que ser del año en curso.
Declaración jurada donde se indique que tiene planes de abastecimiento de combustible que aseguren el relleno del tanque en caso de cortes eléctricos prolongados, tomado en cuenta días feriados, fines de semana y otras situaciones especiales como embotellamientos, bloqueos, derrumbes etc., que afecten el transporte terrestre, que permitan la operación continua de los servicios ubicados en el espacio o espacios donde se encuentre la solución.
Declaración jurada que demuestre que al menos cuatro (4) empresas del gobierno operan en el centro de datos ofrecido.</td><td></td><td></td><td></td></tr>
<tr><td>1.140.</td><td>Este servicio debe contemplar el alojamiento de los siguientes equipos:<table><tr><th>Marca</th><th>Descripción</th><th>Can-tidad</th><th>Es-pacio en U</th><th>Consumo en Watts</th><th>En-trada</th></tr><tr><td>IBM</td><td>Power System 850C</td><td>1</td><td>4</td><td>8000</td><td>200-240V</td></tr><tr><td>IBM</td><td>PCI-E Expansion Drawer</td><td>1</td><td>4</td><td>300</td><td>100-240V</td></tr><tr><td>IBM</td><td>PCI-E Expansion Drawer</td><td>1</td><td>4</td><td>300</td><td>100-240V</td></tr></table></td><td></td><td></td><td></td></tr>
</table>

Nº	Descripción del Cartel	Cumple		Descripción del oferente
		Sí	No	

IBM	PCI-E Expansion Drawer	1	4	300	100-240V	
IBM	PCI-E Expansion Drawer	1	4	300	100-240V	
IBM	HMC	1	1	300	100-240V	
IBM	FlashSystem V9000 Storage Enclosure	1		450	200-240V	
IBM	System Networking SAN24B-5	1	1	80	100-240V	
IBM	System Networking SAN24B-5	1	1	80	100-240V	
Lenovo	Flex System Enterprise Chassis	1	10	12,900	200-240V	
EMC	Data Domain 6300	1	2	530	200-240V	
EMC	ES30 Expansion Shelf	1	3	230	100-240V	
EMC	ES30 Expansion Shelf	1	3	230	100-240V	
CISCO	MDS 9396T	1	2	555	100-240V	
CISCO	MDS 9396T	1	2	555	100-240V	
Totales		**15**	**45**	**25110**		

1.141.	Dada la necesidad de la habilitación del Centro de Procesamiento Alterno es requerido que el oferente considere dentro de su propuesta los siguientes elementos de comunicación.			
1.142.	Dos enlaces de Fibra Oscura entre el CPP y el CPA, que permitan la multiplexación de la red LAN y SAN, estos enlaces deben ser provistos por rutas distintas.			
1.143.	Un enlace de HUB de Fibra Oscura de al menos 800 Mbps			
1.144.	La CCSS será responsable del traslado del enlace actual de Internet que se encuentra ubicado en las oficinas centrales al nuevo CPA.			
1.145.	El adjudicatario debe participar brindando apoyo y coordinación en el proceso en el que CCSS ejecute el switch del rol como HUB Principal del enlace de Internet de Fibra Oscura de al menos 800 Mbps actual de Oficinas Centrales al CPP ubicado en CODISA. Dicho movimiento va ser responsabilidad de la CCSS.			
1.146.	El movimiento del actual enlace HUB de Oficinas Centrales al Centro de Procesamiento Principal, se encontraba bajo la responsabilidad de la CCSS.			
1.147.	En adición el oferente debe contemplar los costos de alojamiento para la Infraestructura como Servicio (IaaS), equipos que va a ser hospedados en este mismo Centro de Datos conforme a la solicitud del subitem 1.2, cumpliendo con todos los requerimientos estipulados en este punto.			
1.148.	El oferente debe contemplar los gastos de embalaje, seguros, desinstalación, instalación y transporte de los equipos que se indican en el punto 1.140 al CPA, estos equipos se encuentran ubicados actualmente en el piso 11 en el edificio de oficinas centrales de la CCSS, ubicado sobre la avenida segunda.			
1.149.	**Mesa de Ayuda**			
1.149.1.	El servicio de mesa de ayuda deberá de ser accesible al menos por los siguientes medios:			

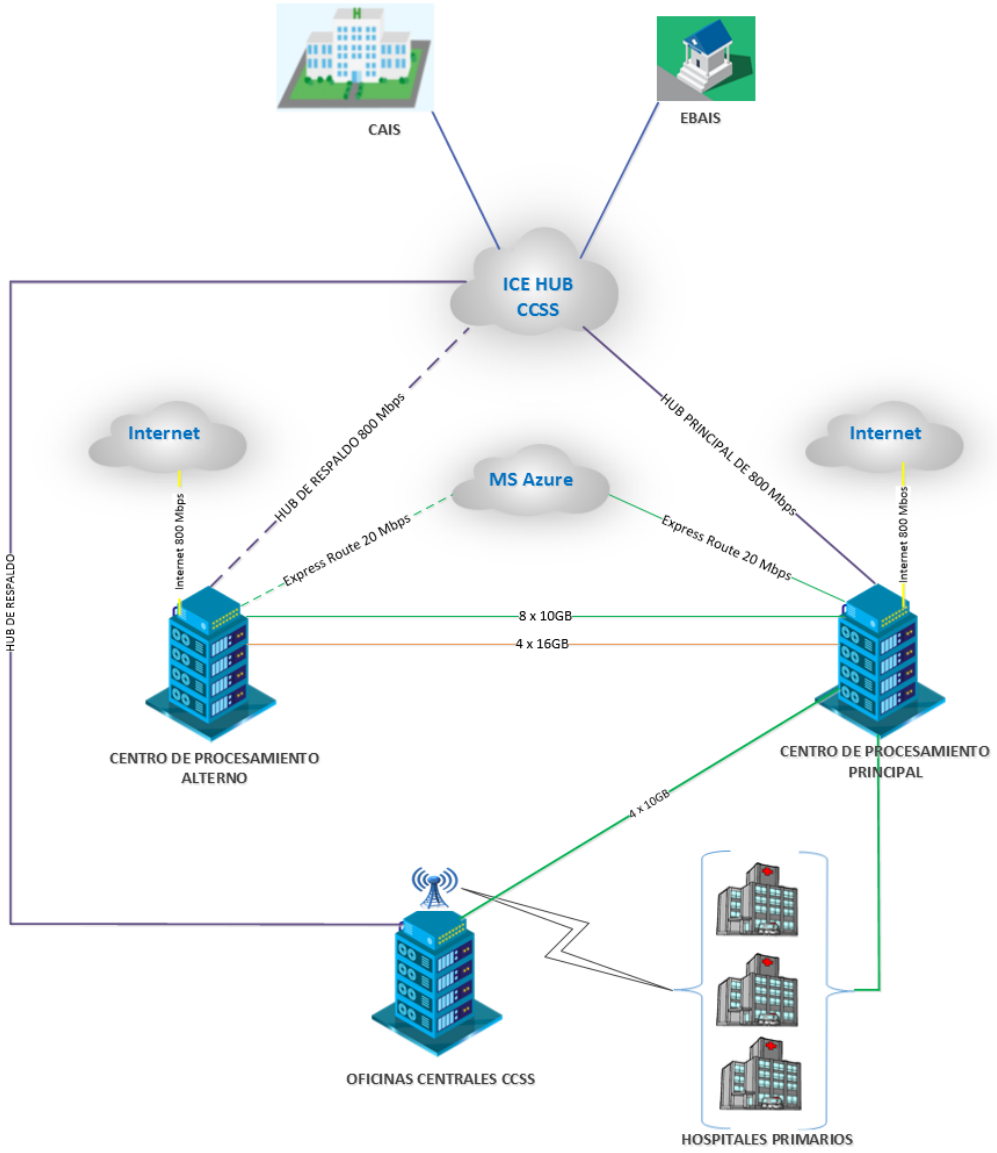
Nº	***Descripción del Cartel***	***Cumple***		***Descripción del oferente***
		Sí	***No***	
	a) Soporte telefónico: Deberá de brindarse un número telefónico para realizar los reportes de incidentes y requerimientos en un número local en el país. b) Correo Electrónico: Deberá de brindarse un correo electrónico donde se pueda colocar el reporte de incidente el cual deberá de responderse según el SLA establecido en el apartado de Niveles de Servicio c) Portal Web: Gestión de autoservicio para la apertura de tickets de soporte.			
1.149.2.	Los objetivos que debe cumplir para el servicio, son: ➢ Registro y Control Centralizado de Incidentes y requerimientos (End to End). ➢ Asignación de los recursos a grupos resolutores. ➢ Atención y solución de los incidentes y requerimientos reportados en forma remota. ➢ Seguimiento y Cumplimiento de SLAs comprometidos. ➢ Análisis estadístico y Gestión del Conocimiento (lecciones aprendidas). ➢ Entrega de Reportes mensuales sobre la gestión de Mesa de Ayuda.			
1.149.3.	Se debe colocar a disposición de la CCSS, operadores de Call Dispatch (Nivel 1) que tomarán las llamadas, Correos o Self Service vía Web, y registrarán los tickets en la herramienta proporcionada, asignarán los tickets al personal de soporte remoto/especializado del adjudicatario.			
1.149.4.	La mesa de ayuda dará seguimiento a cada uno de los incidentes y requerimientos hasta que lleguen a su status de cerrado. Todo esto realizado con personal altamente calificado que garantice el cumplimiento de dicho requerimiento.			
1.149.5.	Todo el servicio ofertado debe ser ejecutado aplicando las mejores prácticas de la industria y basados en los procesos de (ITIL).			
1.149.6.	Se debe considerar para brindar este servicio al menos la implementación complementaria de los siguientes procesos de ITIL: ➢ Gestión de Incidentes ➢ Gestión de Problemas ➢ Gestión de Eventos ➢ Gestión de la continuidad			
1.150.	**Niveles de servicio**			
1.150.1.	La medición de los niveles de servicio será de acuerdo a la naturaleza de cada Subítem donde así se amerite.			
1.150.2.	Para el Subíem 1.2 la medición de los equipos que se encuentren en sitio en el Centro de Procesamiento Principal (CODISA) va ser por tiempo de atención y reparación.			
1.150.3.	La indisponibilidad del CPA, y se calculará de la siguiente manera:			

Nº	*Descripción del Cartel*	*Cumple*		*Descrip-ción del oferente*
		Sí	*No*	
	Disponibilidad = 100% - (Σ (horas no disponibles del servicio) / (días-mes*24hrs)). Variables: • Disponibilidad: porcentaje de disponibilidad total por mes. • Horas no disponibles del servicio: tiempo expresado en horas en el cual el servicio no estudio disponible. • Días-mes: total de días del mes. Por cada incidente que interrumpa el servicio se computará la in-disponibilidad como el lapso que media entre cuando un incidente es registrado en el sistema, asignando el ticket correspondiente, y hasta que el mismo es reparado restableciéndose la continuidad del servicio.			
1.151.	**Reportes del servicio**			
1.151.1.	Reporte Gerencial – (Mensual) **Descripción**: Este debe resumir los aspectos más importantes ocurridos en el mes para el servicio. Su objetivo es entregar una vista general de los datos de entrada, cumplimiento de los SLAs y niveles de atención. El Reporte Gerencial debe contener: a) Datos de entrada (Correos, llamadas, autogestiones) b) Cantidad de Tickets por servicio c) Niveles de servicio entregados d) Cumplimiento de SLAs e) Recomendaciones / Lecciones aprendidas			
1.151.2.	➢ Consolidado de Tickets por Tipo-Servicio – (Semanal) **Descripción**: El consolidado debe mostrar todos los Tickets con todos sus campos, ordenados por tipo y Servicio **Contenido**: El consolidado será presentado en una hoja de cálculo electrónica que contendrá los campos básicos y dinámicos de todos los tickets, en un rango de tiempo especificado: • Numero de Ticket • Fecha de creación • Descripción • Usuario que reportó • Grupo Resolutor • Tiempo de asignación • Tiempo de notificación			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	• Fecha de cierre • Tiempo respuesta Grupo Resolutor • Estatus • Prioridad • Clasificación • Servicio • Resolución • Responsable			
1.151.3.	Taza de solución en primer nivel por Tipo-Servicio – (Mensual) **Descripción**: Taza de solución del primer nivel de solución, en el que se mostrará el nivel de solución obtenido por servicio. **Contenido**: El reporte se entregará en una hoja de cálculo electrónica, que mostrará: Servicio vs Taza de solución en primer nivel en el mes.			
1.151.4.	➢ Promedio de Tiempo de Resolución de Tickets por tipo-Servicio – (Mensual) **Descripción**: Este informe debe mostrar el tiempo promedio de resolución de los Tickets cerrados por servicio, remarcando los responsables de la ejecución. **Contenido**: El reporte tendrá la información básica del Ticket con el detalle del tiempo que tomo al responsable resolver el Ticket, ordenado por tipo-servicio: a) Numero de Ticket b) Fecha de creación c) Descripción d) Fecha de cierre e) Prioridad f) Clasificación g) Servicio h) Descripción i) Responsable j) Tiempo de solución			
1.152.	**Monitoreo**			
1.152.1.	Se debe proveer el monitoreo de los dispositivos que estaría aportando el oferente como parte del servicio, con una cobertura de 7x24.			
1.152.2.	El servicio del oferente debe tener la capacidad de administrar los eventos que se presentan dentro de la infraestructura como servicio, de los dispositivos complementarios para habilitar el CPA.			

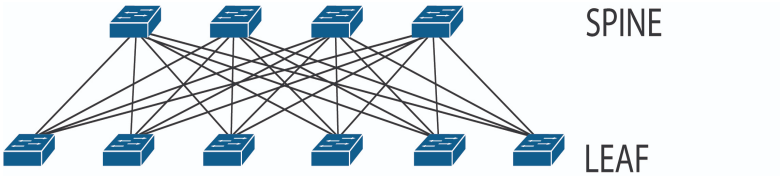
Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
1.152.3.	Configuración de umbrales mínimos en los parámetros en el monitoreo de los elementos incluidos en el servicio que permita la creación de eventos al caer por debajo del umbral definido. Al mismo tiempo la solución debe permitir la creación de incidentes por concepto de violación de umbrales en los elementos en el servicio.			
1.152.4.	Configuración de umbrales máximos en los parámetros en el monitoreo de los elementos incluidos en el servicio que permita la creación de eventos al superarse el umbral definido. Al mismo tiempo la solución debe permitir la creación de incidentes por concepto de violación de umbrales en los elementos en servicio.			
1.152.5.	El servicio de administración de eventos debe tener la capacidad de realizar notificaciones vía correo electrónico.			
1.152.6.	La frecuencia de monitoreo de umbrales para generación de eventos debe ser posible cambiarla de acuerdo al recurso o función monitoreada en el servicio.			
1.152.7.	El servicio debe estar en capacidad de procesar consultas por medio del protocolo SNMP enviados por los equipos y generar alarmas con base en estos eventos. Las alarmas críticas pueden generar diferentes acciones para notificación a la CCSS: - Correo electrónico - Creación de casos			
1.152.8.	Como parte del servicio de monitoreo el oferente debe contar con un centro de Operaciones que debe contar con al menos 5 años de Operación, el cual debe cumplir con lo siguiente: • El equipamiento de Red del Centro de Operaciones deberá estar debidamente instalado y acondicionado en un Centro de Operaciones independiente a otro centro de datos en caso de que existan ambos en un mismo edificio. • Este centro deberá contar con unidades de potencia eléctrica alterna que garanticen la continuidad de las operaciones (24 x 7) ante una falla del fluido eléctrico público, sistema de aire acondicionado, control de acceso electrónico y cámaras de seguridad. • Debe contar con, al menos 4 pantallas LCD o superiores para proyección del monitoreo. • Debe contar con sistemas de comunicación redundantes que garanticen la continuidad en la prestación de los servicios: - Doble enlace de Internet. - Doble equipamiento de Seguridad de la Red. - Doble equipamiento LAN.			
1.152.9.	El personal de la CCSS, se reserva el derecho de realizar visitas de inspección a las instalaciones del oferente durante el plazo de la contratación para verificar la infraestructura del centro de monitoreo y la correspondiente prestación de los servicios.			

Nº	***Descripción del Cartel***	***Cumple***		***Descripción del oferente***
		Sí	***No***	
1.152.10.	El oferente debe mostrar los indicadores de Monitoreo en temas de desempeño y disponibilidad de la Red del Centro de Operaciones de los últimos 12 Meses al personal de la CCSS, durante la visita de evaluación del oferente para comprobación de los puntos anteriores.			
1.152.11.	El oferente debe contar con un portal publicado de autoservicio para que la CCSS pueda consultar el estado del rendimiento del ambiente del servicio.			
1.152.12.	Este centro de operaciones debe operar y monitorear los servicios en una disponibilidad de 24 x 7 durante el plazo de la contratación.			
1.152.13.	Este centro de operaciones debe contar con al menos 20 clientes activos a los cuales se les esté prestando dicho servicio, para lo cual se debe presentar una declaración jurada con una lista de al menos el mínimo indicado la cual debe contener el nombre de la compañía, nombre del contacto, número de teléfono, la CCSS se reserva el derecho de confirmar la información.			
2.	**Visión final de referencia del proyecto**			

Nº	Descripción del Cartel	Cumple		Descrip-ción del oferente
		Sí	No	
2.1.				
3.	**Subítem 1.2 Equipamiento y servicios para el rediseño y Actualización de la Infraes-tructura de Comunicaciones para el Centro de Procesamiento Primario y Alterno.**			
	Alcance → • CPP; El Centro de Procesamiento Principal de la CCSS (en adelante CPP), está ubicado físicamente en CODISA, en Llo-rente Tibás, contiguo a la escuela Anselmo Llorente. Es importante aclarar que este factor no cambia con esta contratación.			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	• CPA; El Centro de Procesamiento Alterno de la CCSS (en adelante CPA), se planea contratar mediante las especificaciones de este cartel. • Los enlaces Inalámbricos con los que cuenta la Institución se encuentran hoy día en Oficinas Centrales; este factor no cambia con esta contratación. Este subítem tiene en varias secciones que detallan el requerimiento de los servicios a contratar: • Requerimientos Técnicos de Dispositivos para Conectividad del CPP. • Requerimientos de Arquitectura Lógica de la Solución de Conmutación del CPP. • Requerimientos Técnicos del Servicio de Integración de la Plataforma de Comunicaciones. • Requerimientos Técnicos de los Procesos de Migración hacia el Nuevo Ambiente de Comunicaciones.			
4.	**Situación de Red Actual**			
4.1.	La infraestructura de comunicaciones existente para el centro de datos principal en adelante denominado como CPP (Centro de Procesamiento Principal) está distribuida en varios módulos lógicos operativos asociados a los roles que se requieren para la presentación de servicios internos y externos a la organización. Estos bloques lógicos agrupan los dispositivos en función de la ubicación física y lógica en el flujo de tráfico de comunicaciones e incorporan elementos de varios ámbitos, tales como dispositivos de seguridad, conmutación, enrutamiento y otros. Estos segmentos del área de comunicaciones son los descritos a continuación: • Segmento CORE: es el área topológica de la red que permite la conmutación en alta velocidad para interconectar todos los bloques operativos. • Segmento Datacenter: permite la conectividad de red a los dispositivos de procesamiento internos estableciendo consideraciones de seguridad y enrutamiento entre este y el resto de los segmentos de la infraestructura. • Segmento de Borde: es el área de la topología de comunicaciones donde se agrupan los dispositivos que permiten establecer la comunicación desde y hacia los diferentes medios de comunicaciones existentes, tales como enlaces de datos públicos y privados, y otro tipo de conexiones hibridas. Si bien la infraestructura topológica de la red de comunicaciones cuenta con la segmentación descrita anteriormente, algunos de lo			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	módulos operativos disponibles no cuentan con todas las características necesarias para ofrecer los servicios de forma completamente autónoma. En las siguientes secciones se amplía respecto a esta consideración. La arquitectura existente cuenta con un segmento de comunicaciones para servicios de procesamiento ubicado en el Edificio de Oficinas Principales. Este bloque topológico se conoce como Centro de Procesamiento Alterno, en adelante denominado CPA. En el CPA se cuenta con la misma estructura modular existente en el CPP sin embargo existe un módulo adicional que provee conectividad de red a los usuarios ubicados en los 2 edificios de la Oficina Principal de la CCSS. Este segmento de denomina "Segmento de Agregación de Usuarios". Adicionalmente, el ambiente de comunicaciones de red del CPA es el punto donde se centralizan la mayoría de los enlaces de comunicaciones externos (privados y no privados) que se utilizan para la provisión del servicio. Es importante considerar que la información provista en este documento tiene el propósito de ofrecer al oferente una visión general de la operación de red actual de tal forma que se pueda contextualizar con respecto a las circunstancias globales actuales. No se ha incluido información específica y puntual respecto a elementos físicos o lógicos de la red actual debido a que será responsabilidad del oferente, una vez adjudicado, ejecutar los procesos de levantamiento de información y ejecución de los procesos de documentación descritos posteriormente y que se consideran como parte del servicio. La oferta de servicios deberá ser provista basándose en la información general propuesta. A continuación, se hace referencia detallada a la arquitectura de comunicaciones existente en el CPP y CPA.			
4.2.	**Segmento de CORE** El segmento CORE permite la conectividad de red entre los diferentes módulos operativos de la tecnología de comunicaciones. Particularmente, en el CPP, el segmento CORE está basado en una pareja de dispositivos Cisco Nexus 7010, donde de momento, se maneja la comunicación hacia el bloque de interconexión de servidores (Segmento de Datacenter), pero donde se interconectan directamente los dispositivos disponibles del ambiente de borde en una estructura colapsada, es decir, los dominios de broadcast del segmento de borde están integrados en el mismo contexto o VDC donde está funcionando operativamente el segmento de CORE. En el CPP los dispositivos actuales de comunicaciones están configurados con mecanismos para ofrecer servicios de alta disponibilidad como protocolos de enrutamiento dinámico y protocolos de redundancia de primer salto como HSRP.			
4.3.	**Segmento de DataCenter**			

