Respuesta a observaciones sobre EM No. 001-2021
Interventoría Integrada A Proyectos Estratégicos de Transformación Digital
Programa Apoyo a la Modernización de la DIAN
Contrato Préstamo BID 5148/OC-CO

Fecha preguntas:	Desde el 29 de abril hasta el 10 de mayo de 2021	Consolidado de Respuestas

No.	OBSERVACIÓN	RESPUESTA
1	El servicio de Interventoría se describe como integral, que abarcan las áreas técnicas, de integración, administrativa, financiera y jurídica. ¿Es posible presentar el servicio de Interventoría por separado (una, dos o todas)? En ese sentido entendemos que el área Técnica (en todos sus tipos), de Integración y Administrativo (entendido como de gestión y control) funcionan como un grupo enfocado en los entregable y artefactos de software a diferencia de los dos restantes que velan por presupuesto y complimiento legal y normativo. Entendemos que es una buena práctica para la ejecución de programas de este tipo separar el servicio de Interventoría en tres, esto conlleva los siguientes beneficios, entre otros: · Transparencia de los servicios durante la ejecución del programa · Independencia de equipos y foco en temas específicos · Control cruzado de equipos y servicios	Lo que se espera es que una sola firma ejerza todos los servicios de interventoría, dado que el ejercicio de todos ellos implica una visión holística de los compromisos de los contratistas de los PETD. Como respuesta a este estudio de mercado es posible presentar diferentes alternativas para organizar los equipos de trabajo y los esquemas de gestión de los mismos para la prestación de todas las áreas de interventoría solicitadas
2	Respecto a los PETD, ¿se entiende que cada proyecto contará con un Gerente de Proyecto de la Unidad Ejecutora? Adicional a esto, ¿habrá un Gerente de Programa que vele por el programa en su conjunto (todos los PETD)?	SI. Además de los cargos de gestión del proyecto que debe asignar el contratista de cada PETD, la DIAN asignará un gerente de proyecto para la gestión del mismo. El Fondo DIAN tiene una unidad de coordinación de los proyectos financiados con recursos del BID y la DIAN cuenta con un Centro de Gestión de Innovación y Proyectos que realizará las veces de PMO/TMO y trabajará en coordinación con las dependencias de gestión de procesos y calidad, gestión de tecnología y las Direcciones de Gestión involucradas con los PETD.
3	Documento “Estudio de Mercado interventoría.pdf”, Página 11: a que se refieren cuando dicen “Elaborar los conceptos técnicos, financieros, jurídicos, administrativos, operativos, de seguridad y salud en el trabajo…”	Se refiere a conceptos solicitados por la DIAN y/o el FONDO DIAN, cuando se requiera en el marco de la ejecución de las actividades de interventoría, en los ámbitos mencionados (técnicos, financieros, jurídicos, administrativos, operativos, de

		seguridad y salud en el trabajo). Igualmente, para dar respuesta a los derechos de petición, solicitudes, requerimientos de autoridades gubernamentales, organismos de control o de otras entidades competentes, relacionados con la ejecución de los PETD.
4	Página 12, punto 3.2.2. Interventoría Financiera: ¿Es correcto entender que la interventoría dará soporte al área financiera de la Unidad Ejecutora? Adicionalmente, se entiende que la Interventoría no será quien apruebe y realice pagos, ¿es correcta esta aseveración?.	Es correcto el entendimiento planteado en la solicitud, la Interventoría dará soporte a nivel financiero y no realizará los pagos correspondientes. No obstante, la revisión técnica de la interventoría a los productos si es base para la recepción de los mismos y el consecuente pago por parte del Fondo DIAN Colombia.
5	A lo largo del documento se mencionan actividades de verificar, revisar y aprobar y, realizar revisión especializada, ¿Cuál es el alcance de dichas actividades? ¿Cuál es la responsabilidad o compromiso que se espera asuma el Interventor?	El alcance y compromiso relacionado con dichas actividades se encuentra descrito en el numeral 3.3. Productos e informes, particularmente en los numerales 3.3.2. Informe de Revisión, 3.3.3. Informe de Verificación y 3.3.4. Informe de revisiones especializadas.
6	Página 18, punto 3.2.5.2.2, sub punto 2 tema b: dice “Verificar el de validación de migración de información” falta una palabra para dar sentido a la frase.	Se aclara que ese punto corresponde a "b. Verificar el **Plan** de validación de migración de información"
7	Página 28: Cuando se refieren a “Construir el plan de proyecto” se habla del plan integral de todos los PETD o es el plan del servicio de interventoría?	Corresponde al numeral 3.4.1.1. Planificación del servicio de interventoría, y se trata del Plan del Servicio de Interventoría.
8	Página 26 se indica: · Optimizar el proceso de prueba, orientado a rastrear los diferentes pasos del proceso de pruebas evaluando oportunidades de mejora (por ejemplo, en función de la proporción de defectos no detectados) y definiendo las recomendaciones correspondientes. Puede implicar la realización de pruebas para identificar la causa raíz de alguna problemática particular,	Lo que se busca es generar valor agregado del servicio de interventoría, en este caso al proceso de pruebas del software, sin perdida de la independencia frente a los contratistas del PETD; las recomendaciones de carácter técnico que surjan de esta actividad, estarán orientadas a la minimización de los riesgos y la optimización del proceso de prueba del software y serán entregadas a la Gerencia del Proyecto de la DIAN, quien gestionará con el contratista del PETD las características de su aplicación.