Nº	Descripción del Cartel	Cumple		Descripción del oferente
		Sí	No	
	El segmento de Datacenter tiene como propósito ofrecer conectividad de red a los elementos que ejecutan los servicios de procesamiento y que proveen los servicios que la organización dispone para los usuarios internos y externos. En el caso del CPP, existe un ambiente de comunicaciones independiente basado en dispositivos Cisco Nexus 9000 en modalidad de “Software Define Networking”. Este segmento está implementado en un modelo topológico denominado “Leaf Spine” que provee conectividad de red a los dispositivos de procesamiento comportándose prácticamente como un solo dispositivo y manteniendo un plano de control centralizado.  El ambiente de comunicaciones existente en el CPP cuenta con un clúster de 3 dispositivos de control operando en modo activo-activo-activo, proveyendo disponibilidad N + 2. Con relación al modelo de seguridad actual, en el caso del CPP, la solución de comunicaciones permite la integración de dispositivos contrafuegos para establecer reglas de control de acceso entre segmentos de red externos y el Datacenter. Esta integración permite también que se puedan establecer flujos de comunicación lógicos de tal forma que no sea necesaria la interconexión física de dispositivos en el paso del tráfico ya que se pueden establecer condiciones lógicas del flujo de tráfico y forzar que este transcurra a través de dispositivos de seguridad tales como contrafuegos, IPS o balanceadores de carga. En resumen, la estructura topológica de interconexión en el segmento de Datacenter del CPP se maneja de forma completamente lógica y no requiere de esquemas especiales de interconexión de red. En el ambiente de procesamiento virtualizado del CPP existen conmutadores lógicos que proveen conectividad a las máquinas virtuales existentes. Estos conmutadores lógicos han sido integrados con el modelo de gestión y plano de control centralizado de tal forma que la estructura de flujos lógicos de comunicación involucra la microsegmentación de servicios extensibles hasta el ambiente de procesamiento virtual. Cabe mencionar que esto aplica únicamente en el caso del CPP ya que en el caso del CPA no se cuenta con esta tecnología y los modelos de provisión de comunicación son más convencionales pues están basados en la segmentación tradicional de VLAN. Para mitigar el riesgo en el pase a operación de la solución y su posterior soporte y optimización, los servicios de implementación			

<table>
<tr><th rowspan="2">Nº</th><th rowspan="2">Descripción del Cartel</th><th colspan="2">Cumple</th><th rowspan="2">Descripción del oferente</th></tr>
<tr><th>Sí</th><th>No</th></tr>
<tr><td></td><td>deben involucrar la participación del fabricante directo de los equipos en conjunto con el oferente, las tareas a realizar durante esta implementación deben ser distribuidas de la siguiente manera
<table>
<tr><th>Fase</th><th>Actividad</th><th>CISCO</th><th>Oferente</th></tr>
<tr><td rowspan="4">Planeamiento</td><td>Gerente de proyecto de inicio a fin</td><td>X</td><td>X</td></tr>
<tr><td>Taller de descubrimiento (ACI evaluación de adopción)</td><td>X</td><td>X</td></tr>
<tr><td>Documentación de requerimientos</td><td>X</td><td></td></tr>
<tr><td>Colección de requerimientos</td><td>X</td><td></td></tr>
<tr><td rowspan="3">Diseño</td><td>Documentación de encuesta en sitio</td><td></td><td>X</td></tr>
<tr><td>Documentación de diseño</td><td>X</td><td></td></tr>
<tr><td>Equipamiento listo para el uso</td><td></td><td>X</td></tr>
<tr><td rowspan="6">Implementación</td><td>Cableado e instalación física</td><td></td><td>X</td></tr>
<tr><td>Equipamiento listo para su ejecución o función</td><td></td><td>X</td></tr>
<tr><td>Implementación del fabric</td><td>X</td><td></td></tr>
<tr><td>Integración (L4-L7/ Hipervisores)</td><td>X</td><td></td></tr>
<tr><td>Ejecución de plan de pruebas</td><td></td><td>X</td></tr>
<tr><td>Transferencia de conocimiento</td><td>X</td><td></td></tr>
<tr><td rowspan="5">Migración</td><td>Integración con los Hipervisores</td><td>X</td><td></td></tr>
<tr><td>Plan de migración de red para 4 aplicaciones</td><td>X</td><td></td></tr>
<tr><td>Calendarización del cambio de soporte MW para 4 aplicaciones</td><td>X</td><td></td></tr>
<tr><td>Soporte Post-Implementación para 4 aplicaciones</td><td>X</td><td></td></tr>
<tr><td>Plan de migración de red para las aplicaciones remanentes</td><td></td><td>X</td></tr>
<tr><td>Calendarización del cambio de soporte MW para aplicaciones remanentes</td><td></td><td>X</td></tr>
<tr><td>Soporte Post-Implementación para aplicaciones remanentes</td><td></td><td>X</td></tr>
</table></td><td></td><td></td><td></td></tr>
<tr><td>4.4.</td><td>Situación Actual del Segmento de Borde y Periferia

El segmento de borde y conexiones periféricas permite la interconexión de los segmentos internos y externos hacia el CORE y Centro de Datos para consumir los servicios de procesamiento proporcionados.
En esta sección se consideran los segmentos de borde de conexiones externas y periféricas, así como las conexiones de usuarios finales recibidas en las oficinas administrativas denominadas como Oficinas Centrales.</td><td></td><td></td><td></td></tr>
<tr><td>4.5.</td><td>Segmento de Borde

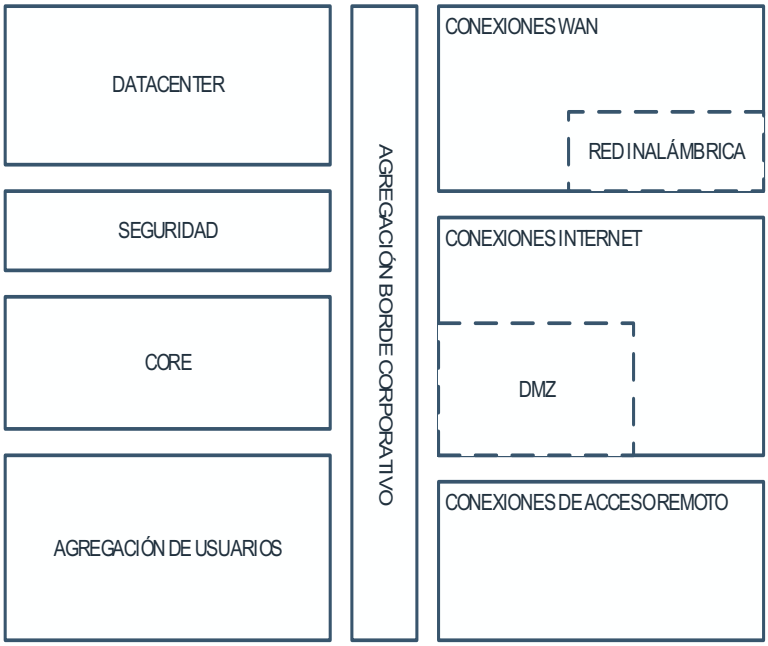
El segmento de borde tiene como propósito centralizar los diferentes enlaces de comunicaciones que interconectan tanto el CPP y CPA con el resto del mundo, sea por medio del Internet o bien a través de los enlaces de datos privados contratados a oferentes de servicios.

En el caso particular de los servicios de comunicaciones de borde, existes varias condiciones operativas singulares que deben ser consideradas para tener una visión contextual e integral de la operación actual.</td><td></td><td></td><td></td></tr>
</table>

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	En primer lugar, si bien el CPP se considera como el punto principal de manejo y prestación de servicios, es en Oficinas Centrales donde de momento se centraliza la conectividad de red en relación con los enlaces de datos privados o públicos. La CCSS cuenta con una serie de conexiones de red hacia diferentes ámbitos tales como instituciones gubernamentales, instituciones financieras privadas, hospitales y clínicas periféricas, y por supuesto enlaces de Internet. Para la conectividad WAN (Wide Area Network) que se proporciona hacia los hospitales y clínicas periféricas, la CCSS cuenta con una infraestructura inalámbrica propia, donde se habilita la comunicación como mecanismo principal hacia algunas de las sucursales, manteniendo enlaces con oferentes de servicios como medio alternativo de comunicación. En este particular existen diferentes condiciones operativas, ya que las condiciones varían en función de la ubicación física de cada punto periférico que requiere conectividad. Para la operación apropiada y segura de los enlaces de datos, se han provisto diferentes mecanismos que optimizan los servicios transportados, así como fortalecen los principios de seguridad establecidos en este ámbito de red. Como en cualquier ambiente de comunicaciones, existen dispositivos contrafuegos e IPS con el fin de asegurar el flujo de red con los diferentes enlaces de borde disponibles. De igual forma se dispone de dispositivos para concentración de conexiones VPN de acceso remoto y de sitio a sitio. Para el caso de los enlaces con Hospitales y Clínicas, se ha aprovisionado una solución que permite la optimización de flujos de comunicaciones, estableciendo políticas de utilización de ancho de banda entre los centros de datos y cualquiera de las sucursales periféricas. En el caso particular del CPP, las sucursales remotas no tienen de momento conexión directa hasta este centro de datos, debido a que no se han habilitado enlaces de oferentes de servicios hasta su ubicación física. De igual forma, dadas las condiciones geográficas del CPP no es posible habilitar una interconexión entre los nodos inalámbricos hasta este centro de datos, por lo que la posibilidad de utilizar el CPP como punto central de comunicación no es viable. Por lo anterior, la mayoría de los servicios de borde han sido habilitados únicamente en Oficinas Centrales y es por medio de los enlaces de fibra oscura entre CPP y Oficinas Centrales que se pueden consumir los servicios de procesamiento de datos ubicados en el sitio primario.			
4.6.	**Segmento de Agregación de Usuarios** La infraestructura de comunicaciones de Oficinas Centrales está			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	complementada con un segmento operativo denominado "Agregación de Usuarios", el cual permite la conectividad de red a los conmutadores que a su vez interconectan los usuarios ubicados en los 2 edificios de Oficinas Centrales de la CCSS. En el caso particular de Oficinas Centrales, actualmente se cuenta con una pareja de dispositivos Nexus 9500 que operan como dispositivos CORE para agregar las conexiones de los segmentos de agregación de usuarios y la de dispositivos CORE. Cada edificio de oficinas cuenta con dispositivos de agregación de la familia Cisco Catalyst 4500X, que funcionan como punto central de interconexión para los diferentes conmutadores ubicados en cada uno de los pisos donde se encuentran oficinas de usuarios. Estos dispositivos de agregación a su vez se interconectan con los dispositivos CORE que centralizan la comunicación de toda la infraestructura. La estructura lógica está basada en mecanismos de segmentación tradicionales, donde son los elementos de agregación los que definen la segmentación de la red en diferentes VLANs, y para cada una se establece su segmento de red IP.			
5.	**Requerimientos Técnicos de Arquitectura de Comunicaciones General** Si bien las condiciones establecidas en este documento definen que el requerimiento del servicio se hace en relación con la definición de la estructura de comunicaciones del Centro de Procesamiento Alterno, es necesario que el servicio sea considerado de forma integral, contemplando actividades de adaptación necesarias en ambos Centros de Procesamiento para lograr los objetivos planteados por la organización. Como consideración especial, se debe tomar en cuenta que la solución de comunicaciones a implementar para el CPA puede no estar ubicada en las mismas premisas donde actualmente opera el Centro de Datos de Oficinas Centrales, por lo que los diseños preparados deben considerar las implicaciones de trasladar o reestructurar los servicios de comunicaciones basados en que la ubicación del Sitio Alterno estará ubicado en cualquier locación dentro del territorio nacional. Los diseños topológicos propuestos deben proveer la flexibilidad y adaptabilidad para que se consideren las 3 observaciones descritas a continuación: A. Que el CPA sea ubicado en un punto que requiera la implementación de mecanismos de configuración e integración hacia la red corporativa de Oficinas Centrales por			

Nº	Descripción del Cartel	Cumple		Descripción del oferente
		Sí	No	
	medio de enlaces de datos. B. Que los servicios de red inalámbrica de interconexión hacia hospitales y clínicas que actualmente se utiliza como método de conexión primaria no puede ser migrado al Sitio Alterno y deben proporcionarse mecanismos de interconexión indirecto a Oficinas Centrales para considerársele como un tercer nodo dentro del modelo topológico. C. El nodo de oficinas centrales debe tener interconexión hacia ambos centros de datos CPP y CPA para asegurar disponibilidad de acceso, no solo de los usuarios de la red administrativa, sino de las interconexiones indirectas por medio de la red inalámbrica hacia hospitales y clínicas.			
5.1.	Los objetivos o premisas establecidas para el servicio son descritas a continuación: • En primer lugar, uno de los principales objetivos de la organización en cuanto al servicio, es que ambos centros de comunicaciones cuenten con las mismas condiciones operativas, es decir, que todos los servicios de red disponibles en el CPP estén habilitados también en el CPA y viceversa. • En relación con el punto anterior, la solución de comunicaciones debe proveer mecanismos de comunicación tales que, desde el punto de vista del servicio o dispositivos de procesamiento, sea indiferente estar en uno u otro Centro de Datos. Esto implica, una extensión de datos transparente pero que no comprometa la integridad operativa de los centros de datos entre sí. • La solución de comunicaciones debe proveer elementos que limiten en la medida de lo posible mecanismos de convergencia que impliquen interrupción temporal del servicio, se debe garantizar la continuidad operativa en todo momento. • Todos los componentes de hardware y software requeridos para la operación del servicio deben contar con mecanismos internos de disponibilidad, y deben ser diseñados de forma redundante, de tal forma que la indisponibilidad parcial o total de un dispositivo no comprometa la operación del servicio. • Dado que se trabajará sobre una red productiva, es necesario que los métodos de implementación, integración y migración sean no disruptivos, de modo que durante el proceso de establecimiento de la solución no exista indisponibilidad del servicio. Las ventanas de mantenimiento necesarias serán programadas, sin embargo, es necesario que se diseñen mecanismos que reduzcan la cantidad de interrupciones programadas. • En la medida de lo posible, debe lograrse la reutilización de los dispositivos de comunicaciones existentes, incluyendo las			

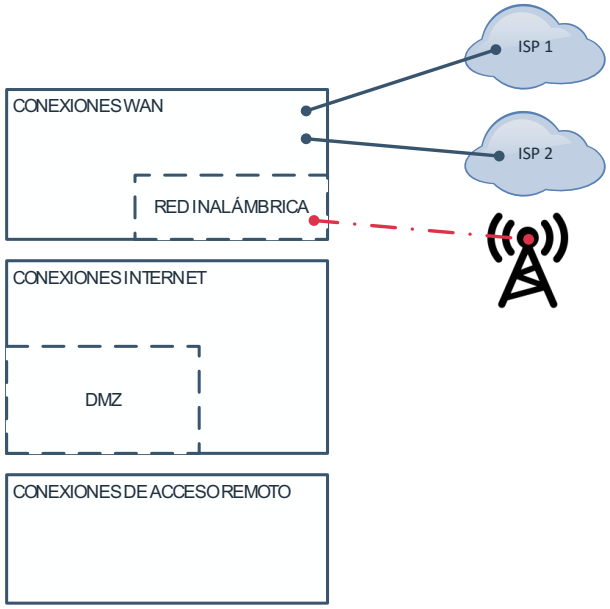
Nº	***Descripción del Cartel***	***Cumple***		***Descripción del oferente***
		Sí	***No***	
	soluciones de seguridad, balanceo de carga y soluciones de optimización de ancho de banda.			
5.2.	Una vez definidas las bases del servicio, es necesario establecer ciertas condiciones técnicas asociadas con las preferencias de la organización, respecto a la estructura general del servicio. La estrategia definida por la organización es la segmentación de la infraestructura de comunicaciones en módulos, de tal forma que se puedan realizar procesos de especialización en cada uno de los segmentos operativos, optimizando así el rendimiento de cada dispositivo y reduciendo los tiempos en el aprovisionamiento y resolución de fallas.			
5.3.	En función de esta premisa, se requiere que como parte del servicio se tome en consideración el siguiente modelo segmentado en la definición de la estructura topológica de comunicaciones:  Dadas las condiciones operativas existentes, es necesario que el oferente prepare la estructura topológica de comunicaciones en función de las siguientes consideraciones operativas de cada bloque:			
5.3.1.	**Segmento de DataCenter** Las condiciones para el servicio solicitado requieren que el segmento de DataCenter provea conectividad de red ethernet a los elementos de procesamiento que también serán habilitados en el CPA. Dado que ya se cuenta en el CPP con una arquitectura de comunicaciones para el Datacenter que esta basada en tecnología de “Software Define Networking” se quiere que la nueva infraestructura de comunicaciones del CPA se pueda integrar			

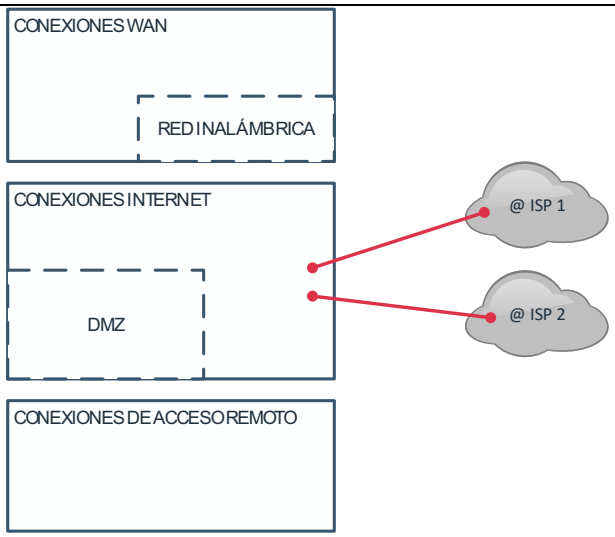
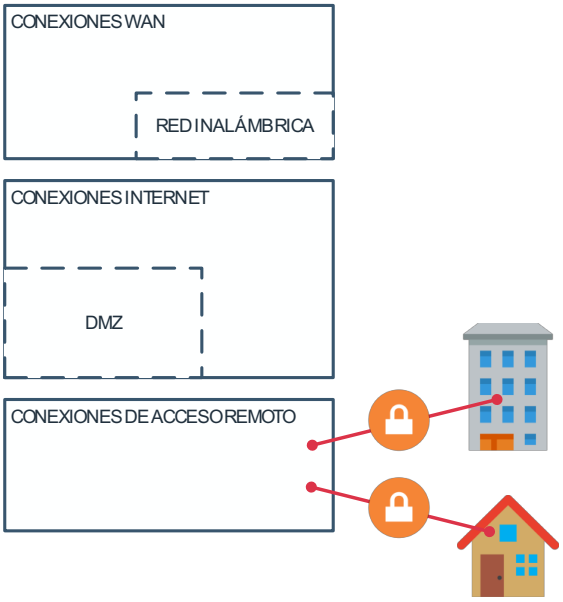
Nº	Descripción del Cartel	Cumple		Descripción del oferente
		Sí	No	
	transparentemente al mismo modelo de gestión y aprovisionamiento. También es necesario que se pueda realizar una integración transparente a nivel del plano de datos debido a que los servicios de procesamiento deberán estar habilitados en condiciones que permitan la movilidad dinámica de elementos de procesamiento que no requieran modificaciones en la estructura de red. Los dominios de broadcast donde está ubicados los servicios de procesamiento en el CPP deben ser extendidos y estar también disponibles en el CPA. La organización prefiere que la estructura de comunicaciones de Datacenter en CPP y CPA se comporte como un solo segmento integrado para facilitar la transición de servicios entre ambos puntos. Es importante considerar que en algún momento la organización puede requerir la utilización de la infraestructura del CPA como punto principal para la habilitación de servicios, y por lo tanto las condiciones deben estar dadas para que esto sea posible sin que se requieran modificaciones adicionales o procesos de convergencia, excepto aquellos necesarios para habilitar el puerto físico o lógico donde se conectará el elemento trasladado o habilitado. El segmento de DataCenter está interconectado al segmento de CORE, sin embargo, hay un bloque operativo a considerar que permite la habilitación de mecanismos de control de acceso e inspección del tráfico de red desde y hacia otras partes de la red. Tradicionalmente se habilitan dispositivos en línea que examinan e inspeccionan el 100% del tráfico del DataCenter, no obstante, se requiere que la solución de comunicación implementada permita la flexibilidad de incorporar dispositivos de seguridad para examinar flujos de tráfico específicos que estén asociados a comunicación vertical y horizontal en le DataCenter. Esto requiere que la plataforma permita la estructuración lógica de flujos dinámicos que incorporen procesos de control e inspección de acuerdo con la conveniencia de la organización. Se debe considerar una solución que brinde visibilidad en tiempo real de las actividades que ocurren dentro de la red (CPP y CPA) Debe recopilar y analizar la telemetría de red, como flujos (NetFlow) desde los Switches tipo “Leaf” para supervisar el comportamiento de la red de los centros de datos. El sistema debe realiza análisis sofisticados y técnicas de machine learning en los datos de la red para detectar automáticamente comportamientos anormales que pueden significar un ataque. Debe tener la capacidad de identificar el comportamiento normal del entorno para facilitar la identificación de algo sospechoso			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	Adicional tener la capacidad de identificar comportamientos relacionados con amenazas de día cero, amenazas internas, amenazas avanzadas persistentes, intentos de denegación de servicio distribuido y otros compromisos que puedan poner en riesgo a los centros de datos. Se debe supervisa los comportamientos de la red en busca de indicadores de amenazas Los datos de telemetría se deben analizan para proporcionar una imagen completa de la actividad de la red Debe obtener las conversaciones generadas por los "Leaf" del centro de datos, sin la necesidad de seleccionar los enlaces a monitorear. La solución debe buscar la mejora del rendimiento de la red y apoyar en la planificación de la capacidad. Con una visión en profundidad de todo lo que sucede en la red, debe generar una línea base del comportamiento normal. Se debe incluir el licenciamiento para recolección, gestión y el análisis de telemetría de flujos. Se debe incluir licenciamiento para inteligencia de amenazas, que permita aprovechar información global para generar alertas y un índice de preocupación de eventos para marcar las comunicaciones sospechosas para que puedan ser investigadas rápidamente. El oferente debe incluir las plataformas para recolección de flujos y para administración de la solución, y su configuración. El oferente debe incluir la configuración para obtener los flujos de los equipos "Leaf", que serán enviados a la plataforma de recolección. Esta solución debe ser diseñada e implementada por el fabricante.			
5.3.2.	**Segmento de CORE** El segmento de CORE debe proveer esencialmente la conectividad de red entre todos los bloques operativos disponibles. En el caso propuesto, los dispositivos CORE brindan conectividad hacia los segmentos de DataCenter, Agregación de Usuarios y Agregación de Borde, así como cualquier otro bloque topológico incorporado posteriormente en la arquitectura. La arquitectura de comunicaciones debe proveer los protocolos de alta disponibilidad y enrutamiento dinámico necesarios para			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	que los diferentes segmentos puedan comunicarse entre sí. En el caso particular del CPA, existe la posibilidad de que la infraestructura de comunicaciones a ser provista no esté ubicada en las mismas premisas donde actualmente se ubican los dispositivos operativos del Centro de Datos de Oficinas Centrales. En este caso es necesario que se consideren un modelo de comunicación que permita incorporar una interconexión directa entre el segmento de CORE y el segmento de Agregación de Usuarios que si quedara disponible y habilitado en los edificios de Oficinas Centrales. El diseño topológico debe proveer esta flexibilidad operativa que permita la integración de los módulos operativos, aunque no estén ubicados en las mismas premisas. En este caso, la CCSS proveerá los enlaces de transporte entre Oficinas Centrales y el punto geográfico donde esté ubicado el Centro de Datos del CPA.			
5.3.3.	**Segmento de Agregación de Usuarios** La infraestructura de comunicaciones de Agregación de Usuarios ya existe y está concentrada en dispositivos Cisco Catalyst 4500X. Como parte del servicio propuesto se debe incorporar este bloque operativo al modelo de comunicaciones integral realizando las interconexiones necesarias y proveyendo los mecanismos lógicos de conexión y convergencia que permitan una operación transparente de la solución. El oferente deberá proveer y documentar las mejores prácticas de configuración provista por el fabricante y definida por la industria, para asegurar que este segmento cuenta con las consideraciones de ingeniería consistentes con el resto de la solución a implementar. Complementariamente, en el edificio de Oficinas Centrales, los dispositivos de agregación de usuarios están interconectados a una pareja de dispositivos de CORE (Nexus9500) que deberán tener interconexión directa hacia ambos centros de datos, CPP y CPA, utilizando mecanismos dinámicos de convergencia que permitan la disponibilidad del acceso en todo momento. La interconexión hacia estos nodos se realizará por medio de enlaces de datos dedicados utilizando protocolos de enrutamiento dinámico para permitir ese proceso de convergencia y disponibilidad continuos.			
5.3.4.	**Segmento de Borde** Este es uno de los segmentos que involucra un poco más de complejidad topológica, pues es necesario considerar ciertos principios de asociación de servicios en el desarrollo de los diseños.			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	En principio, se debe interpretar al segmento de Borde como el bloque operativo de la red, donde se agrupan aquellas conexiones externas a la organización, ya sea por medio de enlaces de datos privados, fibras oscuras, redes WAN inalámbricas, servicios de Internet y cualquier conexión a redes privadas y externas para consumir o proveer servicios. Se excluye del segmento de Borde, aquellas conexiones necesarias para la integración entre el CPA y el CPP. Tampoco se incluye la interconexión entre el CPA y la red corporativa de Oficinas Centrales en caso de que estas sean las circunstancias. Dada la estructura topológica deseada para el segmento de Borde, es necesario se provea un bloque interno denominado "Agregación de Borde", que permita colapsar o agregar las conexiones a las distintas capas que se deben proveer. Este bloque interno de Agregación estará interconectado con el Segmento de CORE, por lo que se deben realizar los mecanismos de alta disponibilidad y enrutamiento dinámico que permitan las comunicaciones entre el segmento de Borde y el resto de la infraestructura de comunicaciones. Como se menciona anteriormente, el foco del servicio requerido en este documento es el CPA, sin embargo, se requiere que como parte del servicio exista un proceso de estandarización del segmento de Borde tanto en el CPA como el CPP, por lo que las condiciones establecidas en esta sección aplican para ambas áreas. Debe también considerarse que para desarrollar un proceso de migración transparente que reduzca la cantidad de interrupciones en el servicio, es necesario habilitar todos los servicios de borde en el CPP, de tal forma que pueda iniciar un proceso de operación productivo que permita modificaciones en la estructura topológica de CPA, sin la interrupción de los servicios a los usuarios. Más información respecto a este requerimiento técnico es proporcionada en las secciones posteriores. En relación con la estructura topológica del segmento de Borde, es necesario incorporar 3 capas que agrupen los servicios basados en el siguiente criterio:			
5.3.4.1.	**Capa de Conexiones WAN:** Es el segmento de red que agrupa las conexiones privadas hacia el CPP y CPA respectivamente. Es esta capa se habilitan los servicios de enrutamiento, seguridad, inspección y optimización de tráfico necesario para la correcta operación del servicio. En esta capa se incluye el servicio de conexión inalámbrica de enlaces WAN hacia hospitales y clínicas. Uno de los criterios de separación en una capa independiente es el aprovisionamiento			

Nº	Descripción del Cartel	Cumple		Descripción del oferente
		Sí	No	
	de políticas de control y gestión de tráfico coherentes con el tipo de servicio provisto. Todos aquellos enlaces donde ambos extremos de la conexión estén bajo el control y gestión de la organización serán incorporados en esta capa.  			
5.3.4.2.	**Capa de Conexiones de Internet:** Es el segmento de red donde se manejan las conexiones hacia Internet. De igual forma que en cada bloque mencionado, es esta capa se habilitan los servicios de seguridad necesarios para proporcionar conectividad apropiada hacia los segmentos internos de la red. En este mismo bloque se habilitan los segmentos de DMZ necesarios para la publicación de servicios a Internet, considerando que los mecanismos de conectividad deben ser seguros, asimismo proveyendo las zonas de seguridad necesarias y estableciendo controles de acceso requeridos entre estos bloques. Todos los enlaces públicos que no cuenten con mecanismos de cifrado de datos se ubicarán en esta Capa.			

Nº	Descripción del Cartel	Cumple		Descrip-ción del oferente
		Sí	No	
				
5.3.4.3.	**Capa de Conexiones de Acceso Remoto:** Es el segmento de red que concentra las conexiones de acceso remoto incluyendo todas aquellas que requieran mecanismos de cifrado por medio de VPN y otros mecanismos de encapsulación. En esta capa deben habilitarse las conexiones VPN de acceso remoto de usuarios, también las conexiones VPN de LAN a LAN para conectividad con cualquier institución u organización externa que requiera conectividad de red hacia servicios internos de la CCSS. 			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
5.3.5.	Con respecto al segmento de borde, se debe considerar que los requerimientos del servicio de integración involucran la habilitación de la estructura de comunicaciones para los dispositivos de seguridad, de acuerdo con los modelos definidos en este documento, así como el acompañamiento en el proceso de configuración de los servicios de seguridad incorporados a la topología habilitada. Dado que la organización cuenta con plataformas de seguridad, inspección y optimización de tráfico, se requiere que el oferente incorpore estos elementos como parte de las plataformas a adquirir, de acuerdo al diseño topológico que contempla los dos Centros de Datos. La distribución de plataformas a nivel del ambiente de comunicaciones de borde está constituida de la siguiente manera: • Plataformas de Control de Acceso: La infraestructura de control de acceso está basada en dispositivos contrafuegos de la familia Cisco Firepower 2100 integrados en línea para la definición de políticas de control de acceso. La plataforma cuenta con interfaces de 10GE para la conectividad de red hacia las diferentes zonas de seguridad. • Plataforma de Inspección: La solución de inspección de tráfico está basada en plataformas de seguridad IPS como dispositivo físico integrado en línea con el tráfico de borde. Parte del proceso de optimización involucrará la reestructuración topológica de módulos de inspección, para mejorar el rendimiento del servicio de tal forma que se apliquen políticas de seguridad e inspección alineadas al tipo de tráfico inspeccionado. • Plataforma de Optimización de Ancho de Banda: Específicamente para el tráfico WAN hacia Hospitales, Clínicas y otras sucursales, se utiliza la plataforma de optimización y control de la familia Exinda de GFI Software, que permite establecer políticas de utilización de ancho de banda para el tráfico de red, estableciendo límites por tipo de protocolo de transporte. Considerando los puntos anteriores, es necesario que el oferente proponga los mecanismos óptimos de integración de las plataformas al nuevo modelo topológico, considerando las implicaciones del proceso de migración y actualización estructural. También que se proporcionen los elementos de seguridad de red necesarios para ofrecer las capas de control e inspección en los subsegmentos de borde descritos previamente.			
6.	**Requerimientos Técnicos de Dispositivos para Conectividad del Centro de Datos**			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	En esta sección se detallan los requerimientos técnicos de hardware establecido por la CCSS, determinado en el proceso de actualización de este segmento de acceso. Cabe mencionar que este proceso de actualización de infraestructura no implica únicamente sustitución de hardware, sino que se pretenden obtener nuevos beneficios tecnológicos y de replanteamiento topológico, como parte de la visión general que la CCSS ha definido en su plan de inversiones a mediano y largo plazo. Las consideraciones de definición de hardware están basadas en los diseños establecidos internamente y la aplicación de los modelos de comunicación hacia los que se desea migrar, por lo que se requiere que las propuestas de equipos estén alineadas con los requisitos explícitos detallados a continuación.			
6.1.	**Dispositivos de Red de Acceso** Los dispositivos de comunicaciones de acceso proveerán la conectividad de red hacia los diferentes elementos de acceso existentes y los que en un corto plazo deseen integrarse a esta infraestructura. A diferencia del ambiente existente, los dispositivos conmutadores requeridos, proveerán conectividad hacia cualquier elemento final de forma redundante. Cualquier conexión debe ser habilitada al menos a dos (2) dispositivos de acceso.			
6.1.1.	**Especificaciones Técnicas de Dispositivos de Acceso de Fibra Óptica** Se requieren cuatro (4) dispositivos conmutadores con las características descritas a continuación:			
6.1.1.1.	48 puertos de 10 Gbps base SFP+.			
6.1.1.2.	12 puertos de 40/100 Gbps base QSFP28.			
6.1.1.3.	Los 48 puertos SFP+ en los dispositivos deben soportar velocidades de conmutación de 1, 10, 25 Gbps.			
6.1.1.4.	Los dispositivos deben contar con al menos 2 interfaces de gestión independientes utilizando medios ethernet para ser interconectados a la red de gestión fuera de banda.			
6.1.1.5.	Los dispositivos deben estar habilitados con 2 fuentes de poder AC reemplazables en caliente.			
6.1.1.6.	Los dispositivos deben tener unidades de ventilación redundante y reemplazable en caliente.			
6.1.1.7.	Los dispositivos deben soportar la habilitación de FCoE para agregación de tráfico de redes LAN y SAN hacia dispositivos finales de procesamiento.			
6.1.1.8.	Los dispositivos deben soportar métodos de cifrado de tramas por medio del estándar 802.1ae.			

Nº	***Descripción del Cartel***	***Cumple***		***Descripción del oferente***
		Sí	***No***	
6.1.1.9.	Los dispositivos deben estar aprovisionados con mecanismos de encapsulación de tráfico capa 2 sobre infraestructura capa 3 con el uso de protocolos de enrutamiento.			
6.1.1.10.	Los dispositivos deben contar con la capacidad de agregar puertos en una misma interface de agrupaciones de puertos integrando interfaces de otros dispositivos similares.			
6.1.1.11.	Los dispositivos deben tener interfaces redundantes para gestión fuera de banda que no tengan relación con la operación productiva.			
6.1.1.12.	Cada dispositivo debe contar una capacidad de escalabilidad real de direcciones MAC hasta 256,000.			
6.1.1.13.	Cada dispositivo deben contar con una capacidad de escalabilidad real de direcciones IP hasta 890,000 direcciones de dispositivos finales.			
6.1.1.14.	Cada dispositivo debe soportar hasta 512 grupos de agregación de puertos para permitir la interconexión hacia otros elementos.			
6.1.1.15.	Cada grupo de agregación de interfaces debe soportar incorporar hasta 32 puertos independientes.			
6.1.1.16.	Cada dispositivo debe soportar la habilitación de hasta 4 sesiones de monitoreo en puertos operando de manera simultánea.			
6.1.1.17.	La tabla de flujos para análisis generada por cada dispositivo debe ser de hasta 64,000 registros.			
6.1.1.18.	Cada dispositivo debe soportar el balanceo de tráfico utilizando hasta 64 caminos físicos independientes.			
6.1.1.19.	Los dispositivos deben soportar un rango operativo de 100 a 240V en AC.			
6.1.2.	**Especificaciones Técnicas – Acceso Cobre** Se requieren ocho (8) dispositivos conmutadores con las características descritas a continuación:			
6.1.2.1.	48 puertos de 10 Gbps base T.			
6.1.2.2.	6 puertos de 40/100 Gbps base QSFP28.			
6.1.2.3.	Los 48 puertos de cobre a 10Gbps en los dispositivos deben soportar velocidades de conmutación de 100Mbps así como 1 y 10 Gbps.			
6.1.2.4.	Los dispositivos deben contar con al menos 2 interfaces de gestión independientes utilizando médios ethernet para ser interconectados a la red de gestión fuera de banda.			
6.1.2.5.	Los dispositivos deben estar habilitados con 2 fuentes de poder AC reemplazables en caliente.			
6.1.2.6.	Los dispositivos deben tener unidades de ventilación redundante y reemplazable en caliente.			
6.1.2.7.	Los dispositivos deben soportar la habilitación de FCoE para agregación de tráfico de redes LAN y SAN hacia dispositivos finales de procesamiento.			
6.1.2.8.	Los dispositivos deben soportar métodos de cifrado de tramas por medio del estándar 802.1ae.			
6.1.2.9.	Los dispositivos deben estar aprovisionados con mecanismos de encapsulación de tráfico capa 2 sobre infraestructura capa 3 con el uso de protocolos de enrutamiento.			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
6.1.2.10.	Los dispositivos deben contar con la capacidad de agregar puertos en una misma interface de agrupaciones de puertos integrando interfaces de otros dispositivos similares.			
6.1.2.11.	Los dispositivos deben tener interfaces redundantes para gestión fuera de banda que no tengan relación con la operación productiva.			
6.1.2.12.	Cada dispositivo debe contar una capacidad de escalabilidad real de direcciones MAC hasta 512,000.			
6.1.2.13.	Cada dispositivo deben contar con una capacidad de escalabilidad real de direcciones IP hasta 1,790,000 direcciones de dispositivos finales.			
6.1.2.14.	Cada dispositivo debe soportar hasta 512 grupos de agregación de puertos para permitir la interconexión hacia otros elementos.			
6.1.2.15.	Cada grupo de agregación de interfaces debe soportar incorporar hasta 32 puertos independientes.			
6.1.2.16.	Cada dispositivo debe soportar la habilitación de hasta 4 sesiones de monitoreo en puertos operando de manera simultánea.			
6.1.2.17.	La tabla de flujos para análisis generada por cada dispositivo debe ser de hasta 64,000 registros.			
6.1.2.18.	Cada dispositivo debe soportar el balanceo de tráfico utilizando hasta 64 caminos físicos independientes.			
6.1.2.19.	Los dispositivos deben soportar un rango operativo de 100 a 240V en AC.			
6.2.	**Dispositivos de Agregación**			
6.2.1.	**Especificaciones Técnicas – Agregación Centro de Datos** Se requieren dos (2) conmutadores para agregar los dispositivos de acceso que cuenten con las características descritas a continuación:			
6.2.1.1.	64 puertos de 100 Gbps QSFP+.			
6.2.1.2.	Todos los puertos del dispositivo deben operar en modalidad “non-blocking”, es decir, sin restricciones de ancho de banda por puerto en full-dúplex.			
6.2.1.3.	Los dispositivos deben estar habilitados con dos (2) fuentes de poder AC reemplazables en caliente.			
6.2.1.4.	Los dispositivos deben tener unidades de ventilación redundante y reemplazable en caliente.			
6.2.1.5.	Los dispositivos deben estar aprovisionados con discos de estado sólido para almacenamiento de al menos 250GB.			
6.2.1.6.	Los dispositivos deben soportar métodos de cifrado de tramas por medio del estándar 802.1ae.			
6.2.1.7.	Los dispositivos deben estar aprovisionados con mecanismos de encapsulación de tráfico capa 2 sobre infraestructura capa 3 con el uso de protocolos de enrutamiento.			
6.2.1.8.	Los dispositivos deben contar con la capacidad de manejar múltiples caminos para balancear tráfico de forma dinámica (ECMP). La cantidad de caminos simultáneos de balanceo debe ser de al menos 64 caminos simultáneos soportados para hacer ECMP.			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
6.2.1.9.	Los dispositivos deben poder agregar diferentes puertos por medio de un "Port-Channel" soportando al menos 32 puertos en la misma interface "Port-Channel".			
6.2.1.10.	Los dispositivos deben tener la capacidad de crear al menos 64 interfaces "Port-Channel".			
6.2.1.11.	Los dispositivos deben contar con la capacidad de segmentar tráfico de capa 3 por medio de VFR, soportando al menos 1000 diferentes instancias virtuales.			
6.2.1.12.	Los dispositivos deben poder terminar túneles de capa 2 sobre infraestructura de capa 3, soportando al menos 256 túneles diferentes terminados localmente en los dispositivos.			
6.2.1.13.	Los dispositivos deben tener interfaces redundantes para gestión fuera de banda que no tengan relación con la operación productiva.			
6.3.	**Plataforma de Gestión, Control y Conectividad**			
6.3.1.	**Especificaciones Técnicas de la Plataforma de Gestión, Control y Monitoreo** Se requiere la incorporación de dispositivos físicos independientes que puedan realizar la gestión de la solución de conmutación a integrar. Esta solución debe contar con un arreglo de dispositivos que operan en modalidad activo-activo considerando los siguientes requerimientos técnicos:			
6.3.1.1.	La plataforma de control debe operar en modalidad activo-activo en formato de arreglo y debe estar habilitado utilizando mecanismos de alta disponibilidad por medio de la integración con el ambiente de gestión de DataCenter existente en el CPP.			
6.3.1.2.	La plataforma debe estar habilitada para soportar la cantidad de dispositivos de acceso establecidos como parte de este requerimiento y el crecimiento futuro, donde se podrían exceder los 1000 puertos de interconexión hacia los dispositivos finales.			
6.3.1.3.	La plataforma debe permitir el manejo de inventario y la configuración de dispositivos conmutadores que forman parte de la solución requerida.			
6.3.1.4.	Se requiere que la plataforma pueda realizar aprovisionamiento sin necesidad de realizar ningún tipo de configuración del lado de los dispositivos conmutadores.			
6.3.1.5.	Todos los dispositivos deben formar parte de la misma estructura de conmutación. Esta estructura lógica debe ser aprovisionada de forma integral por parte de la plataforma de gestión centralizada.			
6.3.1.6.	La plataforma debe tener la funcionalidad de manejar fallas e identificar los puntos donde existan problemas de operación o configuración para ejecutar tareas de resolución de forma expedita.			
6.3.1.7.	La incorporación o remoción de los dispositivos conmutadores como parte del esquema de conmutación centralizado, debe realizarse por medio de la plataforma de gestión, sin que exista interrupción de servicios operativos en el resto de la infraestructura.			
6.3.1.8.	La plataforma debe permitir que se puedan habilitar esquemas de virtualización de red a nivel de toda la infraestructura conmutada. Esta virtualización de ambientes de red debe ser homogénea a lo			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	largo de todos los dispositivos de la solución, haciendo que los mismos se comporten como un solo repositorio de recursos.			
6.3.1.9.	La plataforma debe permitir la integración con plataformas de terceros, para el proceso de orquestación y automatización basado en API en un marco de referencia como Openstack.			
6.3.1.10.	La plataforma debe permitir la integración de programación de políticas por medio de lenguajes como Python, Chef o Puppet.			
6.3.1.11.	La plataforma debe permitir la integración con un ecosistema abierto de dispositivos firewalls, IPS, balanceadores de carga y otros servicios, de tal forma que el proceso de incorporación sea transparente.			
6.3.1.12.	La plataforma debe tener las características necesarias para permitir la integración con ambientes de virtualización tales como VMWARE, Hyper-V o Containers, de manera que puedan aprovisionar los servicios y configuraciones de red indirectamente desde esta plataforma.			
6.3.1.13.	La plataforma debe permitir microsegmentación de servicios de red, de tal forma que se pueda realizar segmentación de diferentes servicios a nivel de cada puerto asociando cada tráfico al ambiente virtualizado correspondiente, de acuerdo con los requerimientos establecidos por la organización.			
6.3.1.14.	La solución debe permitir e incluir la integración de una plataforma superior de orquestación para el control de varios nodos o sitios creando zonas independientes de disponibilidad y permitiendo que se puedan incorporar diferentes ambientes de dispositivos bajo un solo esquema de aprovisionamiento.			
6.3.1.15.	La solución de orquestación debe ser implementada en un ambiente virtualizado soportado sobre Vmware ESXi 6.0 para orquestar los dispostivos dedicados de la capa de gestión ubicados en cada nodo CPP y CPA.			
6.3.1.16.	Se debe proveer la infraestructura de interconexión entre los centros de datos para permitir que pueda existir la operación integrada entre las infraestructuras de comunicaciones de Centro de Datos que puedan ser integradas al esquema de orquestación centralizada y de manera que pueda ser posible la encapsulación y extensión de los dominios de broadcast del Centro de Datos para ambos nodos.			
6.4.	**Requerimientos Técnicos Específicos de la Solución General** Adicionalmente a lo mencionado, se requiere que la solución planteada funcione de forma integral, esto quiere decir que toda la infraestructura de conmutación opere de manera unificada. A continuación, se presentan los diferentes requerimientos técnicos específicos para la solución de conmutación general:			
6.4.1.	**Requerimientos técnicos específicos**			
6.4.1.1.	La solución de conmutación debe soportar al menos 80 dispositivos de conmutación a ser integrados.			
6.4.1.2.	La solución de conmutación debe soportar al menos 24 dispositivos de agregación a ser integrados.			

Nº	***Descripción del Cartel***	***Cumple***		***Descripción del oferente***
		Sí	***No***	
6.4.1.3.	La solución de conmutación debe soportar un esquema de virtualización o modularización virtual de servicios de comunicación a lo largo de toda la infraestructura, de tal forma que exista segmentación lógica y administrativa. La solución debe soportar al menos 1000 instancias virtuales.			
6.4.1.4.	De la misma forma, es necesario que la solución pueda definir instancias virtuales de capa 3 por medio de VRF. La solución debe soportar al menos 1000 VRF.			
6.4.1.5.	La solución debe soportar la característica para definir bloques de dispositivos finales que puedan ser asociados. La asociación en estos bloques de dispositivos debe ser agnóstica a las características tradicionales de comunicación tales como VLAN, direccionamiento IP y otros. La solución debe soportar al menos 15,000 bloques de dispositivos.			
6.4.1.6.	La solución debe permitir que se puedan incorporar de forma nativa mecanismos de filtrado y control de tráfico entre los bloques de dispositivos. Estos filtros deben ser aplicados para que se definan permisos de control de tráfico en una modalidad de lista blanca, donde solamente los permisos explícitos permitan la comunicación entre los bloques de dispositivos. La solución debe soportar al menos 10,000 sentencias de filtrado de tráfico.			
6.4.1.7.	Dado que el modelo de conmutación requerido demanda de un ambiente integral, se requiere la utilización de mecanismos de definición de redes IP que no tengan que residir lógicamente en un solo dispositivo, sino que operen de forma global en todo el ambiente lógico de la infraestructura. Es necesario que la solución soporte al menos 15,000 dominios virtuales para la definición de estas características de capa 3 y las características de capa 2 relacionadas.			
6.4.1.8.	En su integración con ambientes virtualizados, es necesario que la solución permita la gestión y aprovisionamiento de al menos 200 VDS en un ambiente de VMWARE, de tal forma que se puedan aprovisionar los grupos de puertos correspondientes para que posteriormente sean asignados a las máquinas virtuales.			
6.4.1.9.	La solución debe tener características de monitoreo de las máquinas virtuales asociadas a los VDS de VMWARE aprovisionados. La solución debe soportar esta visibilidad en el aprovisionamiento de al menos 3200 máquinas virtuales.			
6.4.1.10.	Los dispositivos de conmutación de la solución deben soportar en conjunto al menos 576 “Port-Channel” locales o virtuales.			
6.4.1.11.	De la misma manera, la solución de conmutación debe permitir la posibilidad de habilitar al menos 1750 encapsulaciones por cada puerto o “Port-Channel” para lograr los mecanismos de granularidad necesarios para la segmentación del tráfico en diferentes servicios.			
6.4.1.12.	La solución debe soportar al menos 24,000 dispositivos finales a ser incorporados en la topología de conmutación, esto implica soporte de 24,000 direcciones MAC y 24,000 direcciones IP por cada dispositivo de conmutación independiente. A nivel de todo el ambiente de conmutación global la solución debe soportar 360,000 direcciones MAC y al menos un total de 180,000 direcciones IP de dispositivos finales.			