	· Recomendar según el caso, la aplicación de los diferentes enfoques para interactuar con el software sujeto de prueba (SSP) como pruebas de interfaz de Programación de Aplicaciones, pruebas a través de la interfaz de usuario del SSP (por interfaz gráfica o por la línea de comando), pruebas a través de un servicio. ¿Cuál es la expectativa que tiene la administración en relación a estas actividades?. La pregunta tiene su origen en que consideramos que el Interventor no debe realizar ninguna recomendación Al CONTRATISTA pues sería juez y parte, en todo caso debería solicitar al éste mejoras.	
9	Anexo 6: presupuesto: ¿En la intersección de cada Fila/Columna (por ejemplo, Administrativa-Data R) se debe consignar el porcentaje sobre el total del presupuesto o sobre el subtotal de la línea (en el ejemplo Administrativa)?	Se hace la aclaración en el Anexo 6, el cual fue ajustado para mayor claridad
10	De acuerdo con lo definido en el numeral 3.2. Alcance de la interventoría, solicitamos amablemente compartir la ruta de implementación y el plazo de ejecución de cada uno de los proyectos	Se tiene previsto que todos los proyectos se ejecuten en paralelo y se han considerado los prerrequisitos que existen entre ellos (por ejemplo, con la migración de información histórica y la disponibilidad de servicios de plataforma requeridos para la entrada en producción de las soluciones, entre otros). La fecha esperada de inicio de la ejecución de los proyectos es entre Diciembre de 2.021 y Enero de 2.022. Ver el Anexo 1. De las respuestas - Planes de Trabajo de los PETD.
11	Con relación al numeral 3.4.1.3.Gestión del repositorio documental del servicio de interventoría, se indica que se debe hacer a través de la herramienta dispuesta para ello, sin embargo en este mismo capitulo se indica como parte de las actividades “Diseñar e Implementar el repositorio Documental que incluya la Base Documental y de Conocimientos del Servicio de Interventoría”, razón por la cual agradecemos a la entidad aclarar cual es la herramienta sobre la cual se debe realizar la implementación del repositorio documental de las	La DIAN dispone de herramientas como SharePoint y Confluence para la gestión documental de los proyectos. Al inicio del contrato se acordará la herramienta a utilizar por el proveedor del servicio de interventoría. La actividad de "Diseñar e Implementar el repositorio Documental que incluya la Base Documental y de Conocimientos del Servicio de Interventoría" se debe entender como el diseño e implementación de la estructura,

	interventorías; y como se planea realizar la transferencia de conocimiento para tener las capacidades para realizar el diseño e implementación	nomenclatura, control de versiones, procedimientos y demás aspectos necesarios para el registro y consultas de la documentación del servicio de interventoría, en la herramienta que se adopte.
12	Sobre el numeral 3.4.2.3.Recursos y herramientas de soporte, agradecemos aclarar el alcance de este requerimiento, con relación a suministrar herramienta de Colaboración para la Dian (como ejemplos Slack, Microsoft Teams)	La herramienta de comunicación y colaboración se definirá en el inicio del contrato, la DIAN actualmente cuenta con Microsoft Teams. De ser esta la herramienta seleccionada, el proveedor del servicio de interventoría deberá suministrar y dar acceso a una instalación de Microsoft Teams que permita la interacción con el personal de los contratistas de cada PETD y de la DIAN a que haya lugar, en relación con los servicios de interventoría.
13	Sobre el numeral 3.4.2.3.Recursos y herramientas de soporte, entendemos que la herramienta para desarrollar las pruebas de la interventoría será utilizada por el equipo de interventoría y únicamente estará disponible durante las etapas de pruebas de ejecución de cada uno de los proyectos que lo requieran; la documentación producto del ejercicio será colocada en la herramienta de gestión documental del proyecto. Agradecemos confirmar nuestro entendimiento al respecto.	Es correcto el entendimiento.
14	En caso de requerir acceso a las herramientas mencionadas en el numeral 3.4.2.3.Recursos y herramientas de soporte, al personal de la Dian, agradecemos confirmar el número de personas que tendrán acceso a la herramienta para considerarla en las estimaciones de licenciamiento/acceso.	Se precisa que se deben incluir las licencias necesarias para gestión de tareas de proyecto de interventoría, gestión documental del proyecto de interventoría, colaboración entre todos los proyectos y pruebas de los proyectos. El número de licencias dependerá de los equipos definidos en cada proyecto para estas labores.
15	Con relación al Anexo 6 – Cuadro de precios propuesto Interventoría, solicitamos por favor confirmar nuestro entendimiento sobre si lo esperado por parte de ustedes en la pestaña “Cuadro de precios”, es que se diligencie el porcentaje de cada uno de los tipos de interventoría involucrados en cada proyecto, hasta llegar al 100% del valor total por	Ver Respuesta a la Pregunta 9

	proyecto; en caso de no ser así, agradecemos por favor aclarar que información se espera en esta pestaña.	
16	En el numeral 3.2 “Alcance de la Interventoría” en el documento estudio de mercado, se menciona que: “El INTERVENTOR deberá presentar los informes de revisión de los productos entregados por los CONTRATISTAS incluyendo su concepto sobre la aceptación o no de los mismos,” , así mismo, en otros apartados del documento se hace referencia a la obligación de la interventoría de generar concepto de cumplimiento de las actividades y entregables a realizar por cada uno de los contratistas de los proyectos del programa de transformación digital de la DIAN, sin embargo, frente a este punto, es importante tener en cuenta que la interventoría no debería ser juez y parte del proceso y por consiguiente, la interventoría lo que expediría serían conceptos de conformidad de las actividades y entregables frente a los compromisos contractuales y criterios de aceptación que se acuerden entre las partes (DIAN y Contratistas).	Se precisa que el hecho de dar un concepto sobre la aceptación o no de los productos entregados por los contratistas, no debe generar ningún conflicto, ya que dicho concepto se deriva de la revisión/verificación de las características establecidas para dichos productos.
17	En el numeral 3.2.1. “Interventoría administrativa” en su sub numeral 5 se menciona: “Asistir y participar en reuniones, visitas, inspecciones y/o auditorías de seguimiento y control, para verificar el cumplimiento de cada PETD. Estas visitas contarán con la participación del GP de la DIAN, el CONTRATISTA y los demás actores necesarios”. Con lo anterior, entendemos que el proceso de interventoría se realizará en su mayoría de forma virtual y se realizará un plan de visitas a las sedes de la DIAN y de los contratistas las cuales se realizarán de manera presencial, ¿es correcto nuestro entendimiento?	Se aclara que no hay un condicionamiento previo sobre la modalidad (presencial/virtual) que se adopte para las diferentes actividades, siempre y cuando estas sean pertinentes al tipo de acción a realizar y permitan cumplir los objetivos de las mismas
18	Comedidamente solicitamos a la entidad aclarar dónde será el domicilio contractual de la ejecución del contrato y si se prevén visitas fuera de dicho domicilio contractual.	El domicilio contractual de la ejecución del contrato será la ciudad de Bogotá y en el momento no se prevén visitas fuera de esta ciudad. En caso de requerirse a futuro, serían en Colombia, dentro de las sedes de la DIAN.
19	Amablemente solicitamos a la entidad eliminar la obligación contenida en el sub numeral 2 del numeral 3.2.4 “Interventoría a la integración”, el	Se considera pertinente la observación y en consecuencia se retiran los ítems 2 y 8 del numeral 3.2.4. Interventoría a la