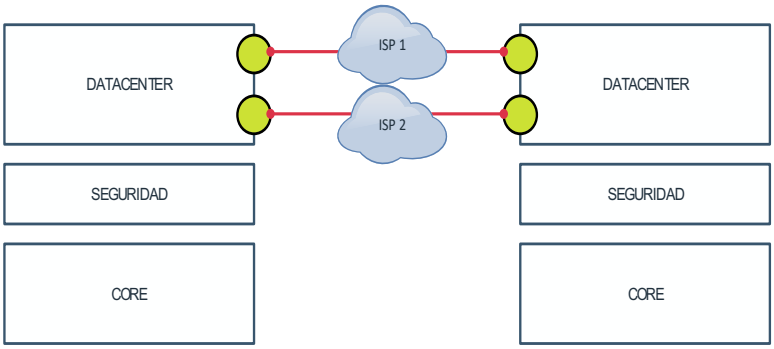
Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
6.4.1.13.	La solución debe soportar la habilitación de sesiones SPAN que permitan derivar el tráfico de cualquier puerto de la infraestructura hacia un punto final de recolección. Se deben soportar al menos 8 sesiones SPAN bidireccionales o bien 4 sesiones SPAN unidireccionales.			
6.4.1.14.	La solución debe soportar al menos 3000 contextos VRF a nivel de la infraestructura global.			
6.4.1.15.	La solución debe soportar al menos 1000 dominios virtuales de conmutación por dispositivo y 1750 por cada contexto VRF a nivel de toda la infraestructura global.			
6.4.1.16.	La solución debe soportar la integración con protocolos de enrutamiento dinámico como BGP, OSFP y EIGRP.			
6.4.1.17.	La solución debe soportar la integración con diferentes vCenter de VMWARE hasta un valor de al menos 200 instancias individuales.			
6.4.1.18.	La solución debe soportar la configuración con dominios SVCMM diferentes habilitando la integración de 5 dominios diferentes independientes.			
6.4.1.19.	La solución debe soportar integración con dominios de autenticación y autorización Active Directory/LDAP para la asignación de accesos y permisos de control de acceso para administración.			
6.5.	**Requerimientos Técnicos de Interconexión Lógica entre Centros de Datos** Complementariamente es necesario implementar mecanismos de interconexión entre los centros de datos que permitan que los dominios de broadcast puedan ser extendidos, permitiendo que los ámbitos de operación puedan ser implementados de manera extendida de tal manera que las aplicaciones puedan estar alojadas en cualquiera de los nodos sin penalización en la operación. Desde el punto de vista de la infraestructura de comunicaciones la solución general debe operar en modalidad Activo-Activo para que pueda balancearse cargas de procesamiento en ambos centros de datos y pueda consumirse independientemente de su ubicación. Para lograr lo anterior en necesario implementar una capa lógica de extensión de red que operará sobre la arquitectura de red óptica definida en este documento que deberá permitir la comunicación a nivel del plano de datos. Tanto para el CPP como para el CPA, se deben proporcionar los dispositivos que permitan la interconexión de red en alta velocidad considerando los esquemas de alta disponibilidad y teniendo un ancho de banda disponible de al menos 10Gbps por cada uno de los enlaces primario y secundario disponible. Los dispositivos proporcionados deben contar con las capacidades de enrutamiento y conmutación necesarias para que el modelo de integración entre nodos pueda ser posible. De la misma forma, los dispositivos proporcionados deben habilitarse considerando un esquema de alta disponibilidad por lo que deben habilitarse en parejas y utilizando mecanismos automáticos de convergencia a nivel interno y			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	externo.			
6.6.	**Requerimientos de Arquitectura Lógica de la Solución de Conmutación del Centro de Datos** La solución de comunicaciones solicitada requiere que pueda integrarse con todos los elementos habilitados y que operen como un solo ecosistema, permitiendo la conectividad y definición de flujos de tráfico lógicos, en función de las aplicaciones o servicios transportados. La solución de comunicaciones debe ser diseñada para que se garantice la disponibilidad de los servicios transportados aún en el caso de fallas operativas. Los procesos de convergencias deben ser tales que, aunque existan fallas en alguno de los componentes de la infraestructura, los servicios transportados no se vean comprometidos. La solución de comunicaciones debe contar con los mecanismos necesarios para establecer flujos de tráfico lógicos a nivel de la topología lógica de transporte, sin que estos tengan que limitarse a la asociación de servicios o dispositivos por medio de VLAN. Es necesario que la solución ofrezca suficiente flexibilidad para que se puedan habilitar modelos de flujos por aplicación independientes. Será responsabilidad del oferente, definir, documentar y aplicar los modelos de comunicación lógicos y flujos de tráfico de las aplicaciones transportadas sobre la nueva infraestructura de comunicaciones. De la misma forma, se debe considerar que los futuros procesos de comunicación a nivel del Centro de Datos deben basarse en el crecimiento de esta infraestructura de transporte, por lo que es necesario estandarizar dicha topología lógica de comunicación. Como parte de la definición de la arquitectura, es necesario que el oferente adjudicado defina la jerarquía de componentes de red lógicos necesarios para el modelo de comunicaciones requerido por la CCSS. Los componentes lógicos requeridos son mencionados a continuación:			
6.6.1.	Contextualización Virtual: se deben definir modelos de virtualización de manera que se puedan establecer instancias virtuales, las cuales segmentan los ambientes de comunicación a nivel de capa 2 y capa 3, e inclusive de plano de control si fuera necesario.			
6.6.2.	Dominios de Capa 3: de la misma manera, es necesaria la definición de los diferentes ambientes asociados que permitan la segmentación de dominios de capa 3 por medio de VRF.			
6.6.3.	Conmutadores Distribuidos Virtuales: se deben definir las instancias lógicas de conmutación que estén distribuidas a lo largo de toda la infraestructura, de tal forma que interfaces físicas o lógicas			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	de diferentes dispositivos puedan pertenecer a la misma instancia virtual.			
6.6.4.	Flujos de Aplicaciones: la solución debe poder agrupar los diferentes componentes lógicos subyacentes en un flujo de aplicación que incorpore los dispositivos físicos y lógicos relacionados a la aplicación correspondiente, sin que el tráfico de otras aplicaciones tenga que mezclarse lógicamente con estas aplicaciones. Los flujos de aplicaciones deben soportar e incorporar los componentes externos a ser integrados como parte del proceso de aseguramiento o tratamiento del tráfico de red de las aplicaciones. Estos componentes externos ´pueden ser firewalls, analizadores de tráfico, balanceadores de carga y cualquier otro dispositivo físico o lógico relacionado.			
6.6.5.	Bloques de dispositivos: se definirán y asociarán a estos bloques los dispositivos definidos a nivel de la aplicación, en función del rol operativo y de la posición que tienen a través del flujo de tráfico.			
6.6.6.	Como parte del proceso de implementación definido, es necesario que el oferente adjudicado documente cada uno de los elementos mencionados anteriormente en las secciones correspondientes, de manera que se defina de forma clara la estructura de comunicación lógica y física en toda la solución de comunicaciones.			
6.7.	**Requerimientos de Integración con el Ambiente de Data Center del CPP** La solución requerida para el segmento de comunicaciones del Centro de Datos debe estar basada en la plataforma de red existente en el CPP, debido a que uno de los objetivos que se pretenden alcanzar en la construcción de la arquitectura de DataCenter en el CPA, es que maneje el mismo plano de control del CPP. Esto quiere decir, que la plataforma de control y gestión existente en el CPP debe integrarse de tal forma que la definición de políticas de acceso, control y otras configuraciones puedan aprovisionarse desde cualquiera de los centros de datos. Esto permitirá tener una red homogénea que pueda operar con completa independencia pero que no requiera ejecutar actividades de configuración redundantes. Dado que ya existen políticas configuradas en el ambiente productivo actual, es necesario que se pueda realizar una extrapolación sencilla de éstas al ambiente de comunicaciones de DataCenter en el CPA. Una vez que exista una completa integración entre los segmentos de DataCenter de CPP y CPA, la parte de la plataforma de gestión ubicada en el CPA debe tener la capacidad de respaldar todas las políticas configuradas para el CPP de modo que cuando el sitio principal vuelva a estar disponible no haya pérdida de las configuraciones habilitadas. En resumen, los segmentos de comunicaciones de DataCenter del CPP y CPA deben comportarse como un solo Centro de Datos, donde se puedan distribuir los servicios transportados y			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	donde sea indiferente la ubicación física de los dispositivos de procesamiento. Para lograr el objetivo plateado anteriormente es necesario proveer una solución que permita integrar los ámbitos de gestión de tal manera que se logre el objetivo de centralizar la solución.			
6.7.1.	**Requerimientos de la Plataforma de Orquestación del Centro de Datos** La solución de comunicaciones debe contar con una plataforma de orquestación centralizada que permita la definición de políticas hacia cada una de las consolas de Control que estarán ubicadas en cada uno de los nodos operativos del banco. Esta plataforma de orquestación deberá estar ubicada en el nodo primario en la infraestructura virtual provista para plataformas de administración orquestación y gestión que se mencionan en el presente documento. A continuación, se menciona la lista de requerimientos técnicos necesarios para la plataforma mencionadas:			
6.7.2.	La plataforma de orquestación debe ser integral con las plataformas de gestión y monitoreo mencionadas anteriormente. Esta gestión involucra la habilitación de mecanismos de comunicación que permita enviar políticas de configuración para la operación de la infraestructura de comunicaciones en cada uno de los nodos.			
6.7.3.	La plataforma de orquestación será implementada en la arquitectura virtual dispuesta para todos los elementos de gestión, Administración, monitoreo y orquestación.			
6.7.4.	La plataforma de orquestación deberá ser implementada en una modalidad de tres nodos lógicos que operen en cluster.			
6.7.5.	Cada uno de los tres nodos que componen el cluster de la consola de orquestación deberá operar en su propio host físico del ambiente virtual para asegurar que aunque exista una falla operativa en cualquiera de los servidores físicos, siempre existirá disponibilidad de los nodos restantes.			
6.7.6.	La plataforma de orquestación debe permitir la creación de usuarios y administradores con los respectivos permisos de operación asociados a la segmentación lógica que se determine en cada uno de los nodos primario y secundario.			
6.7.7.	La plataforma de orquestación debe permitir la creación, modificación y eliminación de sitios, nodos o centros de datos que pertenezcan a la infraestructura de la CCSS.			
6.7.8.	La plataforma de orquestación debe contar con una consola central que permita tener una visión integral de los elementos de la infraestructura que componen la solución de comunicaciones, mostrando información relevante respecto al estado de los dispositivos, su salud general y el estado operativo de la infraestructura lógica que opera en ambos centros de datos.			
6.7.9.	La plataforma de orquestación debe proveer la posibilidad de crear plantillas de configuración que puedan ser utilizadas de manera recurrente para generar políticas de definición de flujos de tráfico.			

Nº	***Descripción del Cartel***	***Cumple***		***Descripción del oferente***
		Sí	***No***	
6.7.10.	La plataforma de orquestación debe permitir la creación, eliminación y modificación de instancias virtuales que luego pueden ser implementadas en cualquiera de los nodos gestionados.			
6.7.11.	La plataforma de orquestación debe permitir segmentar ambos centros de datos para que sean identificados como dos zonas de disponibilidad independientes. Esto significa que ante una falla en cualquiera de los nodos, la infraestructura debe continuar su operación de manera transparente e independiente.			
6.7.12.	La plataforma de orquestación debe permitir la definición de flujos lógicos que involucren dispositivos finales físicos o lógicos de cualquiera de los dos centros de datos, de tal manera que el aprovisionamiento de flujos se pueda ejecutar considerando la infraestructura de comunicaciones del sitio primario y del sitio secundario.			
6.7.13.	La plataforma de orquestación debe permitir que las máquinas virtuales ubicados en cualquiera de los centros de datos pueden ser desplazadas entre uno y otro sitio considerando la portabilidad de dirección IP, de tal manera que desde el punto de vista de los dispositivos finales, físicos o lógicos, no existe diferencia entre ambos centros de datos.			
6.7.14.	La topología general considerada en esta solución incluye la incorporación de un tercer nodo ubicado en la nube pública de Azure. Éste será considerado el tercer nodo de la infraestructura de comunicaciones orquestada.			
6.7.15.	La solución de orquestación debe considerar que se extenderán dominios de broadcast estre todos los nodos en cuestión por lo que la resolución de direcciones IP debe ser posible en los dominios de broadcast extendidos.			
6.7.16.	La plataforma debe permitir la incorporación de un máximo de hasta 12 sitios orquestados como parte de la solución.			
6.7.17.	La solución debe permitir hasta 200 conmutadores para conectividad de dispositivos finales en cada sitio y hasta 1600 conmutadores en total por todos los sitios.			
6.7.18.	La solución debe permitir la definición de hasta 400 instancias de virtualización.			
6.7.19.	La solución debe permitir un máximo de hasta 1000 instancias de enrutamiento virtuales.			
6.7.20.	La solución debe permitir hasta 500 conexiones externas de enrutamiento definidas en el modelo centralizado de orquestación.			
6.7.21.	La solución de orquestación debe permitir la creación de hasta 50 usuarios.			
6.7.22.	**Interconexión de los Segmentos de DataCenter del CPP y CPA** Con relación al proceso de interconexión, considerando la solución de comunicaciones existente en el ambiente de DataCenter del CPP y considerando el tipo y ancho de banda de los enlaces entre el CPP y CPA, deben habilitarse mecanismos de extensión de LAN que permitan extender las características de virtualización de servicios de red entre ambos Centros de Datos.			

Nº	Descripción del Cartel	Cumple		Descripción del oferente
		Sí	No	
	Dadas las características de contextualización virtual habilitadas por la plataforma de comunicaciones, es necesario que el modelo de comunicaciones en el CPA cuente con la misma distribución de contextos virtuales habilitados en el DataCenter, esto para permitir que eventualmente se pueda contar con una arquitectura de procesamiento completamente simétrica entre el CPP y CPA. Para lograr este modelo equivalente, es necesario que los mecanismos de extensión del ambiente de comunicaciones preserven las características de virtualización habilitadas.  De igual manera, la solución de gestión y administración debe ser extendible por medio de los enlaces de datos habilitados. El oferente debe considerar que los enlaces habilitados para los servicios de extensión de LAN dependen de la ubicación final del CPA, por lo que debe asumirse que los enlaces de datos serán habilitados a través de conexiones a oferentes de servicios con un rango de ancho de banda disponible de entre 1Gbps y 10Gbps. El oferente debe considerar los dispositivos necesarios que permitan realizar el proceso de encapsulación de datos a través de los enlaces, preservando la separación de tráfico entre los diferentes segmentos virtualizados en el modelo de comunicaciones. Los dispositivos habilitados deben soportar los anchos de banda de transporte requeridos para el aprovisionamiento del servicio de extensión de LAN, sin sacrificar rendimiento en el transporte, ya que se requiere una considerable cantidad de ancho de banda para el tráfico de red horizontal entre el CPP y CPA.			
7.	**Requerimientos Técnicos de Dispositivos de Enrutamiento y Conmutación de Borde** Con el propósito de habilitar la infraestructura del ambiente de borde en los nodos del CPP y CPA es necesario estructurar la topología física y lógica tal como se ha definido previamente de tal manera que se puedan separar los servicios de borde.			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	El proveedor deberá proporcionar los dispositivos que a continuación se requieren y se debe garantizar que todos ellos sean del mismo fabricante para lograr garantizar la compatibilidad en la interacción entre ellos y con el resto de la infraestructura. También se debe garantizar que exista completa compatibilidad con la plataforma de comunicación del Centro de Datos por lo que se desea que estos dispositivos sean del mismo fabricante que el resto de la infraestructura de comunicaciones del Centro de Datos.			
7.1.	**Requerimientos Técnicos de Dispositivos de Agregación de Borde** Se requieren 2 dispositivos conmutadores para el Centro de Datos del Sitio Alterno con las características descritas a continuación:			
7.1.1	Cada dispositivo debe contar con al menos 48 puertos de 1/10/25 Gbps base SFP/SFP+/SFP28.			
7.1.2	Cada dispositivo debe contar con al menos 4 puertos de 40/100 Gbps base QSFP28.			
7.1.3	Los 48 puertos SFP+ en los dispositivos deben soportar velocidades de conmutación de 1, 10, 25 Gbps.			
7.1.4	Los dispositivos deben contar con al menos 1 interfaces de gestión independientes utilizando médios ethernet para ser interconectados a la red de gestión fuera de banda.			
7.1.5	Los dispositivos deben estar habilitados con 2 fuentes de poder AC reemplazables en caliente.			
7.1.6	Los dispositivos deben tener unidades de ventilación redundante y reemplazable en caliente.			
7.1.7	Los dispositivos deben soportar métodos de cifrado de tramas por medio del estándar 802.1ae.			
7.1.8	Los dispositivos deben soportar capacidades de aprovisionamiento remoto por medio de plataformas centralizadas de gestión al momento de conexión inicial a la red.			
7.1.9	Los dispositivos deben contar con la capacidad de agregar puertos en una misma interface de agrupaciones de puertos integrando interfaces de otros dispositivos similares.			
7.1.10	Cada dispositivo debe contar una capacidad de escalabilidad real de direcciones MAC hasta 85,000.			
7.1.11	Cada dispositivo deben contar con una capacidad de escalabilidad real de direcciones IP hasta 210,000 direcciones de dispositivos finales.			
7.1.12	Cada dispositivo debe soportar hasta 1000 instancias de STP.			
7.1.13	El dispositivo debe soportar la capacidad de marcar los paquetes de datos con etiquetas de grupos pudiendo manejar hasta 30000 etiquetas distintas.			
7.1.14	La tabla de flujos para análisis generada por cada dispositivo debe ser de hasta 90,000 registros.			
7.1.15	Los dispositivos deben soportar un rango operativo de 100 a 240V en AC.			
7.2.	**Requerimientos Técnicos de Dispositivos de Interconexión entre Centros de Datos**			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	Se requieren 2 dispositivos conmutadores en cada uno de los Centros de Datos con las características descritas a continuación:			
7.2.1	48 puertos de 10 Gbps base SFP+.			
7.2.2	12 puertos de 40/100 Gbps base QSFP28.			
7.2.3	Los 48 puertos SFP+ en los dispositivos deben soportar velocidades de conmutación de 1, 10, 25 Gbps.			
7.2.4	Los dispositivos deben contar con al menos 2 interfaces de gestión independientes utilizando médios ethernet para ser interconectados a la red de gestión fuera de banda.			
7.2.5	Los dispositivos deben estar habilitados con 2 fuentes de poder AC reemplazables en caliente.			
7.2.6	Los dispositivos deben tener unidades de ventilación redundante y reemplazable en caliente.			
7.2.7	Los dispositivos deben soportar la habilitación de FCoE para agregación de tráfico de redes LAN y SAN hacia dispositivos finales de procesamiento.			
7.2.8	Los dispositivos deben soportar métodos de cifrado de tramas por medio del estándar 802.1ae.			
7.2.9	Los dispositivos deben estar aprovisionados con mecanismos de encapsulación de tráfico capa 2 sobre infraestructura capa 3 con el uso de protocolos de enrutamiento.			
7.2.10	Los dispositivos deben contar con la capacidad de agregar puertos en una misma interface de agrupaciones de puertos integrando interfaces de otros dispositivos similares.			
7.2.11	Los dispositivos deben tener interfaces redundantes para gestión fuera de banda que no tengan relación con la operación productiva.			
7.2.12	Cada dispositivo debe contar una capacidad de escalabilidad real de direcciones MAC hasta 256,000.			
7.2.13	Cada dispositivo deben contar con una capacidad de escalabilidad real de direcciones IP hasta 890,000 direcciones de dispositivos finales.			
7.2.14	Cada dispositivo debe soportar hasta 512 grupos de agregación de puertos para permitir la interconexión hacia otros elementos.			
7.2.15	Cada grupo de agregación de interfaces debe soportar incorporar hasta 32 puertos independientes.			
7.2.16	Cada dispositivo debe soportar la habilitación de hasta 4 sesiones de monitoreo en puertos operando de manera simultánea.			
7.2.17	La tabla de flujos para análisis generada por cada dispositivo debe ser de hasta 64,000 registros.			
7.2.18	Cada dispositivo debe soportar el balanceo de tráfico utilizando hasta 64 caminos físicos independientes.			
7.2.19	Los dispositivos deben soportar un rango operativo de 100 a 240V en AC.			
7.3.	**Requerimientos Técnicos de Dispositivos de Acceso para Proveedores de Servicio** Se requieren 6 dispositivos conmutadores en cada uno de los Centros de Datos con las características descritas a continuación:			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
7.3.1	Los dispositivos deben contar con 48 puertos 1Gbps ethernet de cobre base T y 4 puertos de 10Gbps Base SFP+.			
7.3.2	Los dispositivos deben contar con fuentes de poder redundantes y que sean removibles en caliente.			
7.3.3	Los dispositivos deben contar con una capacidad de tabla de direcciones MAC de hasta 16,000.			
7.3.4	Los dispositvos deben tener la capacidad de manejar hasta 11,000 rutas IPv4.			
7.3.5	Los dispositivos deben tener una capacidad de conmutación de hasta 95 Mpps.			
7.3.6	Los dispositivos deben tener una capacidad de buffer de hasta 6MB.			
7.3.7	Los dispositivos deben poder apilarse en grupos de hasta 8 dispositivos.			
7.4.	**Requerimientos Técnicos de Dispositivos de la Red de Gestión Fuera de Banda** Se requieren 2 dispositivos conmutadores en cada uno de los Centros de Datos con las características descritas a continuación:			
7.4.1	Los dispositivos deben contar con 48 puertos 1Gbps ethernet de cobre base T y 4 puertos de 10Gbps Base SFP+.			
7.4.2	Los dispositivos deben contar con fuentes de poder redundantes y que sean removibles en caliente.			
7.4.3	Los dispositivos deben contar con una capacidad de tabla de direcciones MAC de hasta 16,000.			
7.4.4	Los dispositvos deben tener la capacidad de manejar hasta 11,000 rutas IPv4.			
7.4.5	Los dispositivos deben tener una capacidad de conmutación de hasta 95 Mpps.			
7.4.6	Los dispositivos deben tener una capacidad de buffer de hasta 6MB.			
7.4.7	Los dispositivos deben poder apilarse en grupos de hasta 8 dispositivos.			
7.5.	**Requerimientos Técnicos de Dispositivos Enrutadores para el segmento WAN** Se requieren 2 dispositivos enrutadores para el Centro de Procesamiento Alterno con las características descritas a continuación:			
7.5.1	Los dispositivos deben contar con al menos 6 puertos de 1Gbps base SFP y 2 puertos de 10Gbps base SFP+ habilitados.			
7.5.2	Los dispositivos deben soportar un rendimiento de hasta 2.5 Gbps para manejo de ancho banda.			
7.5.3	Los dispositivos deben soportar protocolos de enrutamiento dinámico tales como OSPF, EIGRP y BGP.			
7.5.4	Los dispositivos deben ser ampliables por medio de licencias para soportar hasta 20 Gbps de rendimiento.			
7.5.5	Los dispositivos deben contar con fuentes de poder redundante y reemplazable en caliente.			
7.5.6	Los dispositivos deben soportar visibilidad de aplicaciones a nivel de capa 7 por medio de análisis de tráfico.			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
7.5.7	Los dispositivos deben soportar el rendimiento de tráfico cifrado de hasta 8 Gbps.			
7.5.8	Los dispositivos deben soportar la característica de implementación de contrafuegos basados en zonas.			
7.5.9	Los dispositivos deben soportar hasta 3,500,000 de rutas IPv4 o 3,000,000 de rutas IPv6.			
7.5.10	El dispositivo debe soportar redundancia de software de manera intrínseca para incrementar el nivel de disponibilidad de la plataforma.			
7.5.11	El dispositivo debe soportar la habilitación de cifrado AES y el establecimiento de tuneles IPSec.			
7.5.12	El dispositivo debe soportar la habilitación de protección a nivel de control planel en caso de ataques de denegación de servicio.			
7.5.13	El dispositivo debe soportar alta disponibilidad y convergencia de túneles VPN sin interrupción de sesiones activas.			
7.5.14	El dispositivo debe soportar el análisis de tráfico por medio de capturas Netflow.			
7.6.	**Requerimientos Técnicos de Dispositivos Enrutadores para el segmento de conexión a INTERNET** Se requieren 2 dispositivos enrutadores para el Centro de Procesamiento Alterno con las características descritas a continuación:			
7.6.1	Los dispositivos deben contar con al menos 6 puertos de 1Gbps base SFP y 2 puertos de 10Gbps base SFP+ habilitados.			
7.6.2	Los dispositivos deben soportar un rendimiento de hasta 2.5 Gbps para manejo de ancho banda.			
7.6.3	Los dispositivos deben soportar protocolos de enrutamiento dinámico tales como OSPF, EIGRP y BGP.			
7.6.4	Los dispositivos deben ser amplicables por medio de licencias para soportar hasta 20 Gbps de rendimiendo.			
7.6.5	Los dispositivos deben contar con fuentes de poder redundantes y reemplazables en caliente.			
7.6.6	Los dispositivos deben soportar visibilidad de aplicaciones a nivel de capa 7 por médio de análisis de tráfico.			
7.6.7	Los dispositivos deben soportar el rendimiento de tráfico cifrádo de hasta 8 Gbps.			
7.6.8	Los dispositivos deben soportar la característica de implementación de contrafuegos basados en zonas.			
7.6.9	Los dispositivos deben soportar hasta 3,500,000 de rutas IPv4 o 3,000,000 de rutas IPv6.			
7.6.10	El dispositivo debe soportar redundancia de software de manera intrinseca para incrementar el nivel de disponibilidad de la plataforma.			
7.6.11	El dispositivo debe soportar la habiltiación de cifrado AES y el establecimiento de tuneles IPSec.			
7.6.12	El dispositivo debe soportar la habilitación de protección a nivel de control plane en caso de ataques de denegación de servicio.			
7.6.13	El dispositivo debe soportar alta disponibilidad y convergencia de túneles VPN sin interrupción de sesiones activas.			
7.6.14	El dispositivo debe soportar el análisis de tráfico por medio de capturas Netflow.			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
7.7.	**Requerimientos Técnicos de Dispositivos Enrutadores para el segmento de conexión con Terceros** Se requieren 2 dispositivos enrutadores para el Centro de Procesamiento Alterno con las características descritas a continuación:			
7.7.1	Los dispositivos deben contar con al menos 6 puertos de 1Gbps base SFP y 2 puertos de 10Gbps base SFP+ habilitados.			
7.7.2	Los dispositivos deben soportar un rendimiento de hasta 2.5 Gbps para manejo de ancho banda.			
7.7.3	Los dispositivos deben soportar protocolos de enrutamiento dinámico tales como OSPF, EIGRP y BGP.			
7.7.4	Los dispositivos deben ser amplicables por medio de licencias para soportar hasta 20 Gbps de rendimiendo.			
7.7.5	Los dispositivos deben contar con fuentes de poder redundantes y reemplazables en caliente.			
7.7.6	Los dispositivos deben soportar visibilidad de aplicaciones a nivel de capa 7 por médio de análisis de tráfico.			
7.7.7	Los dispositivos deben soportar el rendimiento de tráfico cifrádo de hasta 8 Gbps.			
7.7.8	Los dispositivos deben soportar la característica de implementación de contrafuegos basados en zonas.			
7.7.9	Los dispositivos deben soportar hasta 3,500,000 de rutas IPv4 o 3,000,000 de rutas IPv6.			
7.7.10	El dispositivo debe soportar redundancia de software de manera intrinseca para incrementar el nivel de disponibilidad de la plataforma.			
7.7.11	El dispositivo debe soportar la habiltiación de cifrado AES y el establecimiento de tuneles IPSec.			
7.7.12	El dispositivo debe soportar la habilitación de protección a nivel de control plane en caso de ataques de denegación de servicio.			
7.7.13	El dispositivo debe soportar alta disponibilidad y convergencia de túneles VPN sin interrupción de sesiones activas.			
7.7.14	El dispositivo debe soportar el análisis de tráfico por medio de capturas Netflow.			
8.	**Requerimientos Técnicos de la plataforma de transporte óptico DWDM** En esta sección se detallan los requerimientos mínimos para la solución de replicación óptica de los centros de datos de la CCSS, tomando en cuenta características de latencia, capacidad, seguridad, monitoreo y control. Las consideraciones de definición de hardware están basadas en los diseños establecidos internamente y la aplicación de los modelos de comunicación hacia los que se desea migrar, por lo que se requiere que las propuestas de equipos estén alineadas con los requisitos explícitos detallados a continuación			
8.1.	Se requiere de una solución de transporte óptico multi-servicio DWDM para comunicar los dos centros de procesamiento de datos que actualmente tiene el CCSS			

Nº	Descripción del Cartel	Cumple		Descripción del oferente
		Sí	No	
	La solución a ser implementada debe proveer transparencia de servicios, flexibilidad de topologías, variedad de interfaces de cliente y patrones de tráfico reconfigurables.			
8.2.	La solución implementada debe estar conformada por una plataforma modular que albergue las diferentes tarjetas de servicios ópticos. La plataforma propuesta DWDM debe ser redundante en todos sus elementos comunes (fuentes de poder, sistemas de enfriamiento, tarjetas de control). También la configuración propuesta deberá ser una de alta disponibilidad, contemplando conexión en anillo ente los dos sitios vía dos (2) rutas de planta externa de fibra independientes con diversidad geográfica, permitiendo completa protección del tráfico aprovisionado en caso de un corte de fibra.			
8.3.	La plataforma DWDM propuesta deberá contemplar el uso de dos (2) subracks por sitio, distribuyéndose las tarjetas muxponder y módulos fotónicos activos entre ellos (un subrack sería espejo del otro). El conjunto de dos subracks en un sitio se deberá poder administrar como un único nodo DWDM en configuración multichasis. Para el potencial crecimiento del sistema añadiendo nuevas tarjetas, cada subrack deberá ofrecer la posibilidad de al menos quince (15) slots universales que permitan hospedar módulos fotónicos y muxponders.			
8.4.	Los subracks de los nodos DWDM deberán ofrecer en forma nativa la posibilidad de canalización de aire en su sistema de enfriamiento de la parte frontal a la posterior (“front to back”), de manera de habilitar su instalación en data centers con sistema de control de temperatura basada en “pasillo frio – pasillo caliente”. Los nodos DWDM deberán poder ser instalados en racks de 19’ o en gabinetes cerrados de los usados en centros de computo			
8.5.	El sistema DWDM propuesto debe permitir que operaciones de inserción y remoción de tarjetas puedan hacerse en caliente (hot swap), sin afectar el funcionamiento del resto de los módulos del sistema.			
8.6.	El sistema DWDM propuesto debe permitir actualizaciones de software sin afectación de los servicios aprovisionados y operativos (in service software upgrade)			
8.7.	Los subracks de los nodos DWDM deberán ser alimentados por energía AC 220V. Las fuentes de poder deben ser nativas usando			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	energía AC sin la necesidad de usar rectificadores externos. Las fuentes de poder deberán ofrecer una configuración redundante 2+2 o mejor.			
8.8.	El sistema de enfriamiento de los subracks deberá estar compuesto por un “fran tray” con multiples ventiladores de velocidad variable controlados y alimentados a través de circuitos independientes.			
8.9.	La configuración propuesta para los sistemas DWDM deberá ser una de alta disponibilidad, contemplando conexión en anillo ente los dos centros de cómputo vía dos (2) rutas de planta externa de fibra independientes con diversidad geográfica, permitiendo completa protección del tráfico aprovisionado en caso de un corte de fibra. La redundancia a ser contemplada, deberá incluir distribuir tarjetas muxponder y módulos fotónicos activos entre los dos subracks en cada sitio, (un subrack sería espejo del otro). Las interfaces tributarias (4x10GE y 2x16GFC) de la plataforma DWDM que hacen interfaz con los centros de cómputo serán interconectadas en forma dual a tarjetas muxponders en cada subrack, construyendo así una arquitectura tolerante a fallas extremo a extremo.			
8.10.	Los sistemas DWDM provistos deberán contar con tarjetas de control redundantes. Estas tarjetas deberán poseer memorias flash para almacenar el software de los equipos, los archivos de configuración y logs de alarmas. La tarjeta de control de la plataforma DWDM debe efectuar: la inicialización del sistema, aprovisionamiento, mantenimiento, diagnósticos, detección y resolución de direcciones IP, terminación del canal óptico de servicio (OSC) de la red de comunicaciones de datos DWDM y detección de fallas en el sistema para cada plataforma de la solución. Estas tarjetas de control deberán también soportar la funcionalidad OTDR, integrada junto el puerto para el canal de servicio óptico (OSC). El OTDR deberá ofrecer conexiones dedicadas para cada ruta de fibra para poder realizar mediciones de manera bidireccional en ellas, permitiendo determinar perdidas de inserción, reflexiones y atenuaciones. Cada subrack deberá contar con dos (2) tarjetas de control y una de ellas tendrá habilitada la funcionalidad OTDR y la otra podrá ser una de tipo regular (sin OTDR) El OTDR deberá ser de tipo digital en vez de usar pulsos de luz de alta energía. El sistema de gestión deberá presentar las mediciones de manera gráfica y permitir exportarla en formato SOR.			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
8.11.	La solución para implementar debe ser llave en mano, o sea, que la oferta debe cubrir tanto los equipos DWDM, como los servicios profesionales requeridos para la implementación, pruebas y puesta en operación. Se deberá entregar la documentación de la red construida ("as build diagrams"), el reporte de presupuesto óptico (Optical Link Budget) y el reporte de los servicios aprovisionados.			
8.12.	La instalación y puesta en servicio de la plataforma DWDM debe ser ejecutado por personal del fabricante de los equipos o por "partners" certificados en la tecnología. En el caso de que los trabajos sean realizados por personal de "partners", el fabricante de los equipos deberá certificar de manera escrita la experiencia y adiestramientos el "partner" que lo califiquen para acometer los trabajos. De preferencia, el "partner" que realice los trabajos deberá también tener experiencia comprobada tecnología equipos de red Cisco usados en centros de computación de manera de facilitar la integración y pruebas.			
8.13.	El fabricante de los equipos DWDM deberá tener experiencia comprobada en Costa Rica, con al menos tres (3) clientes distintos que interconecten sus centros de cómputo con interfaces Ethernet y Fibra Canal. Los sistemas DWDM en estos clientes de referencia deben estar ya implementados y en servicio al menos dieciocho (18) meses previos al momento de presentar la propuesta.			
8.14.	Los centros de computación usan equipamiento Cisco en sus redes, los cuales serán interconectados al sistema DWDM solicitado. En tal sentido el sistema DWDM propuesto deberá estar certificado para inter-operar con los sistemas Cisco existentes, por lo cual se deberá presentar una carta emitida por Cisco Systems Costa Rica que certifique que el sistema DWDM ofertado y en la configuración provista está certificado en su interoperabilidad garantizando un óptimo funcionamiento. También, se deberá garantizar de manera escrita la interoperatividad de la solución DWDM con las plataformas de Cisco interconectadas tanto para futuras versiones de software y para actualizaciones de HW dentro de las mismas familias de productos. Los centros de computación a ser interconectados usarán Cisco ACI (familia Nexus 9000) y SAN con Cisco MDS 9710/9396T.			
8.15.	En el caso que el fabricante del sistema DWDM propuestos no poseer experiencia certificada con los sistemas Cisco indicados, el proveedor se deberá comprometerse a hacer pruebas de certificación de con los equipos Cisco. Esto deberá ser contratado por el proveedor del sistema DWDM directamente con Cisco Systems Costa Rica y deberá hacerse cargo de cubrir los todos costos los servicios profesionales propios y los que deba contratar a Cisco, así como el uso de laboratorio y cualquier otro tema de logística u costo suplementario. Estas pruebas se deberán realizar en laboratorios especializado donde se pueda modelar el ambiente y arquitectura específicos de los centros de computación, los sistemas DWDM se deberán llevar allí y probar todos los aspectos funcionales necesarios para			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	garantizar una óptima interoperabilidad con los sistemas de los centros de computación. La decisión final sobre el uso del sistema DWDM propuesto estará condicionada a que todas las pruebas de interoperabilidad sean exitosas según un alcance acordado previamente. Todas las pruebas que se realicen y los costos que puedan conllevar las pruebas serán por cuenta y riesgo del proponente del equipo DWDM, sin responsabilidad alguna en su resultado por parte de la CCSS ni en los costos en que se incurran. En cualquier caso, el tiempo que tome la realización de todas las pruebas y validaciones deberá ajustar con el cronograma de implementación solicitado, siendo no aceptable la modificación del mismo. Se deberá presentar una carta donde se haga el compromiso con todo lo antes indicado y también se deberá presentar una carta de Cisco Systems Costa Rica donde se establezca que se ha acordado con ellos realizar estas pruebas.			
8.16.	La solución implementada debe operar como un ROADM (Reconfigurable Optical Add/Drop Multiplexer) en los dos extremos del anillo (WSS 2x1) para facilitar la agregación de nuevos servicios sin necesidad de intervenir en la capa fotónica del sistema DWDM propuesto. Las tarjetas necesarias que habiliten la funcionalidad ROADM estarán distribuidas en dos (2) subracks por redundancia (una en casa subrack). Las tarjetas ROADM deberán integrar en una misma unidad junto con el WSS el módulo de amplificación EDFA a nivel de pre-amplificador y de ser requerido por el diseño fotónico propuesto un booster (post-amplificador)			
8.17.	La solución implementada debe incluir todo el hardware y software necesario para operar como un ROADM de 40 canales (espaciamiento 100GHz según canalización estándar ITU)			
8.18.	Junto con el hardware y software necesarios para habilitar la funcionalidad de ROADM, se deberán incluir los módulos pasivos Mux/Demux. Los mismos deberán estar disponibles en unidades de 40 canales o en unidades más pequeñas de cuatro canales, las cuales deben venir en diez variantes según los grupos de canales que tengan y permitir también la interconexión de ellos (“Daisy chaining”). Para la configuración propuesta de podrán usar Mux/Demux de cuatro canales, uno por cada grado del ROADM en cada sitio. Los mux/demux si bien son elementos pasivos, que se instalan fuera de los slots del subrack, deberán estar interconectados al mismo			

Nº	***Descripción del Cartel***	***Cumple***		***Descripción del oferente***
		Sí	***No***	
	via puertos USB o similares, para poder detectar su presencia en el sistema para propósitos de inventario.			
8.19.	La solución propuesta deberá incluir tarjetas Muxponder de alta capacidad, tales que permitan atender las necesidades inmediatas y futuras de manera modular, activando el uso de capacidad / BW de puertos y otras funcionalidades vía licenciamiento de software			
8.20.	Los Muxponders requeridos deberán proveer las siguientes características mínimas: 1. El Muxponder será una única pieza de HW en la que vienen embebidos los puertos troncales DWDM y los puertos clientes (tributarios) 2. Los Puertos DWDM (cantidad 2) que habiliten troncales DWDM con láser sintonizables, transmisión coherente a 100Gbps, 150Gbps o 200Gbps. Estos puertos DWDM deberán ser modulares con transceivers CFP2 ACO 3. Puertos clientes (tributarios) que habiliten la posibilidad de interconectar los sistemas de red de los centros de cómputos con interfaces 10GE y 16G Fibra Canal (16G FC). Se deberán ofrecer al menos diez (10) puertos que usen transceivers multipuerto QSFP+ para interfaces 10GE y 16GFC. La capacidad total de fanout de trafico deberá ser de hasta 400Gbps por tarjeta, disponiéndose también de otros tipos de puertos como 8G FC/ 10GFC, 40GE y 100GE que pueden activarse vía la incorporación de otros transceivers para habilitar puertos 40GE y 100GE 4. El Muxponder deberá ofrecer un modelo de licenciamiento que permita usar la capacidad de manera modular, habilitando puertos clientes y DWDM a medida que sean requeridos 5. Los servicios agregados en los muxponders deberán ser transportados de manera transparente entre los sitios. 6. Los puertos troncales DWDM se deberán poder configurar con diferentes técnicas de modulación digital, habilitando capacidad incremental en ellos: 100Gbps (QPSK), 150Gbps (8QAM) y 200Gbps (16QAM). También los puertos deberán implementar un SD-FEC fuerte para detección y corrección de errores en la transmisión. 7. La tecnología coherente usada en las líneas DWDM deberá ofrecer una transmisión óptica eficiente, ofreciendo también capacidades avanzadas como compensación electrónica de la dispersión cromática acumulada y compensación al PMD. 8. El muxponder deberá soportar otros features avanzados como PBRS, LLDP, Encriptación de tráfico en capa 0 (AES 256), y conmutación/agregación de trafico via un motor OTN embedido (no requiriendose switch fabric externo)			

Nº	Descripción del Cartel	Cumple		Descripción del oferente
		Sí	No	
	9. La tarjeta Muxponder debe soportar Pseudo Random Binary Sequence (PRBS), lo que habilita la prueba de circuitos extremo a extremo entre dos localidades. 10. La tarjeta Muxponder deberá tener un buen desempeño en en su requerimiento de OSNR (optical signal-to-noise ratio): Minimum B2B OSNR 0.1nm RWB for BER <10E-15: 11.3dB for CP-QPSK, 19.6 dB for CP-16QAM) 11. La tarjeta Muxponder debe ser robusta en el manejo de la dispersión cromática eliminando la necesidad del uso de equipo suplementario para su manejo (Mínimo +/-70.000 ps/nm fpara CP-QPSK, +/-25.000ps/nm para CP-16QAM) 12. Los puertos troncales DWDM deben proveer soporte a mediciones de desempeño (performance monitoring) transparente de acuerdo a las especificaciones en ITU G.709 Optical Transport Network (OTN) y G.8021 standards. El cálculo y acumulación de mediciones de desempeño deben soportarse en intervalos de 15-minutos y 24-houras de acuerdo a ITU G.7710. 13. Un sunbrack del sistema DWDM deberá soportar hasta site (7) muxponders como los descritos 14. El fanout de los puertos de 10GE y 16G FC con ópticas monomodo podrá hacerse vía paneles que deberán ser provistos como parte del Sistema. Al ser estos paneles elementos pasivos, se instalan en accesorios externos al subrack del equipo DWDM. Los paneles aunque son elementos pasivos, deberán estar interconectados al subrack (via puertos USB o similares) para poder detectar su presencia en el sistema para propósitos de inventario. Los puertos en el muxponder se conectaran con cables multifibra a estos paneles. En el caso de puertos con opticas multimodo, estos paneles no son requeridos como suministro del proveedor del equipo DWDM, pudiéndose usar cables multimodo MPO a NxLC.			
8.21.	La configuración propuesta para el sistema DWDM solicitado deberá desplegar longitudes de onda de 200Gbps, sobre ellas de deberán multiplexar los servicios Nx10GE y Nx16GFC usando tarjetas Muxponders como las antes descritas. Se deberá usar el modelo de pago por capacidad licenciado disponible para el Muxponder			
8.22.	En la solución propuesta se debe proveer funciones ecualización y control automático de potencia que deben efectuar las siguientes funciones: • Mantener una potencia constante por canal cuando ocurren cambios en el número de canales. La potencia constante por canal maximiza el desempeño del sistema y aumentará la tolerancia a fallas de la red óptica.			