	cual menciona que: "Desempeñar el rol de Integrador de los requerimientos cruzados entre los diferentes PETD", toda vez que la interventoría no puede ser juez y parte del proceso y por consiguiente, el rol de integrador de los requerimientos, supuestos, restricciones, riesgos y demás aspectos que afecten a uno o más componentes del programa, deberían ser gestionados por el Gerente del Programa o Proyecto y la interventoría, por su parte, realizaría una verificación a la gestión de dichos requerimientos.	Integración, y se incluye lo siguiente: Realizar análisis y emitir recomendaciones que faciliten la solución de situaciones que puedan generar conflictos en la integración de las diferentes soluciones.
20	Amablemente solicitamos a la entidad eliminar las obligaciones contenidas en los sub numerales 4 y 5 del numeral 3.2.4 "Interventoría a la integración" toda vez que estos hacen referencia a "Gestionar a los contratistas" lo cual, debería ser responsabilidad del gerente de programa o proyecto, la responsabilidad de la interventoría debería estar ligada a revisar el cumplimiento de los contratistas frente a la obligatoriedad de los mismos a la asistencia a reuniones y la entrega de documentación.	Se modifica el texto de los ítems 4 y 5 del numeral 3.2.4 quedando como sigue: "4. Verificar la asistencia de los CONTRATISTAS de cada PETD a los Comités de Integración. 5. Verificar que cada CONTRATISTA de PETD entregue la documentación del proyecto y los artefactos que el comité de integración solicite"
21	Comedidamente solicitamos a la entidad eliminar la obligación contenida en el sub numeral 6, del numeral 3.2.5.1, se establece que el interventor deberá "Revisar y aprobar las necesidades de licenciamiento para la implementación", toda vez que, la interventoría no puede ser juez y parte del proceso, por lo cual, quien debería aprobar el licenciamiento necesario, así como su costo, duración y mantenimiento en el tiempo, debería ser la DIAN como beneficiario del proyecto.	Se modifica el ítem 1.d del numeral 3.2.5.1. Interventoría Técnica Tipo 1. Aplicaciones quedando como sigue: "d. Revisar y dar concepto sobre el cumplimiento de las obligaciones adquiridas respecto al licenciamiento ofertado"
22	En cuanto a la obligación descrita en el numeral 3.4.1.1, con relación a la elaboración RACI del proyecto, solicitamos aclarar en el documento que la matriz RACI que se entregará con el plan de trabajo de interventoría será la relacionada con los entregables y actividades de interventoría, la matriz de cada uno de los proyectos, debería ser obligación de cada contratista, así como del Gerente del Programa o Proyecto, toda vez que, la interventoría no puede ser juez y parte.	Se aclara que la matriz RACI que se entregará con el plan de trabajo de interventoría (numeral 3.4.1.1. Planificación del servicio de interventoría) será la relacionada con los entregables y actividades de interventoría. La matriz RACI de cada uno de los PETD, será entregada por cada contratista como parte de la fase de planeación de cada proyecto.

23	En el numeral 3.4.2.3, se menciona que: "La DIAN cuenta con la herramienta Azure DevOps o la herramienta que defina la DIAN al momento de iniciar el proceso, para la administración de todo el ciclo de vida de las soluciones, siguiendo las mejores prácticas de la herramienta. Por lo tanto, el INTERVENTOR deberá utilizar dicha herramienta, según las necesidades específicas de los servicios de interventoría, desde el inicio del proyecto,", frente a lo anterior, solicitamos aclarar si las licencias de uso de dicha solución serán suministradas por la DIAN o será obligación del interventor adquirir dichas licencias para la prestación del servicio.	Se aclara que será obligación del interventor adquirir dichas licencias para el desarrollo de la interventoría.
24	Con relación a los ANS propuestos en el numeral 3.4.2.5 del documento, solicitamos a la entidad eliminar los ANS 03 y 04, relacionados con "Calidad de las Pruebas realizadas" y "Defectos que se reabrieron en etapa de construcción" toda vez que, los ANS están diseñados para asegurar la gestión y calidad del servicio a prestar y por lo tanto, no se deberían establecer ANS ajenos a la gestión del contratista, en este caso, el futuro interventor, ya que la calidad de las pruebas y los defectos reabiertos, dependerán del trabajo realizado por cada contratista de los proyectos de transformación de la DIAN, cuya gestión no depende al 100% de la interventoría.	Se revisarán los ANS para que queden relacionados con las actividades propias de la interventoría.
25	Por favor precisar el tiempo de duración del programa, así mismo, con el objetivo de validar si los proyectos que conforman el programa empiezan en paralelo, agradecemos nos compartan la duración de cada proyecto con su respectiva fecha de inicio y fecha fin estimadas.	Ver respuesta a la Pregunta 10
26	En las responsabilidades mínimas del equipo de interventoría, se menciona: • Garantizar el cumplimiento de las fechas establecidas dentro del plan de trabajo • Determinar, monitorear, administrar y mitigar los riesgos del proyecto.	Se aclara que las responsabilidades mínimas del equipo de interventoría, a que se hace referencia en la observación, corresponden específicamente a la gestión del servicio de interventoría, y no tienen alcance sobre las actividades análogas que se realizarán en los PETD.