Nº	***Descripción del Cartel***	***Cumple***		***Descrip-ción del oferente***
		Sí	***No***	
	• Compensar por degradación óptica de la red (efectos de envejecimiento y reparaciones en la fibra a lo largo de su vida útil). Simplificar la instalación y la actualización de la red óptica DWDM, calculando automáticamente los niveles de referencia de los amplificadores.			
8.23.	La plataforma que se implemente deberá contar con un sistema de gestión monitoreo que permita un análisis proactivo de todos y cada uno de los eventos que ocurran, que permita el monitoreo de las interfaces de cliente que se tengan conectados a ésta, así como los troncales DWDM del anillo que permite la interconexión de los centros de cómputo. Este sistema de monitoreo y gestión deberá ofrecer una interfaz gráfica (GUI) sencilla e intuitiva que permita una eficiente administración y configuración del sistema. El sistema de monitoreo deberá ser una aplicación de SW que pueda instalarse en estaciones de trabajo (Windows, Linux o MAC OS) interactuando de manera directa con los nodos DWDM vía la subred de gestión, no requiriéndose de servidores dedicados (bare metal) y/o capacidad de computación en máquinas virtuales (VMs). También deberá ser provisto un software para planeación de la red DWDM, que permita modelar y validar futuros incrementos de capacidad en el sistema así como eventuales cambios en la fibra usada y/o el HW sitios. Este software de planeación deberá ser uno sencillo y gráfico, pudiendo ser instalado en estaciones de trabajo con sistema operativo Windows o Mac OS, sin la necesidad del uso de servidores dedicados (bare metal) o capacidad en máquinas virtuales (VMs)			
8.24.	En la solución implementada, las interfaces suministradas con la plataforma DWDM se deberán acoplar a las interfaces ópticas de los equipos que posee la CCSS y que se indican en la Tabla #1, incluyendo tanto sus tipos, BW y e interfaz óptica (monomodo y/o multimodo)			
8.25.	La solución implementada debe permitir el aprovisionamiento y el monitoreo de las longitudes de onda de extremo a extremo, incluyendo la interfaz de puertos clientes asociados.			
8.26.	En la solución propuesta debe poder permitir medicines directas de la potencia óptica en las diversas partes del sistema, incluyendo puertos clientes, puertos DWDM y amplificadores EDFA. Asimismo, el sistema propuesto debe implementar mecanismos para ecualización automática de potencia óptica en la etapa de inserción/extracción de tráfico.			
8.27.	En la solución implementada, se debe contar con mecanismos de control automático de la ganancia y de control automático de la potencia en las unidades de amplificación óptica que posea. Estos mecanismos permitirán compensar la degradación de la fibra al igual que cambios bruscos en la cantidad de canales sobre la misma.			
8.28.	En la solución implementada, se debe proveer un mecanismo			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	para protección de tráfico que permita atender eventuales escenarios de costes de fibra óptica. En estos casos, al ocurrir el corte en la fibra el sistema conmuta todo el tráfico que estaba cursando por la fibra que está ahora cortada se conmuta a la otra ruta disponible en el anillo en un tiempo igual o menor a 50ms. Bajo esta opción de redundancia, cada troncal DWDM en las tarjetas Muxponders deberá ser interconectado a un switch photonico el cual permite la conexión de un troncal a canales asociados dos rutas diversas en los cables de fibra optica que interconectan los centros de cómputo. Este switch fotonico deberá ser una tarjeta del sistema provisto que ocupe un slot en los subracks por sitio. Debe operar con longitudes de onda en toda la banda C (1529 nm to 1562.5 nm) y ser agnóstico a la velocidades de transmisión de las lontigudes de onda determinadas por la técnica de modulación configurada El switch fotonico deberá permitir el monitoreo de dempeño y el manejo de alarmas ajustando los umbrales, asi como soportar prioridades según ITU-T G.873.1. También se deberá soportar ALS (automatic laser shutdown).			
8.29.	Es importante recalcar que todos y cada uno de los Tributarios (Nx10GE, Nx16GFC) que se conectarán a la plataforma ofertada, deberán de ser duplicados por puerto. Entiéndase con esto, todos los Tributarios se contarán al nodo DWDM con 2 puertos en 2 tarjetas (muxponders) totalmente independientes en esta plataforma, instaladas en 2 subracks independientes. Adicionalmente desde cada subrack se realizarán conexiones independientes a 2 rutas físicas diversas (una por subrack), las cuales permitirán proteger con el uso de switches ópticos la totalidad del trafico aprovisivionado en caso de un corte de fibra (tráfico de ambos subracks), estas conexiones a los cables de fibra deberán ser a dos tarjetas ROADM/amplificadoras independientes.			
8.30.	En la solución implementada, el monitoreo de eventos también debe registrarse en la log de auditoría. Un evento se definirá como el cambio del estado de un elemento dentro de la red. Los eventos externos, eventos internos, cambios en los atributos, y las actividades de carga y descarga de software deberán ser registrados en los rastros de auditoría. El rastro de auditoría se debe almacenar en memoria flash y no debe corromperse por conmutaciones, reinicializaciones, o actualizaciones del procesador.			
8.31.	Para los sistemas DWDM propuestsa, los administradores deben poder configurar múltiples usuarios y asignarles diversas categorías (perfiles) de acuerdo a las funciones específicas que realizan. Estos usuarios pueden ser autenticados localmente en los nodos del sistema DWDM o bien pueden utilizar autentificación RADIUS (Remote Authentication Dial In User Service)			
8.32.	Todos los equipos ofertados en la solución deben ser nuevos, y de la misma marca y fabricante y modelo.			

Nº	Descripción del Cartel	Cumple		Descripción del oferente
		Sí	No	
8.33.	La solución debe ser puesta en producción a satisfacción del CCSS y tomando en cuenta las condiciones que describe el presente documento.			
8.34.	Los sistemas DWDM a ser propuestos deberan soportar operar en ambientes con las siguientes especificaciones: • Operating, nominal: 41 to 104°F (5° to 40°C) Operating, short-term: 23 to 131°F (-5° to 55°C) Non-operating: -40 to 158°F (-40° to 70°C) • Operating humidity: Normal: 5 to 85%, noncondensing. Short-term: 5 to 90% but not to exceed 0.024 kg water/kg of dry air Estándares regulatorios: o EMC (class A) ▪ ICES-003 Issue 4 (2004) ▪ GR-1089-CORE, Issue 4 (Type 2 and Type 4 equipment) ▪ GR-1089-CORE - Issue 03 (Oct 2002) (Objective O3-2 - Section 3.2.1 - Radiated Emissions requirements with all doors open) ▪ FCC 47CFR15, Class A Subpart B (2006) o Safety ▪ CSA C22.2 #60950-1 – Edition 7, March 2007 ▪ UL 60950-1 – Edition 2, March 2007 ▪ GR-1089-CORE, Issue 6 (Type 2 and Type 4 equipment) o Laser ▪ UL 60950-1 – Edition 2, March 2007 ▪ IEC 60825-1: 2001 Ed.1.2 (incl. am1+am2) Safety of laser products Part 1: Equipment classification, requirements and users guide ▪ IEC60825-2 Ed.3 (2004) Safety of laser products Part 2: Safety of optical fiber communication systems + A1:2006 o Environmental ▪ GR-63-CORE Issue 3, Network Equipment Building Standards (NEBS) Physical Protection, March 2006 o Optical ▪ EN or IEC-60825-2 Third edition (2004-06)			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
8.35.	**Servicios de Mantenimiento Preventivo y Correctivo de los equipos**			
8.36.	Se debe realizar un mantenimiento preventivo para el adecuado funcionamiento de la solución en el nuevo ambiente.			
8.37.	Estos servicios tienen una atención permanente a toda la Plataforma Ofertada, en la modalidad 7x24x365.			
8.38.	El contratista debe incorporar en esta solución todas las anticipaciones logísticas, de costos y recursos humanos para cumplir con los requisitos solicitados en este apartado del presente cartel.			
8.39.	El contratista asume toda la responsabilidad sobre la integridad de los equipos en el traslado, elevación y ubicación de estos en ambos Centros de Datos.			
8.40.	Se debe realizar una visita trimestral preventiva, la cual incluya al menos las siguientes labores. • Análisis de acciones recomendadas por el fabricante. • Análisis de comportamiento y funcionamiento de los equipos, revisión de logs, revisión de estadísticas, pruebas de integridad y redundancia (si aplica). • Actualización del sistema operativo de los equipos cuando estos lo requieran según recomendación del fabricante y verificación con el ambiente operacional de la CCSS tras los mantenimientos. • Aplicación de parches cuando estos lo requieran. • Informe de visita trimestral con al menos lo siguiente: ○ Fecha y periodo de la visita. ○ Acciones realizadas. ○ Reporte de situaciones anómalas. ○ Recomendaciones técnicas. ○ Responsable de la visita ○ Estado de los equipos.			
8.41.	En el Servicio de Mantenimiento preventivo, el contratista debe guardar un expediente exclusivo para la CCSS, mediante el cual tenga el registro de todas las versiones instaladas de Sistema Operativos, Release de Patches, versiones de firmware.			
8.42.	Con base en este registro, cada 6 meses el contratista debe comparar las versiones de software y firmware de los equipos de la plataforma instalada contra la más reciente versión liberada por el fabricante, con el objetivo de determinar si es recomendable y factible la actualización de dichos elementos, y planificar la actualización más conveniente que proceda, tomando en cuenta las ventanas de tiempo fuera de línea que podría ofrecer la Plataforma Ofertada para estos menesteres.			
8.43.	El parchado y actualización del sistema operativo será responsabilidad del contratista.			
8.44.	**Servicios de Mantenimiento Correctivo**			
8.45.	El mantenimiento correctivo, incluye:			

Nº	***Descripción del Cartel***	***Cumple***		***Descripción del oferente***
		Sí	***No***	
	• Cambio de partes dañadas. • Atención de averías y problemas de funcionamiento. • Ajuste y/o reemplazo de las partes electrónicas, eléctricas, mecánicas y/o electromecánicas. • Tiempos de respuesta para la atención y corrección de problemas no mayores a 2 horas a partir de la generación del reporte vía telefónica o vía correo electrónico, y máximo 4 horas para la restauración del servicio, en el Centro de Procesamiento Principal. • Para equipos que se encuentren instalados en el Centro de Procesamiento Alterno que se encuentre fuera de la GAM, el tiempo de atención y corrección de problemas no debe ser mayor a 6 horas a partir de la generación del reporte vía telefónica o vía correo electrónico y máximo de 4 horas para la restauración del servicio. • Después de la atención de cada solicitud de servicio realizado por la CCSS, el contratista debe brindar un reporte con al menos lo siguiente: ○ Fecha y periodo de atención. ○ Detalle de las labores realizadas. ○ Identificación de las causas por las cuales el sistema sufrió una caída. ○ Responsable de la visita. ○ Estado de los equipos (impacto). ○			
8.46.	Las labores de mantenimiento que generen interrupción de servicios deben realizar fuera de horario de oficina, previa coordinación y aprobación del encargado general de la contratación.			
8.47.	El contratista debe brindar en forma detallada el método oficial de reporte de averías (MOR) tanto para horario de oficina como horario fuera de oficina.			
8.48.	El servicio de mantenimiento para la atención de averías debe estar disponible las 24 horas del día, los 7 días de la semana.			
8.49.	Debe cubrir los repuestos originales necesarios para reparar el equipo, los gastos de envío o de desplazamiento y la mano de obra.			
8.50.	Cada componente de hardware o software; deben ser aptos para el correcto funcionamiento de la solución indicada en este cartel.			
8.51.	Debe garantizar el correcto ensamblado de cada uno de los componentes de hardware y software de los equipos para la solución indicada en este cartel.			
8.52.	Cada equipo, componente de hardware o software; deben ser la versión más reciente ofrecida en el mercado para la solución indicada en este cartel.			
8.53.	Permitir actualizaciones y parchados liberados por el fabricante para el hardware y software de sistema operativo.			
8.54.	Ante la eventual falla de alguno de los componentes de hardware que forman la solución, la misma Debe ser reemplazada por otra idéntica.			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
9.	**Requerimientos Técnicos del Servicio de Integración de la Plataforma de Comunicaciones** Como parte de los servicios de integración de la solución se requiere que el proceso considere las siguientes metodologías antes, durante y posterior a la instalación:			
9.1.	Una vez adjudicado, el oferente preparará el documento con la descripción detallada de la solución que explique las características a instalar y habilitar, las topologías físicas y lógicas a implementar, la descripción de los dispositivos incorporados y su rol operativo dentro de la arquitectura general.			
9.2.	Una vez adjudicado, el oferente preparará el documento con la definición detallada del alcance de servicios a implementar y donde se detallen las responsabilidades del lado del oferente y de la CCSS en cuanto a cada sección del proceso a implementar. El mismo documento debe detallar los entregables concretos que formarán parte del servicio, incluyendo, pero no limitados a: documentación, proceso de transferencia de conocimientos, diagramas, tablas de información técnica y cualquier otro que sea requerido. También se deben documentar los requerimientos ambientales, físicos y logísticos que puedan ser necesarios para la ejecución del servicio, de tal forma que se realicen las consideraciones respectivas por parte de la CCSS.			
9.3.	El mismo será revisado y aprobado por parte de la CCSS siempre que este cumpla con los requisitos y especificaciones establecidas en este documento.			
9.4.	Una vez adjudicado, el oferente preparará el plan de implementación de los servicios en formato de diagrama de Gantt, donde se detallen las actividades, responsables y tiempos requeridos durante el proceso de instalación e integración de la solución.			
9.5.	Una vez adjudicado, el oferente preparará el documento que detalle las configuraciones a implementar y donde se describa el rol de éstas dentro de la solución general. Este documento Debe incluir tablas de interfaces a utilizar, plan de direccionamiento IP utilizado y el detalle de los procesos de configuración a ejecutar.			
9.6.	Se requiere que todos los elementos de la solución puedan tener habilitada la red de gestión de fuera de banda y será responsabilidad del oferente proveer la definición de arquitectura a implementar en la red existente de la CCSS para que esto posible. Esta red de gestión de fuera de banda debe estar aislada del ambiente de conmutación productivo utilizado actualmente.			
9.7.	Se requiere que como parte del servicio se hagan las evaluaciones necesarias de la infraestructura actual de la CCSS y que cualquier configuración o planteamiento topológico considere las implicaciones técnicas relacionadas a la integración de la solución. Estas evaluaciones no se limitarán únicamente a los dispositivos de comunicaciones, pues deben considerar los dispositivos de procesamiento dentro de la red del Centro de Datos productiva de la CCSS.			
9.8.	Como parte de la propuesta técnica y previo a la adjudicación, el oferente debe proveer donde se describa e ilustre el diseño de la solución, los dispositivos a utilizar, los mecanismos de integración			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	y las características y protocolos incorporados como parte de la solución. Como parte de la propuesta técnica y previa a la adjudicación, el oferente deberá proveer el documento que establezca el proceso de implementación, migración, puesta en producción y adopción de la solución de comunicaciones. Una vez finalizado el proceso de instalación y previo a la entrega final del proyecto, el oferente preparará el informe técnico de la solución que detalle las actividades realizadas, las configuraciones ejecutadas y la descripción del estado en el que la solución queda operando. Este documento incluirá diagramas físicos y lógicos de la interconexión y los flujos de tráfico existentes considerando cualquier instancia virtual que se haya creado en la infraestructura de comunicaciones. El oferente deberá proveer la figura de Gerente de Proyecto durante el transcurso de la ejecución de este de tal forma que exista un seguimiento detallado de las actividades realizadas, los requisitos de ejecución, el manejo de recursos y en general todo lo relativo al desarrollo del proyecto. Este recurso reportará avances periódicamente de acuerdo con los requerimientos establecidos por la CCSS. Este diseño correspondiente a la solución de actualización de la Infraestructura de Comunicaciones para el Centro de Procesamiento Primario y Alterno (Subítem 1.2) de ser en base a los requerimientos descritos y la documentación de este debe ser provisto por el fabricante en base a sus mejores prácticas y capital intelectual. La implementación, integración y migración debe ejecutarse siguiendo las guías y documentación del fabricante con aprobación de la CCSS. El fabricante debe proveer el documento de diseño en detalle (diagramas de red, funcionalidades a ser configuradas, plantillas generales), el documento de plan implementación, el documento de plan de migración y el documento de pruebas de aceptación. Los servicios avanzados de optimización (Subítem 1.8) no deben ser usados para verificar o corregir la implementación de la solución, estos deben enfocarse en el mejoramiento continuo de la solución y en asistir la operación de esta de acuerdo con las necesidades de negocio de la CCSS. El fabricante de la solución debe proveer durante la Etapa de implementación el plan de pruebas y debe ejecutar las mismas de manera conjunta con el oferente y la CCSS como verificación de que la implementación cumple con el diseño especificado.			
10.	**Requerimientos Técnicos de los Procesos de Migración hacia el Nuevo Ambiente de Comunicaciones**			

Nº	***Descripción del Cartel***	***Cumple***		***Descripción del oferente***
		Sí	***No***	
	Una vez integrada la solución, es necesario que se consideren diferentes aspectos como parte del servicio de migración de la infraestructura de comunicaciones existente hacia el nuevo ambiente implementado.			
10.1.	Una vez que la solución de comunicaciones sea implementada, previo al inicio del proceso de migración de servicios, el oferente Debe entregar el documento que detalle la finalización de la fase de instalación inicial, su estado operativo, las pruebas a ejecutar como parte de la evaluación de condiciones de disponibilidad y cualquier otro elemento que garantice a la CCSS que la solución está lista para el inicio del proceso de migración.			
10.2.	El oferente debe ejecutar el plan de pruebas documentado previamente donde se evalúen todos los elementos de disponibilidad de la solución, incluyendo disponibilidad de dispositivos y sus componentes, la disponibilidad de las plataformas de gestión y las evaluaciones de los servicios de transporte entre los diferentes segmentos de la topología. El plan de pruebas a ejecutar debe ser provisto por el fabricante y aprobado previamente por la CCSS. La ejecución del plan de pruebas debe estar a cargo del oferente y hacerse con presencia de la CCSS.			
10.3.	Inicialmente la solución de comunicaciones debe ser integrada con el ambiente de CORE de red existente, de tal manera que se puedan extender los dominios de broadcast productivos, manteniendo las características de capa 3 en los dispositivos CORE. El oferente debe proveer y documentar los mecanismos para asegurar que dicha interconexión no afectará la red productiva de la CCSS.			
10.4.	Se requiere que el proceso de migración sea progresivo y no disruptivo, ya que todos los servicios operativos alojados en la arquitectura productiva existente no pueden ser trasladados al nuevo ambiente de forma simultánea, debido a los riesgos que esto representa. Se requiere preparar la configuración necesaria para que sea el personal de la CCSS quien determine la programación de ventanas de mantenimiento para realizar los movimientos necesarios. Para mitigar el riesgo de afectación de servicios durante la migración y la integración con mínimo impacto al servicio de los dos Centros de Procesamiento con capacidad de operar en modo Activo-Activo, se requiere que el fabricante de la solución entregue un documento plan de migración y provea el soporte (en sitio o remoto) durante las actividades de migración de los servicios críticos de la CCSS.			
10.5.	Todas las configuraciones aplicadas previo al proceso de migración deben considerar la definición de flujos de los servicios conectados al nuevo ambiente productivo, por lo que es necesario que el oferente tenga completa visibilidad de los servicios transportados en la arquitectura existente. Será posteriormente a la adjudicación que el oferente podrá realizar las evaluaciones, análisis y entrevistas necesarias para realizar el levantamiento de la información necesaria.			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
10.6.	Respecto a la definición de dispositivos, el oferente Debe presentar las tablas de Interfaces requeridas en función de los requerimientos de interconexión de dispositivos de procesamiento, elementos que provean servicios de red y cualquier otro elemento relevante en la estructura topológica. Es responsabilidad del oferente considerar los módulos ópticos y eléctricos ethernet requeridos para el proceso de habilitación de la infraestructura.			
10.7.	El oferente debe incluir todos los servicios de diseño, preparación, migración y estabilización de la solución de comunicaciones propuesta.			
10.8.	El oferente debe contar con al menos 3 casos de éxito en Costa Rica documentados, donde se haga referencia a estructuras topológicas equivalentes y donde se hayan utilizados tecnologías y protocolos similares a los requeridos en este proceso.			
10.9.	El oferente debe contar con ingenieros certificados por el fabricante en la instalación de las tecnologías específicas definidas como parte de la solución. Las certificaciones deben estar avaladas por el fabricante y deben ser comprobables a través de portales dispuestos para tal fin.			
10.10.	Todos los criterios de diseño establecidos deben ser descritos y documentados, incluyendo, pero no limitado a, selección de dispositivos, estructura topológica, selección de protocolos y tecnologías y cualquier otro elemento relevante en la definición del diseño propuesto.			
11.	**Requerimientos Técnicos de Instalación y Migración hacia el Nuevo Ambiente de Comunicaciones** El oferente debe considerar los servicios de instalación, homologación, integración y migración de los dispositivos ofertados. Con el objetivo de garantizar una operación tipo espejo entre ambos centros de datos. Dichos servicios de instalación, homologación, integración y migración deben responder a las topologías físicas y lógicas, prácticas y esquemas detallados en los puntos anteriores. A continuación, se describe el mínimo de actividades técnicas que el oferente debe considerar en su ofrecimiento de servicios y serán sus responsabilidades una vez adjudicado.			
11.1.	**Condiciones Generales del servicio de instalación** Es responsabilidad del adjudicatario, indicar y certificar que las condiciones de instalación de los dispositivos bajo su oferta cumplan con las especificaciones detalladas en las hojas de datos del o los fabricantes. Dichas condiciones deben ser incluidas en el documento de despliegue descrito en secciones anteriores.			
11.2.	El adjudicatario debe instalar físicamente todos los dispositivos en los bastidores que la CCSS proveerá en el CPP, cumpliendo con			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	las especificaciones, procedimientos y requerimientos que el oferente indique en las hojas de datos de los dispositivos ofertados. Y son responsabilidad del oferente los equipos la instalación y condiciones que va ofrecer por medio del CPA.			
11.3.	El adjudicatario será responsable de los trabajos de conectorización, identificación y cableado de los enlaces a fin de la entrega funcional de la solución descrita en los documentos de diseño, detallados en secciones anteriores, y de acuerdo con las mejores prácticas establecidas en la industria. El detalle de enlaces debe estar descrito detalladamente, por el adjudicatario en los documentos de diseño y despliegue.			
11.4.	El adjudicatario, debe energizar e inicializar, los dispositivos con el objetivo de asegurar su funcionamiento incorrupto antes de iniciar las labores de configuración, homologación e integración. Dichas pruebas de funcionamiento deberán ser documentadas según secciones detalladas en capítulos anteriores.			
11.5.	Es responsabilidad del adjudicado revisar las versiones de Firmware o Sistema Operativo de los distintos equipos que utilizará. Es también responsable de la actualización dichos dispositivos según recomendaciones del fabricante y en común acuerdo con el personal técnico de la CCSS. El fabricante debe proveer un reporte con el análisis de riesgo de las versiones de software en base a las funcionalidades específicas que serán implementadas para la solución de la CCSS.			
11.6.	El adjudicatario, es responsable de la configuración de una red fuera de banda bajo las mejores prácticas de la industria y según los requerimientos de administración remota de los dispositivos ofertados. Este bloque operativo será el responsable de proveer gestión mediante protocolos IP a los dispositivos dispuestos en el diseño detallado en los documentos pertinentes.			
11.7.	Es responsabilidad del adjudicatario inicializar todos los dispositivos bajo los protocolos de gestión y seguridad designados bajo las mejores prácticas de la industria y según las especificaciones de gestión o funcionamiento indicadas en el documento de diseño del fabricante y aprobado por la CCSS.			
11.8.	El adjudicatario es responsable de la configuración del ambiente de comunicaciones del centro de datos dispuesto en los documentos de diseño y según las capacidades y buenas prácticas de los equipos ofertados. La configuración del ambiente de comunicaciones debe realizarse siguiendo el plan de implementación provista por el fabricante y aprobado por la CCSS.			
11.9.	El adjudicatario, es responsable la configuración de todos los esquemas de acceso, físicos o virtuales, de todas las plataformas de capacidad de procesamiento. Dichos esquemas Deben estar debidamente documentados según requerimientos de procesos detallados en secciones anteriores.			
11.10.	El adjudicatario, es responsable de la configuración de los requisitos de comunicaciones determinados para esquemas de alta disponibilidad de las plataformas de cortafuegos, balanceadores, IPSs, etc. Dichos esquemas deben estar debidamente documentados según requerimientos de procesos detallados en secciones			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	anteriores.			
11.11.	El adjudicatario es responsable de las conexiones físicas y de las configuraciones lógicas para que los centros de datos logren comunicación entre ellos para soportar tecnologías de alta disponibilidad geográfica. Incluyendo pero no limitándose a; redes extendidas, comunicaciones punto a punto y protocolos de enrutamiento entre sitios.			
11.12.	El adjudicatario, es responsable de la configuración de los requisitos de comunicaciones determinados por cada una de las plataformas de capacidad de procesamiento y aplicaciones alojadas en el centro de datos. De igual manera, dicha arquitectura Debe estar documentada según especificaciones descritas en capítulos anteriores.			
11.13.	El adjudicatario es responsable de la configuración de los esquemas de comunicación para la integración del centro de datos y el núcleo de red (core) de datos actual según diseño y plan de implementación provisto y documentado por el fabricante, el oferente y aprobado por la CCSS. Y bajo las mejores prácticas de industria y fabricante.			
11.14.	El adjudicatario, es responsable de la configuración de los ambientes multicapa del módulo de conexión de borde en ambos centros de datos, con el objetivo de asegurar una migración de servicios transparentes para la operación de la CCSS. El diseño y el plan de configuración de los ambientes multicapa debe ser provisto por el fabricante en base a sus mejores prácticas y capital intelectual. Los servicios avanzados de optimización incluidos como parte de este requerimiento no deben ser usados para verificar o corregir la implementación de la solución, estos deben enfocarse en el mejoramiento continuo de la solución y en asistir la operación de esta de acuerdo con las necesidades de negocio de la CCSS. El fabricante de la solución debe proveer durante la etapa de implementación el plan de pruebas y debe ejecutar las mismas de manera conjunta con la CCSS y el oferente como verificación de la implementación cumple con el diseño especificado.			
11.15.	El adjudicatario es responsable de la configuración, homologación e integración de la arquitectura multicapa para las comunicaciones de la red de usuarios anidada a CPA siguiendo el plan de implementación del fabricante. De igual manera, dicha arquitectura debe estar documentada según especificaciones descritas en capítulos anteriores.			
11.16.	El adjudicatario es responsable de la configuración del bloque de arquitectura de red multicapa para las comunicaciones WAN de la CCSS. Dicha arquitectura debe tomar como mínimo los siguientes elementos constituyentes; acceso, optimización, control lógico e inspección, según el sub-módulo de operación como por ejemplo, Internet o acceso remoto. De igual manera, dicha arquitectura debe estar documentada y validada por el fabricante según especificaciones descritas en capítulos anteriores.			
11.17.	**Procesos de Instalación – Ambiente de Conmutación de DC**			