	• Realizar la planificación detallada para el desarrollo del proyecto conforme a las etapas, actividades, obligaciones y duración establecidas para cada una. • Velar por el funcionamiento adecuado de los ambientes de trabajo requeridos para la construcción o adaptación del proyecto. • Cumplir con las dependencias que ocurren durante la ejecución. Frente a lo anterior, solicitamos retirar dichas responsabilidades, o redactarlas de tal forma que, se entienda que la interventoría realizará dichas actividades en la gestión del servicio de interventoría, y no realizará las actividades anteriormente mencionadas frente a los proyectos de transformación, toda vez que, de hacerlo, sería juez y parte del proceso. Estas responsabilidades deberían recaer directamente en el Gerente del Programa o Proyecto, quien sería la persona idónea y con la responsabilidad de gestionar y garantizar, la interventoría por su parte verificará que los compromisos de las partes se desarrollen frente a lo contractualmente establecido y de conformidad con los criterios de aceptación aprobados para la ejecución de los contratos.	
27	Teniendo en cuenta el esquema de multinube híbrida planteado en el Estudio de Mercado y sus anexos sugerimos a la DIAN reformular el requisito de multinube hibridapara considerar un esquema multinube únicamente teniendo en cuenta que las cargas de trabajo que serán ejecutadas requieren de las siguientes capacidades que no están disponibles en una nube privada y solo puede suministrar una nube pública: La nube vs los centros de datos locales La computación en la nube permite a los clientes enfocarse en proyectos que diferencian su organización, sin la carga de las inversiones en el centro de datos y laoperación de infraestructura de TI (como se muestra en la Ilustración 1).	La observación presentada no se relaciona con la prestación del servicio de interventoría objeto de este estudio de mercado. Es un requerimiento del Proyecto de Multinube.

Ilustración 1 – Beneficios clave de la nube de AWS frente a los centros de datos locales

Beneficios generales

A continuación, se detallan algunos de los beneficios clave de la nube de AWS sobrelas soluciones ofrecidas por los centros de datos locales.

- **Beneficios de las economías de escala masivas.** Al usar la computación en lanube, puede lograr un bajo costo variable. Debido a que el uso de millones de clientes activos cada mes se agrega en la nube, los proveedores de computación en la nube como AWS pueden lograr mayores economías de escala, lo que se traduce en precios más bajos de pago por uso.
- **Aumentar la velocidad y la agilidad.** En un entorno de computación en la nube, los nuevos recursos de TI están a solo un clic de distancia, lo que reduce el tiempo que lleva poner esos recursos a disposición de los clientes de semanas a solo minutos. Esto da como resultado un aumento de la agilidad para la organización, ya que el costo y el tiempo que lleva experimentar

	y desarrollar es seguramente significativamente menor. - **Deje de gastar dinero en operar y mantener centros de datos.** Concéntrese en proyectos que son fundamentales para su organización, no en la infraestructura. La computación en la nube le permite concentrar los recursos ensus clientes en lugar de en el trabajo pesado de acumular, apilar, alimentar y proteger servidores. Use la Calculadora del costo total de propiedad (TCO) paraestimar sus ahorros potenciales. - **Parte del trabajo de garantía y cumplimiento está hecho.** AWS es responsable de proteger la infraestructura que ejecuta todos los servicios ofrecidos en la nube de AWS, liberándolo de muchas cargas operativas. AWS cuenta con más de 50 certificaciones y acreditaciones de cumplimiento, lo quesería difícil y costoso de mantener para los sistemas locales independientes. - **Deje de adivinar en la capacidad.** Elimine la necesidad de predecir la capacidad de infraestructura requerida. Cuando toma una decisión sobre la capacidad antes de implementar una aplicación, a menudo termina con recursos inactivos caros o lidiando con una capacidad limitada. Como se ilustra en la Figura 2, con la computación en la nube estos problemas se minimizan. Puede acceder tanto o tan poco como lo necesite y escalar hacia arriba y hacia abajo según sea necesario en minutos	

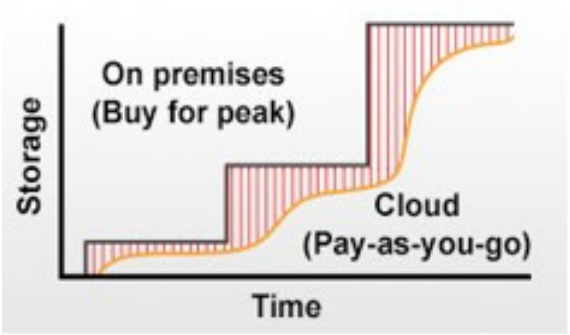

Ilustración 2 – Beneficios del modelo pago por uso

- **Innovación continua de TI.** AWS lanzó 1.017 nuevos servicios y característicasen 2016, 1.430 en 2017 y 1.957 en 2018. Nuestro ritmo de innovación se

  financia y se mantiene a través de nuestras economías de escala y nuestro compromiso de ofrecer los productos y servicios que más importan a nuestrosclientes.

Beneficios específicos de seguridad

La seguridad en la nube en AWS es la máxima prioridad. Como cliente de AWS, se beneficiará de un centro de datos y una arquitectura de red creada para cumplir con losrequisitos de las organizaciones más sensibles a la seguridad. Estamos continuamenteinnovando el diseño y los sistemas de nuestros centros de datos para protegerlos de los riesgos naturales y provocados por el hombre. Luego implementamos controles, construimos sistemas automatizados y nos sometemos a auditorías de terceros para confirmar la seguridad y el cumplimiento.