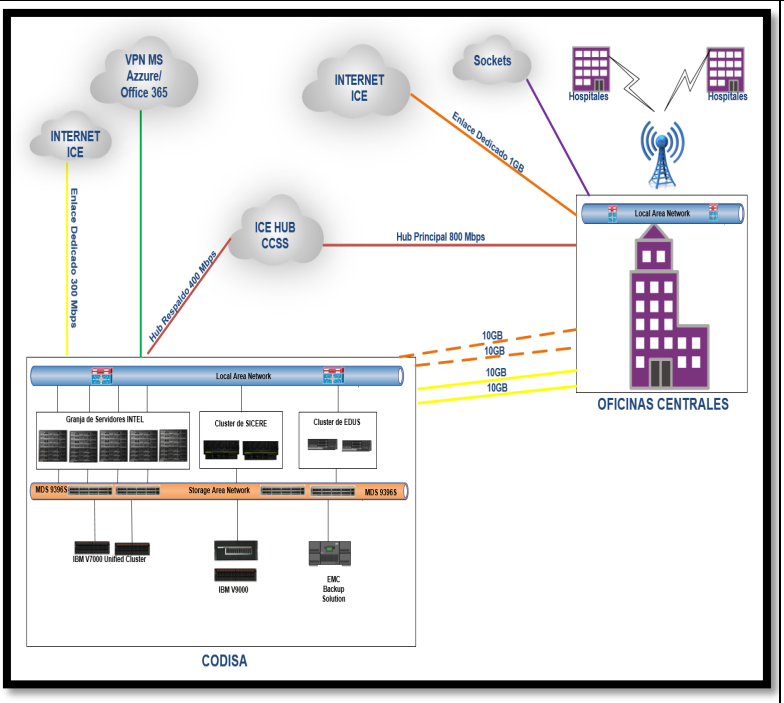
Nº	***Descripción del Cartel***	***Cumple***		***Descripción del oferente***
		Sí	***No***	
	Se enlistan las actividades mínimas de la primera fase del proceso de instalación que involucra la habilitación del ambiente de conmutación del DC del CPA			
11.18.	Como actividad inicial se requiere la instalación y habilitación de los componentes de conmutación del segmento de Datacenter en el CPA			
11.19.	El adjudicatario debe realizar las actividades de integración con el ambiente de gestión existente en el CPP de tal forma que ambos nodos estén operando como un solo clúster a nivel de la estructura de gestión y administración.			
11.20.	El adjudicatario debe realizar las actividades de configuración y de conexión necesarias para habilitar la comunicación entre el ambiente de conmutación de Datacenter en el CPP y el nuevo segmento a habilitar en el CPA.			
11.21.	El adjudicatario debe integrar, siguiendo el plan de implementación del fabricante, la plataforma de conmutación existente al ambiente de procesamiento de Datacenter existente habilitando las características de capa 2 y capa 3 necesarias para el inicio del proceso de migración de las plataformas de procesamiento actuales y de todos los elementos a implementar posteriormente.			
11.22.	El adjudicatario desarrollará de forma programada y no disruptiva el proceso de migración de los elementos de procesamiento en el CPA al nuevo segmento de conmutación de Datacenter disponible.			
11.23.	El adjudicatario desarrollará la habilitación de las características de monitoreo y administración de la plataforma central de acuerdo con las condiciones técnicas establecidas en este documento.			
11.24.	El adjudicatario desarrollará todas las actividades de evaluación de la disponibilidad de la solución instalada para determinar su estado operativo, así como las condiciones técnicas relacionadas.			
11.25.	**Procesos de Instalación – Ambiente de Borde del CPP** Una vez finalizada la habilitación del módulo de conmutación el oferente desarrollará las actividades de habilitación del segmento de borde del CPP que son descritas a continuación:			
11.26.	El adjudicatario habilitará la topología lógica y física requerida para el CPP incluyendo el segmento de agregación de borde a partir de la plataforma de conmutación de CORE existente.			
11.27.	El adjudicatario debe habilita la estructura topológica de 3 capas detallada en este documento.			
11.28.	En la capa de interconexión de enlaces WAN, el adjudicatario debe desarrollar la instalación y configuración de los dispositivos de conmutación y enrutamiento necesarios de acuerdo con el modelo topológico requerido**.** La configuración debe realizarse siguiendo el diseño y plan de implementación que debe ser creado por el fabricante y el adjudicatario.			

Nº	***Descripción del Cartel***	***Cumple***		***Descripción del oferente***
		Sí	***No***	
11.29.	En la capa de interconexión de enlaces WAN, el adjudicatario debe incorporar y habilitar los elementos de seguridad y optimización de tráfico necesario y establecido por la CCSS como requerimiento técnico.			
11.30.	En la capa de interconexión de internet, el adjudicatario habilitará la estructura física y lógica necesaria para la recepción, enrutamiento, control de acceso e inspección de enlaces permitiendo la incorporación de los elementos de seguridad definidos para tal fin. De igual manera, deben habilitarse los medios de interconexión físicos y lógicos para la habilitación de ambientes de DMZ necesarios.			
11.31.	En base a esquemas equivalentes, el adjudicatario habilitará los dispositivos de comunicaciones necesarios para el manejo y recepción de las conexiones de acceso remoto o de conexiones con terceros de acuerdo con los criterios establecidos en este pliego.			
11.32.	Una vez que la infraestructura de comunicaciones de borde esté habilitada en el CPA, el oferente debe ejecutar las pruebas de disponibilidad para determinar las características de continuidad operativa de la solución.			
11.33.	El adjudicatario, desarrollará el proceso de habilitación de servicios de borde de forma productiva en el CPP de tal manera que pueda liberarse la infraestructura de borde existente en Oficinas Centrales. El adjudicatario debe asegurar que todos los servicios de borde están disponibles y habilitados en el CPP.			
11.34.	Las características técnicas específicas relacionadas al servicio serán provistas al oferente una vez que este sea adjudicado, y se inicie el proceso de levantamiento de información.			
11.35.	**Procesos de Instalación – Ambiente de Borde del CPP** Luego de finalizado el proceso de habilitación del segmento de borde el adjudicatario debe iniciar el proceso de habilitación del mismo modelo topológico en el CPA:			
11.36.	El adjudicatario habilitará la topología lógica y física requerida para el CPA incluyendo el segmento de agregación de borde a partir de la plataforma de conmutación de CORE existente.			
11.37.	Se debe realizar la reestructuración de la topología en función de los requerimientos técnicos establecidos en el documento.			
11.38.	El adjudicatario debe habilita la estructura topológica de 3 capas detallada en el pliego.			
11.39.	En la capa de interconexión de enlaces WAN, el adjudicatario debe desarrollar la instalación y configuración de los dispositivos de conmutación y enrutamiento necesarios de acuerdo con el modelo topológico requerido.			
11.40.	En la capa de interconexión de enlaces WAN, el adjudicatario debe incorporar y habilitar los elementos de seguridad y optimización de tráficos necesarios y establecidos por la CCSS como requerimiento técnico.			
11.41.	En la capa de interconexión de internet, el adjudicatario habilitará la estructura física y lógica necesaria para la recepción, enrutamiento, control de acceso e inspección de enlaces permitiendo la			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	incorporación de los elementos de seguridad definidos para tal fin. De igual manera, deben habilitarse los medios de interconexión físicos y lógicos para la habilitación de ambientes de DMZ necesarios.			
11.42.	En base a esquemas equivalentes, el adjudicatario habilitará los dispositivos de comunicaciones necesarios para el manejo y recepción de las conexiones de acceso remoto o de conexiones con terceros de acuerdo con los criterios establecidos en este pliego.			
12.	**Servicios Avanzados de Redes y Comunicaciones**			
12.1.	Con el objetivo de asistir a la CCSS en la operación, adopción y el mejoramiento continuo de la implementación con base a las necesidades de negocio de la CCSS es necesario que el oferente considere como parte de su oferta económica servicios de optimización de la arquitectura ACI, que al mismo tiempo brinde mejoras y recomendaciones futuras a considerar.			
12.2.	Estos servicios deben ser ejecutados directamente por el fabricante de los equipos, durante un periodo de 1 año por lo que el costo a considerar debe ser basado en ese tiempo. Esto a partir de la implementación de la solución.			
12.3.	**Auditoria o revisión de la salud del ambiente**			
12.4.	Consultoría para ayudar a garantizar que las políticas fundamentales para utilizar su solución Cisco ACI se implementen de manera eficiente.			
12.5.	Recopilación de información del Controlador de infraestructura de políticas de aplicaciones (APIC), que incluye puntuaciones de fallas y estado de salud, bitácoras, recursos de hardware y software y datos del sistema.			
12.6.	Revisión de las excepciones y recursos recopilados, así como las relaciones con objetos gestionados, triggers e impactos a la funcionalidad			
12.7.	**Análisis de puntaje de salud según mejores prácticas y aportes de puntajes de salud de APIC, así como otros puntos de datos.**			
12.8.	Asesoramiento sobre cómo optimizar las definiciones de políticas para que su solución funcione según lo previsto.			
12.9.	BENEFICIOS ➢ Operar y optimizar su solución ACI utilizando datos reales y la experiencia de Cisco ACI Identificar y resolver problemas de configuración de ACI ➢ Mejore la alineación entre sus políticas de aplicaciones y las mejores prácticas de Cisco Priorizar proactivamente la utilización de los recursos y apoyar el crecimiento futuro			
12.10.	Estrategia y Análisis			
12.11.	Revisión de la infraestructura existente y proveer recomendaciones para expandir o evolucionar la infraestructura de ACI.			

Nº	*Descripción del Cartel*	*Cumple*		*Descrip-ción del oferente*
		Sí	*No*	
12.12.	Evaluación sus futuros requisitos de red de centros de datos para su crecimiento en la arquitectura ACI para habilitar un modelo de servicios de red basado en políticas			
12.13.	Analizar el cálculo, el almacenamiento, la aplicación, el inventario de servicios compartidos, los datos de rendimiento y los datos del sistema operativo para determinar los próximos pasos para la migración a una infraestructura de Cisco ACI.			
12.14.	Soporte de cambios en la configuración			
12.15.	Trabajo en durante la ventana de cambio y/o mantenimiento implementando una configuración planificada o cambios de software.			
12.16.	Recopilación de múltiples fuentes de información y proporcionar recomendaciones para mejorar su configuración y los procesos de planificación, implementación y soporte de cambios de software.			
12.17.	BENEFICIOS ➢ Reducir el riesgo de re-trabajo mediante la identificación proactiva de las áreas que necesitan mejoras ➢ Evitar costos y retrasos cuando los cambios deben ser modificados ➢ Obtenga la guía y las mejores prácticas de Cisco.			
13.	**Subítem 1.3 Servicios de Implementación para Replicación y Recuperación de Desastres para servicios TIC on-Premise.**			
13.1.	La CCSS se encuentra en un proceso a un mediano plazo para la migración de algunos servicios complementarios a la Nube. Sin embargo, existen una serie de servicios altamente críticos que la CCSS desea mantener on-premise en ambos sitios CPP y CPA.			
13.2.	**Aspectos Generales del Diseño** • Se debe considerar que el CPP será el Data Center Principal actual de la CCSS (CODISA) en la cual se ejecutará la operación institucional del ambiente de producción. • Es responsabilidad absoluta del oferente realizar el adecuado dimensionamiento de las labores e integración de la plataforma tecnológica de la CCSS para brindar la prestación de los servicios solicitados en las presentes especificaciones. • Durante el mantenimiento preventivo y/o correctivo, el servicio productivo brindado no debe ser interrumpido. • El oferente debe considerar todos los aspectos necesarios para establecer la conectividad necesaria a nivel de LAN y SAN de manera que se garantice la continuidad de los servicios.			

Nº	***Descripción del Cartel***	***Cumple***		***Descripción del oferente***
		Sí	***No***	
	En el Subítem 1.2 del presente cartel, se desarrolla todo el tema de conectividad entre CPP y CPA. • Conforme a las buenas prácticas de implementación de Oracle, para los ambientes en plataforma RISC (SICERE, MISE, MDI, SIGES, RHRH) y x86 (EDUS), se debe garantizar la compatibilidad del servicio. La CCSS ya cuenta con el hardware del CPP y CPA (hardware homogéneo en ambos sitios). • Entiéndase como homogéneo, de la misma marca y mismo sistema operativo, pero podría ser diferente modelo y capacidad a nivel de almacenamiento, procesamiento y memoria.			
13.3.	**Servicios Críticos** En la actualidad la CCSS tiene varios servicios que son muy críticos y que se desea mantener on-premise. Hay dos plataformas principales: • Equipos con procesadores de tipo RISC (Power8 570c del fabricante IBM). • Equipos con procesadores de tipo x86 (servidores tipo Blade Lenovo x240 M5). En ambas plataformas residen Bases de Datos y Aplicativos de sistemas de información Core para el negocio, como se muestra en la siguiente imagen:			

Nº	Descripción del Cartel	Cumple		Descrip-ción del oferente
		Sí	No	
				
13.4.	A continuación se da una descripción de la composición de estos sistemas que se debe considerar a nivel local:			

<table>
<tr><th rowspan="2">Nº</th><th rowspan="2">Descripción del Cartel</th><th colspan="2">Cumple</th><th rowspan="2">Descrip-ción del oferente</th></tr>
<tr><th>Sí</th><th>No</th></tr>
<tr><td></td><td>
<table>
<tr><th>Sistema</th><th>Estructura</th></tr>
<tr><td>SICERE</td><td>Sistema Centralizado de Recaudación actualmente se encuentra instalado en una partición de los dos equipos tecnología RISC en Clúster con el producto Real Application Clúster (RAC) bajo el sistema operativo AIX versión 7.2.</td></tr>
<tr><td>MISE</td><td>Modulo Integrado de Seguridad actualmente se encuentra instalado en una partición de los dos equipos tecnología RISC en Clúster con el producto Real Application Clúster (RAC) bajo el sistema operativo AIX versión 7.2.</td></tr>
<tr><td>MDI</td><td>Modelado de Datos Institucional actualmente se encuentra instalado en una partición de los dos equipos tecnología RISC en Clúster con el producto Real Application Clúster (RAC) bajo el sistema operativo AIX versión 7.2.</td></tr>
<tr><td>SIGES</td><td>Sistema de Gestión de Suministros actualmente se encuentra instalado en una partición de los dos equipos tecnología RISC en Clúster con el producto Real Application Clúster (RAC) bajo el sistema operativo AIX versión 7.2.</td></tr>
<tr><td>RRHH</td><td>Portal de Recursos Humanos actualmente se encuentra instalado en una partición de los dos equipos tecnología RISC en Clúster con el producto Real Application Clúster (RAC) bajo el sistema operativo AIX versión 7.2.</td></tr>
<tr><td>EDUS</td><td>Expediente Digital Único de Salud actualmente instalado en dos equipos x86 en Clúster con el producto Real Application Clúster (RAC), bajo el sistema operativo Oracle Linux versión 7.</td></tr>
</table>
</td><td></td><td></td><td></td></tr>
<tr><td>13.5.</td><td>El licenciamiento tanto de Base de Datos, Aplicaciones, Oracle Data Guard Sistema Operativo, Hypervisor va a ser provistos por la CCSS.</td><td></td><td></td><td></td></tr>
<tr><td>13.6.</td><td>Todos los servicios van a estar centralizados en el subsistema de almacenamiento IBM modelo V9000, la CCSS cuenta con un mismo subsistema en el sitio alterno.</td><td></td><td></td><td></td></tr>
<tr><td>13.7.</td><td>La replicación se va a habilitar por medio del software Oracle Data Guard con el objetivo de mantener la consistencia e integridad de los datos.</td><td></td><td></td><td></td></tr>
</table>

Nº	***Descripción del Cartel***	***Cumple***		***Descripción del oferente***
		Sí	***No***	
13.8.	La modalidad por implementar debe ser por medio de un Take Over no Hostil, el cual es un proceso de toma del control por parte de otra instancia de forma controlada			
13.9.	El sitio principal y el sitio alterno estarán interconectados entre sí a través de una LAN extendida.			
13.10.	Para implementar el esquema de replicación de datos se usará un canal dedicado entre el sitio principal y el respectivo sitio alterno.			
13.11.	Los ambientes de contingencia deben estar integrados entre sí en un esquema de resiliencia geográfica, el primero en modo Activo / Pasivo en la capa de presentación y aplicaciones, soportando la ejecución de transacciones y procesos en lote de la Solución, y el segundo en modo Activo / Pasivo, para la capa de bases de datos. El adjudicatario puede proponer mejoras al esquema planteado, lo cual debe ser analizado en la fase de diseño de la Arquitectura y queda sujeto a la correspondiente aceptación y aprobación.			
13.12.	Los ambientes de contingencia deben ser implementados bajo la misma arquitectura: clúster, versiones del software, configuraciones técnicas, nivel de parchado, siendo un ambiente completamente homologo al ambiente de producción.			
13.13.	Los ambientes de contingencia deben permitir la incorporación de una instancia o sitio a solicitud del operador y en forma automática cuando se recupere de una falla o por labores de mantenimiento.			
13.14.	Los ambientes en el sitio principal deben operar en modalidad activa. La instancia en el sitio alterno debe operar en modalidad pasiva.			
13.15.	Se debe considerar seguir las siguientes reglas de Take Over			
13.15.1.	Una falla en la instancia del sitio principal implica que la instancia del sitio alterno debe asumir en forma automática la totalidad del volumen transaccional y los procesos en lote de los Sistemas			
13.15.2.	Una falla en la instancia del sitio principal implica que la instancia del sitio alterno debe pasar en forma automática el modo de operación de pasivo a activo			
13.15.3.	Los ambientes deben permitir iniciar el proceso de takeover no hostil. Se deben invertir los roles de los sitios de Alterno a Principal y viceversa. Esto implica que el oferente debe garantizar que en caso de resultar adjudicatario la replicación de datos será sincrónica y en tiempo real en cualquiera de los dos sentidos			
13.15.4.	La configuración de la replicación de los ambientes productivos y de contingencia debe ser síncrona, si afectar la operatividad del sitio productivo primario			
13.15.5.	El oferente debe realizar instalación y configuración de los componentes de hardware y software ofertados para realizar la replicación de los sistemas (tanto para la capa de aplicaciones y de base de datos) que se consideren necesarios			
13.15.6.	Homologación de los parámetros de configuración de todos los componentes Oracle a habilitar en el sitio de contingencia			