	AWS mantiene medidas de seguridad y cumplimiento que generalmente están más allá del presupuesto y los recursos de la mayoría de las organizaciones. La seguridad de la infraestructura de AWS se basa en los siguientes principios: - **Constantemente monitoreado.** Los componentes de la infraestructura de AWSestán protegidos por una extensa red de sistemas de monitoreo de seguridad que se escanean y prueban continuamente. La red de producción de AWS está segregada de la red corporativa de Amazon, y el acceso a esta red es monitoreado y revisado diariamente por los gerentes de seguridad de AWS. - **Altamente automatizado.** El uso de AWS le permite beneficiarse de herramientas de seguridad especialmente diseñadas para nuestros requisitos únicos de entorno y escala. Dedique menos tiempo a tareas rutinarias y concéntrese en medidas proactivas que puedan aumentar la seguridad de suentorno de AWS Cloud. - **Altamente disponible.** La nube de AWS ha sido diseñada para proporcionar lamayor disponibilidad al tiempo que establece fuertes salvaguardas con respecto a la privacidad y la segregación del cliente. - **Altamente acreditado.** La infraestructura de TI que AWS proporciona a sus clientes está diseñada y administrada de acuerdo con las mejores prácticas deseguridad y una variedad de estándares de seguridad de TI y programas de cumplimiento, que incluyen: o Controles de sistema y organización (SOC) 1, SOC 2 y SOC 3 o Estándar de seguridad de datos de la industria de tarjetas	

	de pago (PCIDSS) ○ Organización Internacional de Normalización (ISO) 27001, 27017, 27018y 9001 ○ Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP) ○ Ley Federal de Gestión de Seguridad de la Información (FISMA) ○ Instituto Nacional de Estándares y Tecnología (NIST) 800-171 ○ Estándar Federal de Procesamiento de Información (FIPS) 140-2	
28	El Anexo 5 establece lo siguiente como uno de los requerimientos de la múltinube híbrida: *"Nube Privada de Resiliencia en Territorio Nacional, en la cual se almacenarán los respaldos, y tendrá una capacidad de procesamiento esencial para un eventual requerimiento de operar desde territorio nacional los sistemas y aplicaciones misionales que se definan."* Sobre este requisito sugerimos a la DIAN tomar en cuenta las siguientes consideraciones sobre residencia y localización de datos al exigir un entorno hibrido: Consideraciones en la formulación de requisitos orientados a infraestructura en el territorio nacional En el complejo entorno informático de hoy las organizaciones del sector público siguen teniendo una preocupación legítima por la seguridad de sus datos. Por este motivo algunos gobiernos han llegado a la conclusión de que exigir la residencia de los datos, es decir, el requisito de que contenido de los clientes procesado y almacenado en un sistema de TI permanezca dentro de las fronteras del país	La observación presentada no se relaciona con la prestación del servicio de interventoría objeto de este estudio de mercado. Es un requerimiento del Proyecto de Multinube.

	específico, brinda una capa adicional de seguridad. La residencia de los datos es una combinación de problemas asociados principalmente a riesgos de seguridad percibidos (y en algunos casos reales) relacionados con el acceso de terceros a los datos, incluidas las autoridades competentes extranjeras. Los clientes del sector público desean tener la certeza de quesus datos están protegidos frente al acceso no deseado de no solo atacantes maliciosos, sino también de otros gobiernos. Una posición en la que se pida rigurosamente la residencia de los datos a veces restringe el uso de proveedores de servicios en la nube (CSP, por sus siglas en inglés) multinacionales a gran escala, denominados a menudo CSP de hiperescala. La preocupación general en torno a la ciberseguridad, así como la posible extralimitación de la vigilancia gubernamental por parte de algunos países han contribuido a que el debate se centre continuamente en mantener los datos en el país. No obstante, esta restricción es contraproducente para el objetivo de proteger de manera efectiva los datos del sector público. Tal y como se detalla a continuación, un CSP de hiperescala,que puede estar ubicado fuera del país, ofrece a la totalidad de la base de clientes la posibilidad de alcanzar altos niveles de protección de datos con la protección de su propia plataforma y con herramientas llave en mano para sus clientes. Estos proveedores ofrecen estos niveles de protección, al mismo que tiempo que mantienen la soberanía reglamentaria de nación-estado. Los servicios en la nube de hiperescala representan una disrupción tecnológica transformacional debido al alto grado de eficiencia, agilidad e innovación en el suministro de servicios de seguridad de clase mundial para dar soporte a sus clientes.Los CSP de hiperescala diseñan, operan y mantienen ofrecimientos que permiten a clientes	

	de diferentes sectores (comercial, público, regulado) abordar algunos de los riesgos de seguridad y vulnerabilidades predominantes. Los clientes confían en los ofrecimientos de los CSP de hiperescala para que apliquen prácticas de seguridad que sean dinámicas y respondan ante amenazas en tiempo real, mejorando así drásticamente la seguridad de cada cliente. Por su parte, los CSP tienen los incentivos adecuados para mantener una ciberseguridad de clase mundial dado que se enfrentarían a consecuencias sustanciales a largo plazo, tales como las repercusiones asociadas a un sistema en peligro, la pérdida de confianza de los clientes y el daño a lamarca. En otras palabras, la seguridad de primer nivel es requerida para el éxito de un CSP. La seguridad tiene que estar totalmente integrada en el diseño, el desarrollo y lasoperaciones de servicios en la nube de hiperescala. Motivos por los que la residencia de los datos no ofrece mayor seguridad La propiedad y la ubicación geográfica de los datos se ha convertido en un tema importante para las iniciativas de ciberseguridad y políticas relacionadas con la nube entodo el mundo. Desde un punto de vista histórico, el comando y el control de los datos confidenciales de las compañías suponía alojar la información localmente en las instalaciones o en instalaciones propiedad del contratista accesibles físicamente dentrode un país. Tener propiedad total de la “plataforma tecnológica”, desde el suelo y las paredes del edificio hasta el software de los servidores, hacía que la gente tuviera la confianza de que sus datos estaban todo lo seguros que podían estar. Este razonamiento sigue estando vigente en muchos gobiernos. A medida que la tecnología ha ido evolucionando, tres realidades fundamentales hanirrumpido en el modelo del “control de la plataforma	

	tecnológica completa" tradicional. *La mayoría de las amenazas se explotan remotamente.* La ubicación física de los datos tiene poco o ningún impacto en las amenazas propagadas a través de Internet. Los sistemas conectados a Internet exponen a una organización a una amplia variedad de amenazas, todas las cuales se propagan desdecualquier ubicación. Por ejemplo, el reciente código malicioso o ransomware Petya afectó a los servicios de salud, debilitando sus operaciones y la capacidad para cuidar a los pacientes. Esto se ha producido como consecuencia del malware que ha afectadoa la propagación de los centros de datos locales a través de Internet. A pesar de los enormes esfuerzos realizados para proteger los sistemas interconectados utilizando firewalls y otros dispositivos anti-intrusión, la experiencia ha demostrado que la seguridad del perímetro es una parte muy pequeña de un sistema protegido. Sea cual sea la ubicación física, si los sistemas de TI están conectados de alguna manera a Internet (u otras redes con varios participantes), aunque sea indirectamente, dichos sistemas corren un riesgo considerable y son susceptibles de sufrir ataques de un amplio espectro de amenazas de acceso lógico. *Los procesos manuales presentan riesgos de errores humanos.* Los procesos humanos tienen un rol preponderante (sino que en su totalidad), en las fallas de la ciberseguridad. Un ejemplo habitual es no aplicar parches en sistemas vulnerables con actualizaciones de software publicadas durante muchos meses antes de que se produzca la vulnerabilidad de seguridad. El proceso manual de actualizaciónde sistemas aplicando los parches más recientes es difícil y no es factible hacerlo periódicamente sin automatización.	

	Las amenazas provenientes del interior siguen siendo un riesgo significativo. La gran mayoría de las situaciones en las que se han puesto en peligro los datos se han producido como consecuencia de errores no intencionados o a que ha habido un comportamiento malicioso intencionado por parte de personas con cuentas autorizadas con derecho a accesar los datos. En los últimos años, los ataques de seguridad con más alto impacto se atribuyeron principalmente a malas prácticas de higiene cibernética. Entre las amenazas a cuentas autorizadas más frecuentes se encuentran los siguientes escenarios: • **Inadvertida:** las credenciales se pierden o se administran incorrectamente, de manera que un atacante puede actuar dentro de un sistema como un usuario válido. • **Ingeniería social:** ataques de phishing y ataques de ingeniería social que engañan a los usuarios o administradores para que divulguen credenciales a losatacantes. • **Maliciosa:** clásica amenaza proveniente del interior – agentes dentro de laorganización con malas intenciones y objetivos ilegales. La ubicación física de los datos no influye en ninguna de las realidades enumeradasanteriormente. En las circunstancias actuales, la administración de riesgo es una tarea aún más complicada teniendo en cuenta la tecnología móvil y las relaciones entre entidades externas e internas. Todos los sistemas que están conectados a Internet son, directa o indirectamente, un vector de ataque potencial, sea cual sea la ubicación física de la infraestructura o el sistema. A medida que la tecnología progresa y que	

	cambian las vulnerabilidades y los vectores que amenazan a los clientes, los gobiernos tienen que reevaluar la forma de modelar sus estrategias y la tolerancia de riesgos. En la vida real se han producido ya casos que demuestran que almacenar los datos en los servidores propios, los centros de datos propios y el propio país no constituye en modo alguno unaforma apropiada de proteger los datos. Por ejemplo, se produjo un grave ataque de seguridad en una agencia gubernamental estadounidense que afectó a más de 20 millones de empleados federales en un entorno local debido a que se habían comprometido las credenciales de usuario. Dichas credenciales se filtraron y se usaron en Internet desde varios puntos pasandopor alto, de esta manera, todas las protecciones del entorno local. Este error de seguridad del organismo gubernamental estadounidense es un buen ejemplo del tipo de amenaza que existe en Internet sin limitantes geográficas. El problema se aplica no solo en los sistemas en contacto directo con Internet. Los sistemas que no cuentan con una conexión directa a Internet pueden permitir que los usuarios obtengan acceso a Internet mediante una conexión de red privada virtual (VPN) desde portátiles, equipos domésticos o dispositivos móviles. Los ataques de seguridad no necesitan tener acceso físico a un servidor, sino que explotan la carenciade controles de seguridad lógicos implementados de manera efectiva. Con esto se demuestra que el requisito de residencia de datos es poco relevante protegiendo la información contra las amenazas más predominantes hoy en día. Por lo tanto, los requisitos de localización geográfica tienen poca importancia cuando se trata de proteger la información contra las amenazas actuales. En cambio, los mejores mecanismos de protección, detección, respuesta y recuperación consisten en usar la seguridad transformacional ofrecida	