Nº	***Descripción del Cartel***	***Cumple***		***Descripción del oferente***
		Sí	***No***	
13.15.7.	La configuración de los componentes de los sistemas a replicar debe contar con reportería y herramientas de monitoreo que permitan validar el estado de la replicación y sincronización y el adjudicatario debe configurar los mismos			
13.15.8.	La solución de replicación de base de datos Debe notificar mediante alertas cuando ocurra un desfase o GAP en la sincronización, cuando esté detenida por completo			
13.15.9.	Para cada componente Oracle que se va a replicar en el sitio de contingencia el oferente debe describir la solución o producto a utilizar, con justificación de ventajas y beneficios			
13.16.	El adjudicatario debe proveer como parte de su oferta un levantamiento de requisitos y revisión general de los ambientes a utilizar para la configuración.			
13.17.	Elaboración de actividades detalladas y cronograma final con base a la disponibilidad de la CCSS.			
13.18.	Adecuación de requisitos de instalación a nivel de sistema operativo (sí aplica)			
13.19.	Descarga de medios e instaladores específicos acorde a la versión actual de los productos.			
13.20.	Instalación de las bases de datos definidas anteriormente			
13.21.	Homologación del nivel parches (one-off, psu, cpu, etc) entre los ambientes principal y de contingencia.			
13.22.	Configuración de parámetros de inicialización.			
13.23.	Configuración para replicación de las bases datos productivas anteriormente definidas			
13.24.	Pruebas unitarias de la configuración.			
13.25.	Documentación del proceso, levantamiento de bitácora.			
13.26.	**Enlaces**			
13.27.	El acceso a los aplicativos informáticos que brinda la CCSS (Salud y Financieras) se brinda a los usuarios a través de las siguientes opciones: 1. Conexión WAN, enlaces a través de la red VPN del ICE para el acceso de usuarios internos. Este tipo de enlaces se encuentran establecidos en un esquema de comunicación Hub and Spoke, donde el modelo de servicio que utiliza el oferente de servicios (I.C.E.) es por medio de VPNs (Virtual Private Network o Red Privada Virtual), esta tecnología permite realizar la comunicación entre redes de forma segura a través de la red pública o Internet. Además las VPNs permiten que las computadoras de un sitio (Hospital, Clínica, Ebais, Direcciones Regionales o Sucursales) envíen y reciban datos sobre la red pública del I.C.E. como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos. Es importante mencionar que bajo el modelo de servicio utilizado, el tráfico de red de cada sitio no se mezcla con ningún otro perteneciente a otros sitios y clientes.			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	La CCSS cuenta con un enlace redundante Hub que llega al Data Center en Tibás, el cual entra en funcionamiento cuando el enlace principal de Oficinas Centrales falla. 2. Conexión WAN, enlaces inalámbricos propios de la CCSS para el acceso de usuarios internos. Este tipo de enlaces son privados propios de la CCSS los cuales se establecen a través de antenas y señales de radio inalámbricas las cuales permiten establecer redes privadas y seguras de un sitio (Hospital, Clínica, Ebais, Direcciones Regionales o Sucursales), hasta Oficinas Centrales en Avenida Segunda. 3. Cooperativas, enlaces dedicados hacia las diferentes cooperativas (COOPESIBA, COOPESALUD, UNIBE, ASEMECO, COOPESANA, COOPESAIN) que brindan servicios de salud en distintos sectores del territorio nacional y requieren acceso a las aplicaciones médicas institucionales. 4. Entidades Externas, enlaces dedicados hacia entes financiaros que colaboran con la CCSS en la recaudación de cuotas obrero patronal. 5. Internet, para el acceso de usuarios externos a la aplicación EDUS Citas Web y las distintas aplicaciones financieras que son utilizadas por asegurados y patronos. La CCSS cuenta con un enlace redundante de Internet que llega al Data Center en Tibás, el cual entra en funcionamiento cuando el enlace principal de Oficinas Centrales falla. 6. Call Center EDUS, es el único acceso que ingresa en forma directa al Data Center, consiste en enlaces dedicados redundantes que instaló la empresa que posee el contrato de servicio de Call Center para acceder a los aplicativos EDUS y brindar el servicio de citas médicas. Todos los usuarios indicados en los puntos del 1 al 4 ingresan a Oficinas Centrales de la Caja y son verificados por los dispositivos de seguridad que posee la institución (Sistema de Muro de Fuego o Firewall y Sistema Prevención de Intrusos o IPS). Estos sistemas de seguridad se encuentran en clúster para garantizar la continuidad de los servicios. La comunicación desde Oficinas Centrales hacia el Data Center donde se encuentran todos los sistemas informáticos instituciones se realiza a través de 2 enlaces dedicados de fibra gris brindados por el ICE, los cuales viajan por rutas diferentes desde San José hasta Tibás para garantizar la continuidad del servicio. En el Data Center las comunicaciones son recibidas nuevamente por sistemas de seguridad en clúster (Sistema de Muro de Fuego o Firewall, Sistema Prevención de Intrusos o IPS, Sistema de Ba-			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	lanceo de aplicaciones y/o servicios). Los cuales de nuevo verifican y validan la comunicación antes de llegar a los servidores que brindan el servicio informático institucional (EDUS, SFA, Correo, Navegación, entre otros). En el Data Center, los distintos servicios informáticos se encuentran separados por medio de contextos virtuales definidos en los equipos de comunicaciones instalados en dicho centro: Conmutador, Firewall y Balanceador. Es importante que el oferente considere que en el CPA no va existir balanceadores físicos, el balanceo va ser mediante software, la CCSS proveerá todo lo necesario a nivel de recursos y licenciamiento correspondiente para brindar la funcionalidad al adjudicatario.			
13.28.	El oferente se debe de encargar como parte de su gestión de coordinar con el personal interno de la CCSS y del oferente ICE para realizar el movimiento del Hub principal de Oficinas Centrales al Centro de Procesamiento Principal (CODISA), así mismo para enlaces que permiten el acceso a Internet de la institución.			
13.29.	Este proceso debe ejecutarse de manera no disruptiva debido a la operación continua de la institución			
13.30.	Se deben coordinar con los distintos involucrados el momento idóneo para realizar el intercambio para minimizar un posible impacto			
13.31.	El oferente debe considerar un plan de emergencia con el oferente del servicio (ICE) dentro del plan en caso de una eventual anomalía durante el intercambio			
13.32.	**Gestión de Proveedores**			
13.32.1.	El oferente debe considerar que el Administrador de proyectos ejecute funciones de Gestión de Oferentes y debe cumplir con las siguientes tareas			
13.32.2.	Controlar las adquisiciones			
13.32.3.	Gestionar el trabajo de todos los partners involucrados para que se realicen las labores necesarias de acuerdo a su participación dentro del proyecto			
13.32.4.	Controlar la calidad, verificar e inspeccionar que los partners cumplan de conformidad con los objetivos de las labores asignadas de acuerdo a su participación			
13.32.5.	Realizar el control integrado de cambios, asegurar que los cambios sean evaluados de acuerdo a las necesidades y los objetivos del proyecto.			
13.32.6.	Control de los riesgos, realizar este control de forma preventiva para mitigar los impactos del proyecto			
13.32.7.	Comunicación, velar por la comunicación fluida entre partners y la CCSS, con el fin de asegurar que las distintas partes funciones alineadas según las necesidades del proyecto			
13.32.8.	Consolidar toda la documentación técnica de todos los partners para generar un repositorio único de la solución			
14.	**Subítem 1.4 Transferencia de conocimientos**			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	El oferente debe considerar los servicios de transferencia de conocimiento, capacitación o adopción según se solicite de acuerdo a las tecnologías de equipos o servicios incluidos en el presente pliego. El objetivo primario de este servicio es garantizar que el conocimiento técnico de la nueva operación sea transferido a los ingenieros, consultores y operadores de la CCSS y la solución sea administrada con independencia por el personal técnico.			
14.1.	**Transferencia de conocimiento del servicio de migración a nivel de comunicaciones** Dichos servicios de transferencia de conocimiento deben responder a las arquitecturas, tecnologías, topologías físicas y lógicas, prácticas y esquemas a implementar en los diseños propuestos en la oferta. Es decir, el contenido de la transferencia de conocimiento debe ser personalizado. A continuación, se describe el mínimo de actividades que el oferente se compromete a completar dentro del apartado de servicios de transferencia de conocimiento.			
14.2.	El adjudicatario diseñará un entrenamiento personalizado en el que se cubran los contenidos técnicos relacionados a las tecnologías implementadas como parte de la solución de comunicaciones descrita en el pliego.			
14.3.	El proceso de entrenamiento estará basado en un esquema práctico en el que los asistentes puedan tener acceso a desarrollar laboratorios y prácticas en un ambiente dispuesto para la ejecución estas actividades.			
14.4.	El proceso de entrenamiento debe desarrollarse en un periodo de 2 semanas calendario con un contenido efectivo equivalente a 40 horas, considerando un horario de medio día.			
14.5.	Se requiere que el entrenamiento se ejecute previo al inicio del proceso de instalación de tal forma que los ingenieros de la CCSS involucrados en el proceso de desarrollo del proyecto cuenten con los conocimientos básicos de la tecnología para acompañar las actividades de integración desarrolladas por el adjudicatario.			
14.6.	El entrenamiento requerido será impartido para 20 participantes. Se deben proveer todos los materiales y accesos a laboratorios para cada uno de los asistentes de tal forma que puedan ejecutar las actividades de forma individual.			
14.7.	Es responsabilidad del oferente, una vez adjudicado, presentar un listado y contenido de los tópicos inherentes a las trasferencias de conocimiento y entrenamientos a realizar.			
14.8.	Es responsabilidad del oferente, una vez adjudicado, facilitar material didáctico para las sesiones de transferencia de conocimiento en idioma español o en sus efectos inglés técnico. Esta información se Debe entregar en un formato electrónico por ejemplo CD, DVD o USB; estos materiales deben contener la misma			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
	información que se da en las sesiones de entrenamiento, sin obviar ningún tema, se deben entregar también las presentaciones en PowerPoint que se utilizan para impartir la clase.			
14.9.	Es responsabilidad del oferente, una vez adjudicado, aportar todos los recursos y la logística necesaria para dar una correcta y satisfactoria capacitación, el aula para recibir la capacitación debe ser cómoda, no estrecha, la alimentación durante la capacitación, esto incluye la logística acerca del lugar, equipo multimedia, computadoras y todo lo necesario para los escenarios de práctica y pruebas incluidos en el curso. Baños para hombres y mujeres, parqueo para participantes coordinado previamente para evitar inconvenientes o cambios a la hora de ingresar, los encargados de vigilancia del parqueo Deben estar enterados del ingreso y debe contarse con el parqueo fijo para los días de la capacitación.			
14.10.	Es responsabilidad del oferente, una vez adjudicado, asumir los gastos de alimentación, hospedaje y transporte de los instructores requeridos para cada capacitación. Además, se encargará de la impresión de los materiales, así como de la emisión de los certificados. Libros Certificados por el Fabricante.			
14.11.	Este entrenamiento incluirá independiente del proceso de transferencia de conocimientos que se realizará una vez finalizado el proceso de instalación, en adición se ejecutará una revisión y discusión general del proyecto.			
14.12.	El proceso de transferencia de conocimientos debe ser preparado para desarrollarse en un espacio de 16 horas distribuidas en función de la disponibilidad del personal técnico de la CCSS.			
14.13.	**Transferencia de conocimiento del producto Oracle Data Guard.** Se debe llevar a cabo una formación de Oracle Database 12c: Data Guard Administración para 10 funcionarios donde se deban realizar laboratorios virtuales, así como la topología ultimada en la implementación de la CCSS, todo esto lo debe proveer el oferente. Estas inducciones deben incluir el lugar, refrigerios así como la alimentación de dichos funcionarios por la duración del curso. La duración del curso será de 40 horas aproximadamente en 2 semanas, esta transferencia debe ser impartida por personal que haya participado durante la implementación de la solución y debe incluir su aplicación de como quedo configurado el ambiente de la CCSS.			
14.13.1.	**Introducción a Oracle Data Guard**			
14.13.2.	Oracle Data Guard: Arquitectura (descripción general)			
14.13.3.	Tipos de servicios de protección de datos			
14.13.4.	Transiciones de roles: conmutación y conmutación por error			
14.13.5.	¿Qué es Oracle Data Guard?			
14.13.6.	Elegir una interfaz para administrar una configuración de Data Guard			
14.13.7.	Tipos de bases de datos en espera			
14.13.8.	Procesos de base de datos primarios			
14.13.9.	Oracle Data Guard Broker Framework			

Nº	*Descripción del Cartel*	*Cumple*		*Descripción del oferente*
		Sí	*No*	
14.13.10.	**Redes para Oracle Data Guard**			
14.13.11.	Configuración de Listener.ora			
14.13.12.	Estática vs registro dinámico			
14.13.13.	Entradas estáticas para operaciones de corredores			
14.13.14.	Configuración de Tnsnames.ora			
14.13.15.	Entradas estáticas para duplicación de bases de datos y mantenimiento de SQL			
14.13.16.	Ajuste de la configuración de red de Oracle			
14.13.17.	Resumen de redes			
14.13.18.	**Creación de una base de datos en espera física mediante el uso de los comandos SQL y RMAN**			
14.13.19.	Pasos para crear una base de datos de espera física			
14.13.20.	Configuración de los registros de rehacer en espera			
14.13.21.	Visualización de información de registro de rehacer en espera			
14.13.22.	Creación de registros de rehacer en espera			
14.13.23.	Modo de registro de fuerza			
14.13.24.	Uso de SQL para crear registros de rehacer en espera			
14.13.25.	Configuración de los parámetros de inicialización en la base de datos principal para controlar el transporte de rehacer			
14.13.26.	Preparación de la base de datos primaria			
14.13.27.	**Oracle Data Guard Broker: Descripción general**			
14.13.28.	Data Guard Broker: Componentes			
14.13.29.	Data Guard Broker: Configuraciones			
14.13.30.	Monitor de Guardia de Datos: Proceso DMON			
14.13.31.	Beneficios de usar el Data Guard Broker			
14.13.32.	Oracle Data Guard Broker: características			
14.13.33.	Comparación de la gestión de la configuración con y sin el agente de Data Guard			
14.13.34.	Data Guard Broker: modelo de gestión			
14.13.35.	Data Guard Broker: Arquitectura			
14.13.36.	**Creación de una configuración de Data Guard Broker**			
14.13.37.	Data Guard Broker: Archivos de registro			
14.13.38.	Creando una Configuración de Broker			
14.13.39.	Data Guard Monitor: Archivo de configuración			
14.13.40.	Data Guard Broker y el SPFILE			
14.13.41.	Adición de una base de datos en espera a la configuración			
14.13.42.	Data Guard Broker: Requisitos			
14.13.43.	Definición de la configuración del agente y el perfil de la base de datos principal			
14.13.44.	Habilitando la Configuración			
14.13.45.	**Creación de una base de datos en espera física mediante Enterprise Manager Cloud Control**			
14.13.46.	Creación de la base de datos en espera: Progreso			
14.13.47.	Creando una Configuración			
14.13.48.	Adición de una base de datos en espera a una configuración existente			

Nº	***Descripción del Cartel***	***Cumple***		***Descripción del oferente***
		Sí	***No***	
14.13.49.	Creación de la base de datos en espera: Procesamiento			
14.13.50.	Uso del Asistente para agregar bases de datos en espera			
14.13.51.	Uso de Oracle Enterprise Manager para crear una configuración de intermediario			
14.13.52.	Creando una Nueva Configuración			
14.13.53.	Verificación de una configuración de Data Guard			
14.13.54.	**Creación de una base de datos de espera lógica**			
14.13.55.	Beneficios de implementar una base de datos de espera lógica			
14.13.56.	Comprobación de tablas con tipos de datos no compatibles			
14.13.57.	Objetos no soportados			
14.13.58.	Preparación para crear una base de datos de espera lógica			
14.13.59.	Tipos de datos no compatibles			
14.13.60.	Base de datos lógica en espera: Arquitectura SQL Apply			
14.13.61.	Proceso de Aplicar SQL: Arquitectura			
14.13.62.	Comprobación de tablas no compatibles			
14.13.63.	**Creación y gestión de una base de datos de instantánea en espera**			
14.13.64.	Snapshot Standby Database: Arquitectura			
14.13.65.	Conversión de una base de datos en espera física a una base de datos en espera instantánea			
14.13.66.	Activación de una base de datos en espera de instantáneas: problemas y precauciones			
14.13.67.	Conversión de una base de datos de instantánea en espera a una base de datos de espera física			
14.13.68.	Visualización de información de la base de datos de instantáneas en espera			
14.13.69.	Base de datos en espera de instantáneas: Restricciones de destino			
14.13.70.	Uso de DGMGRL para ver información de la base de datos de instantánea en espera			
14.13.71.	Bases de datos de espera de instantáneas: Descripción general			
14.13.72.	**Usando Oracle Active Data Guard**			
14.13.73.	Monitoreo Aplicar Lag: V $ DATAGUARD_STATS			
14.13.74.	Configuración de Zero Lag entre las bases de datos principal y en espera			
14.13.75.	Uso de consulta en tiempo real			
14.13.76.	Oracle Active Data Guard			
14.13.77.	Configuración de un nivel de servicio predeterminado para la moneda de las consultas en espera			
14.13.78.	Comprobando el Modo Abierto del Standby			
14.13.79.	Entender la demora en una configuración de Active Data Guard			
14.13.80.	Monitoreo Aplicar retraso: V $ STANDBY_EVENT_HISTOGRAM			
14.13.81.	**Configuración de los modos de protección de datos**			
14.13.82.	Modo de disponibilidad máxima			
14.13.83.	Modo de máximo rendimiento			
14.13.84.	Modo de máxima protección			
14.13.85.	Configuración del modo de protección de datos			

Nº	*Descripción del Cartel*	*Cumple*		*Descrip-ción del oferente*
		Sí	*No*	
14.13.86.	Modos de protección de datos y modos de transporte de rehacer			
14.13.87.	Comparación de los modos de protección de datos			
14.13.88.	Configuración del modo de protección de datos utilizando DGMGRL			
14.13.89.	**Realizar transiciones de roles**			
14.13.90.	Consideraciones al realizar un cambio a una base de datos de espera lógica			
14.13.91.	Situaciones que impiden una conmutación			
14.13.92.	Realización de una conmutación utilizando Enterprise Manager			
14.13.93.	Preparación para un cambio			
14.13.94.	Transiciones de roles: conmutación y conmutación por error			
14.13.95.	Realización de una conmutación utilizando DGMGRL			
14.13.96.	Servicios de gestión de roles			
14.13.97.	**Uso de la base de datos Flashback en una configuración de Data Guard**			
14.13.98.	Configuración de la base de datos Flashback mediante Enterprise Manager			
14.13.99.	Visión general de la base de datos Flashback			
14.13.100	Uso de la base de datos Flashback en una configuración de Data Guard			
14.13.101	Flashback a través de las transiciones de roles de base de datos en espera			
14.13.102	Usando la base de datos Flashback después de RESETLOGS			
14.13.103	Configuración de la base de datos Flashback			
14.13.104	Usando Flashback Database y Real-Time Apply			
14.13.105	Uso de la base de datos Flashback en lugar de aplicar el retraso			
14.13.106	**Habilitar la conmutación por error de inicio rápido**			
14.13.107	Configuración de la conmutación por error de inicio rápido			
14.13.108	Conmutación por error de inicio rápido: descripción general			
14.13.109	Requisitos previos para la conmutación por error de inicio rápido			
14.13.110	Instalación del software Observer			
14.13.111	Configuración de la base de datos primaria para cerrar automáti-camente			
14.13.112	¿Cuándo se produce la conmutación por error de inicio rápido?			
14.13.113	Configuración del límite de tiempo de espera			
14.13.114	Restablecimiento automático después de la conmutación por error de inicio rápido			
14.13.115	**Gestionando la conectividad del cliente**			
14.13.116	Creación de servicios para las bases de datos de configuración de Data Guard			
14.13.117	Entender la conectividad del cliente: usar un servicio de base de datos			
14.13.118	Adición de bases de datos en espera a la configuración de reinicio de Oracle			
14.13.119	Servicios de gestión			
14.13.120	Entender la conectividad del cliente: usar nombres locales			
14.13.121	Evitar que los clientes se conecten a la base de datos incorrecta			
14.13.122	Entendiendo la conectividad del cliente en una configuración de			

Nº	Descripción del Cartel	Cumple		Descripción del oferente
		Sí	No	
	Data Guard			
14.13.123	Configuración de servicios basados en roles			
14.13.124	**Consideraciones de respaldo y recuperación en una configuración de Oracle Data Guard**			
14.13.125	Configuración de ajustes de configuración persistentes			
14.13.126	Creación del catálogo de recuperación			
14.13.127	Descarga de copias de seguridad a un modo de espera físico			
14.13.128	Registro de una base de datos en el catálogo de recuperación			
14.13.129	Uso de RMAN para realizar copias de seguridad y restaurar archivos en una configuración de Data Guard			
14.13.130	Restricciones y notas de uso			
14.13.131	Uso del catálogo de recuperación de RMAN en una configuración de Data Guard			
14.13.132	Copia de seguridad y recuperación de una base de datos de espera lógica			
14.13.133	**Aplicación de parches y actualización de bases de datos en una configuración de Data Guard**			
14.13.134	Actualización de la base de datos Oracle en una configuración de Data Guard con una base de datos en espera física			
14.13.135	Actualización de la base de datos Oracle en una configuración de Data Guard con una base de datos en espera lógica			
14.13.136	Actualización de una configuración de Oracle Data Guard Broker			
14.13.137	Realización de una actualización progresiva mediante DBMS_ROLLING			
14.13.138	Bases de datos de grupos finales y Master de grupos finales			
14.13.139	Principales bases de datos de grupo y líder de grupo Master			
14.13.140	Requisitos para usar DBMS_ROLLING para realizar una actualización progresiva			
14.13.141	Uso de DBMS_ROLLING para actualizar la base de datos Oracle			
14.13.142	**Monitoreo de una configuración de Data Guard Broker**			
14.13.143	Monitoreo de la configuración de Data Guard usando Enterprise Manager Cloud Control			
14.13.144	Métricas de Guardia de Datos			
14.13.145	Gestión de la métrica de Data Guard			
14.13.146	Visualización del historial de valores métricos			
14.13.147	Visualización del estado de configuración de Data Guard			
14.13.148	Monitoreando el rendimiento de la guarda de datos			
14.13.149	Visualización de los detalles del archivo de registro			
14.13.150	Administrador de métricas y alertas de Enterprise			
14.13.151	**Optimización de una configuración de Data Guard**			
14.13.152	Optimización de la transmisión Redo mediante la configuración de MaxConnections			
14.13.153	Configuración de la propiedad de base de datos MaxConnections			
14.13.154	Configuración de la propiedad de la base de datos ReopenSecs			
14.13.155	Compresión de datos Redo mediante la configuración de la propiedad RedoCompression			
14.13.156	Retrasando la aplicación de rehacer			
14.13.157	Configuración de la propiedad de base de datos NetTimeout			

Nº	***Descripción del Cartel***	***Cumple***		***Descripción del oferente***
		Sí	***No***	
14.13.158	Supervisión del rendimiento de la configuración mediante Enterprise Manager Cloud Control			
14.13.159	Optimización de servicios de transporte Redo			
14.13.160	**Resumen de Oracle Database Exadata Cloud Service**			
14.13.161	Migración al servicio en la nube de Exadata			
14.13.162	Seguridad de datos y responsabilidades de gestión			
14.13.163	Aprovisionamiento y gestión simples basados en la web			
14.13.164	Introducción a Exadata Cloud Service			
14.13.165	Configuración de servicio, conexión, arquitectura y disponibilidad			
14.13.166	Copia de seguridad y recuperación			
14.13.167	API REST			
14.13.168	Configuración de almacenamiento y detalles de gestión			