	por los CSP de hiperescala por medio de la modernización y la automatización. Dichos CSP de hiperescala, como es el caso de AWS, invierten en las mejores prácticas de seguridad operativa y técnica, ya que es unelemento fundamental para su operación y ofertas de valor. Los clientes se benefician cuando se apalancan de la infraestructura y soluciones en la nube de los proveedores de servicios en la nube como AWS. Consideraciones al establecer requisitos de residencia de datos Tal y como se ha explicado anteriormente se puede lograr la soberanía estatal o nacional de la ley sobre los datos sin dejar de obtener al mismo tiempo provecho de losbeneficios financieros y de seguridad que aportan los CSP de hiperescala como AWS. Las medidas de seguridad adoptadas en todos los servicios de AWS y verificadas mediante auditorías externas brindan un gran nivel de confianza en la prevención y tratamiento de eventos riesgosos de acceso ilegal a los datos. Alentamos, por tanto, a los gobiernos a considerar las siguientes políticas para cumplir los objetivos de seguridad asociados con la residencia de datos. • Desarrollar políticas y requisitos que permitan el uso de instalaciones de procesamiento de datos fuera del país si dichos datos se procesan y almacenan en un entorno en la nube de hiperescala moderno y de alta seguridad. Los clientes también pueden elegir ubicaciones que tengan leyes de protección de datos similares a las de su país y donde ya existan acuerdos de transferencia dedatos. • Alinear las políticas nacionales y los requisitos reglamentarios con el principio de movimiento libre de datos transfronterizo para	

	equilibrar de manera efectiva objetivos de seguridad, económicos y de modernización de TI. • Evaluar los modelos de transferencia de datos como el Escudo de privacidad UE-EE. UU. (US-EU Privacy Shield, en inglés) y las cláusulas de contratos estandarizadas como los cláusulas modelo de la UE, aprobadas por las autoridades de protección de datos de la UE, y que pueden usarse en acuerdos entre los proveedores de servicios y sus clientes para garantizar que todos los datos personales que salgan del Espacio Económico Europeo se transfieran de acuerdo con el Reglamento General de Protección de Datos (RGPD). Estos tipos de acuerdos de transferencia de datos constituyen una garantía de que losCSP salvaguardarán los datos de manera responsable, además de proporcionarun medio aprobado previamente para proteger y prestar apoyo a la circulación de datos internacional de forma segura y de acuerdo con la normativa. • Asegurarse de que los CSP y los contratistas de terceros demuestren que cuentan con controles de seguridad sólidos para abordar el acceso de terceros no autorizados a datos, sistemas y recursos mediante acreditaciones de tercerosreconocidas a escala internacional (por ejemplo, ISO 27001, ISO 27018, SOC, PCI DSS, etc.). • Clasificar datos y definir roles y responsabilidades de gestión de datos para determinar las obligaciones de protección de datos apropiadas para cada una de las partes. Los gobiernos deben estudiar si aprovechan la norma ISO 27018 para definir los roles del responsable y el encargado del tratamiento de datos. Los gobiernos pueden trabajar con los CSP para comprender y aplicar de manera adecuada las responsabilidades de protección de datos del responsabley el encargado del tratamiento de datos en cada	

	uno de los modelos de servicio en la nube. • Garantizar la comprensión y la implementación por parte del cliente de los servicios de seguridad para el cifrado de datos. AWS ha sido pionera en los servicios de cifrado que ofrecen a los clientes la posibilidad de controlar plenamente las llaves de cifrado. AWS ofrece a los clientes la opción de cifrar datos mediante sus propias llaves que pueden almacenarse fuera de AWS o de manera segura dentro de los servicios ofrecidos, permitiéndoles controlar sus llaves y obtener acceso a datos cumpliendo con estrictas obligaciones de seguridad y conformidad. • Participar en esfuerzos bilaterales y multilaterales para actualizar el proceso del tratado de asistencia judicial recíproca (MLAT) de modo que se equilibren las necesidades de los gobiernos de obtener de inmediato las pruebas necesarias en investigaciones y enjuiciamientos con el derecho de un individuo a la privacidad en relación con el contenido electrónico de su propiedad. Respaldamos la legislación que actualiza la privacidad y el acceso de los organismos encargados del cumplimiento de la ley a las comunicaciones electrónicas, tanto a escala nacional como internacional. También alentamos a los gobiernos a revisar y actualizar su legislación nacional para abordar los roles, las responsabilidades y los mecanismos que rigen el acceso legal a los datos en consonancia con los principios del proceso del tratado de asistencia judicial recíproca. Conclusión Si bien los gobiernos podrían percibir una sensación de mayor seguridad al imponer requisitos de residencia de datos para los datos procesados y almacenados en instalaciones de TI locales debido a que ofrecen proximidad física y control, una evaluación más profunda	

	muestra que restringir los servicios de TI a la jurisdicción local exclusivamente no proporciona una mejor seguridad general de los datos. Desde una perspectiva de riesgo-beneficio, los CSP de hiperescala como AWS pueden ayudar a administrar mejor los riesgos de ciberseguridad al tiempo que minimizan el riesgo de acceso a los datos de gobiernos extranjeros. Los gobiernos también tienen que valorar las contrapartidas significativas asociadas a exigir la residencia de los datos. Los gobiernos que usan requisitos de residencia de datos restrictivos no solo perderán el acceso a algunos de los entornos informáticos más seguros de la tierra, sino que, más allá de la seguridad, se verán obligados a hacer frente a un retraso perpetuo en el acceso a tecnología de vanguardia rentable y necesaria para su propia transformación digital. Exhortamos a los gobiernos a que reevalúen los objetivos de seguridad que realmente consiguen aplicando las restricciones de localización de datos desde el punto de vista de los costos significativos económicos, de modernización de TI y oportunidades de seguridad. Las capacidades de seguridad de los CSP de hiperescala no solo abordan las principales preocupaciones, sino que también proporcionan seguridad a un nivel superior a la que proporcionan las instalaciones locales tradicionales o contratadas localmente. Las soluciones basadas en políticas, como los acuerdos de transferencia de datos y el aprovechamiento de acreditaciones de seguridad internacionales reconocidas, pueden servir como medio suficiente para abordar los objetivos de residencia de los datos al tiempo que se promocionan los objetivos de transformación digital del sector público. Para mayor información sobre residencia de datos por favor consulte el siguiente hipervínculo: https://d1.awsstatic.com/whitepapers/compliance/ES_Whitepapers/Data_Residency_Whitepaper.pdf	

29	Teniendo en cuenta que el punto 3.2.1. Interventoría Administrativa, en el numeral 29 (página 12) establece que: "Realizar el control, verificación y seguimiento, al estricto cumplimiento por parte de cada CONTRATISTA de las obligaciones contenidas en contrato para cada etapa del PETD, lo cual incluye: (…) 29. Verificar que existan y se encuentren vigentes las licencias de productos de software necesarios para el inicio del desarrollo del contrato." Se sugiere ajustar el requerimiento para incorporar los diferentes esquemas de licenciamiento que se puedan llegar a utilizar para desplegar la solución teniendo encuenta que al usar los servicios de nube varias de los componentes de software requeridos para la construcción de la solución pueden ser suministrados bajo los siguientes modelos: Traiga su propia licencia (BYOL – Bring Your Own License). AWS se ha asociado con una variedad de ISV (Independent Software Vendor) que hanpermitido el uso de su producto en Amazon EC2. Esta licencia basada en Amazon EC2es una ruta de baja fricción para mover su software a la nube. Usted compra la licenciade la forma tradicional o usa su licencia existente y la aplica al producto que está disponible como una imagen de máquina de Amazon preconfigurada. Por ejemplo, Oracle, Sybase, Adobe, MySQL, JBOSS, IBM y Microsoft han puesto a disposición su software y soporte en la nube de AWS mediante una opción BYOL. Utilice AWS Marketplace. AWS Marketplace es una tienda de software en línea que ayuda a los	El requisito de "*Verificar que existan y se encuentren vigentes las licencias de productos de software necesarios para el inicio del desarrollo del contrato*", en tanto corresponde a una verificación, es indiferente frente a los tipos específicos de licencias que se establezcan en cada uno de los PETD. Por lo tanto no se considera necesario incluir una lista de las mismas.

	clientes a encontrar, comprar y comenzar a usar de inmediato software que se ejecuta en la nubede AWS. AWS Marketplace ofrece 39 categorías de productos y más de 4.800 listados de software de más de 1.400 ISV. Incluye software de proveedores confiables como SAP, Zend, Microsoft, IBM, Canonical y 10gen, así como muchas ofertas de código abierto ampliamente utilizadas, como WordPress, Drupal y MediaWiki. Los clientes pueden comprar software y licencias directamente de los proveedores. Utilice un modelo de precios de servicios públicos con un paquete de soporte. AWS se ha asociado con ISV de élite para ofrecer su software como una AMI de pago (utilizando el servicio Amazon DevPay). Esta es una licencia de pago por uso en la queno incurre en ningún costo de licencia inicial y solo paga por los recursos que consume.Los ISV cobran una pequeña prima además del costo estándar de Amazon EC2, lo que le brinda la oportunidad de ejecutar cualquier cantidad de instancias en la nube de AWS durante el tiempo que usted controle. Por ejemplo, Red Hat, Novell, IBM y Wowzaofrecen licencias de pago por uso. Los ISV, por lo general, también ofrecen un paquete de soporte que acompaña a la licencia de pago por uso. Utilice un servicio en la nube basado en SaaS de ISV. Algunos de los ISV han ofrecido su software como servicio y cobran una tarifa de suscripción mensual. Ofrecen API estándar e interfaces basadas en web y son bastante rápidas de implementar. Esta oferta se administra total o parcialmente dentro de la nube de AWS. Esta opción suele ser la forma más fácil y rápida de migrar su instalación local existente a una oferta alojada bajo demanda del mismo proveedor o una oferta	

	equivalente de un proveedor diferente. En la mayoría de los casos, los ISV o los integradores de servicios en la nube empresariales independientes de terceros ofrecen herramientas de migración que pueden ayudarlo a mover sus datos. Por ejemplo, Mathematica, Quantivo, Pervasive y Cast Iron proporcionan una oferta de SaaS basada en AWS	
30	Teniendo en cuenta lo dispuesto en el Estudio de Mercado y sus anexos, con relación a la realización de pruebas de seguridad, en específico lo dispuesto en punto 3.4.2.2.3. Revisión especializada a Pruebas de seguridad (página 33): “Estas pruebas hacen parte de las pruebas no funcionales, pero dada su especialidad y relevancia en repositorio y todas sus herramientas se les otorga un capítulo aparte y deberán ceñirse a las especificaciones de controles que identifique el contrato de seguridadde la información, dentro ellas se destacan las pruebas de penetración y *ethical hacking*.” Se solicita respetuosamente a la DIAN tener en cuenta las siguientes recomendacionesde seguridad en la nube: Seguridad Como los clientes de los servicios de informática en la nube crean sistemas sobre la infraestructura de la nube, los proveedores de servicios en la nube y los clientes de estos servicios comparten las responsabilidades en materia de seguridad y conformidad. En un modelo de infraestructura como servicio (IaaS), usted controla el diseño y la protección de sus aplicaciones y los datos que coloca en la infraestructura,mientras que el proveedor de servicios en la nube es responsable de prestar serviciosen una plataforma controlada de alta seguridad y de proporcionar una amplia gama decaracterísticas de seguridad adicionales. El nivel de responsabilidades del proveedor de	El alcance de los servicios de interventoría no incluye la determinación de los niveles de responsabilidad de las partes involucradas en los sistemas de seguridad implementados en los diferentes PETD, ya que se trata de realizar revisión especializada de las pruebas de seguridad que se determinen en cada PETD. Los detalles de las pruebas a realizar se definirán en el plan de pruebas de cada PETD, durante la ejecución del contrato.

	servicios en la nube y del cliente en este modelo de responsabilidad compartida depende del modelo de implementación de la nube (véanse los modelos de definición de la informática en la nube de NIST). El modelo de responsabilidad compartida de AWS se ilustra a continuación.	