

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
	UNIDAD REQUIRENTE:	Página 1 de 55
	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

**PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO
DEL BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL - BIESS**

“CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER”

**Unidad Requirente
COORDINACIÓN DE TECNOLOGÍA /
DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA**

JULIO 2026

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	Página 2 de 55
	UNIDAD REQUIRENTE: COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

ÍNDICE

1. BASE LEGAL.....	4
1.1 NORMATIVAS RELACIONADAS AL OBJETO DE CONTRATACIÓN.....	4
1.2 REGLAMENTO PARA LAS CONTRATACIONES DE GIRO ESPECÍFICO DEL NEGOCIO DEL BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL – BIESS.	5
1.2.1 DE LAS BASES DEL CONCURSO	5
1.2.2 DE LA MODALIDAD DE CONTRATACIÓN	9
2. CARACTERÍSTICAS TÉCNICAS Y CONDICIONES REQUERIDAS PARA LA CONTRATACIÓN	10
2.1 INVITACIÓN O CONVOCATORIA:	10
2.2 ANTECEDENTES:	10
2.3 OBJETIVOS	14
2.4 ALCANCE:.....	14
2.5 METODOLOGÍA DE TRABAJO.....	15
2.6 INFORMACIÓN QUE DISPONE EL BIESS:.....	18
2.7 PRODUCTOS O SERVICIOS ESPERADOS:.....	18
2.8 DEFINICIÓN DE PRESUPUESTO REFERENCIAL:	35
2.9 PLAZO DE EJECUCIÓN:.....	36
2.10 FORMA Y CONDICIONES DE PAGO:.....	36
2.11 GARANTÍAS.....	37
2.12 RIESGOS ASOCIADOS A LOS SERVICIOS PROVISTOS POR TERCEROS	37
3 CONDICIONES PARTICULARES DE LA CONTRATACIÓN.....	37
3.1 OBLIGACIONES DEL CONTRATISTA:.....	37
3.2 OBLIGACIONES ADICIONALES DEL CONTRATISTA:.....	38
3.3 OTRAS CONDICIONES CONTRACTUALES EXIGIDAS POR LOS ENTES DE CONTROL	41
3.4 OBLIGACIONES DEL CONTRATANTE Y ADMINISTRADOR DE CONTRATO	42
3.5 TRATAMIENTO DE DATOS PERSONALES	42
3.6 MULTAS Y PENALIZACIONES:	44
3.7 VIGENCIA DE LA OFERTA:.....	45
3.8 SUBCONTRATACIÓN	45
3.9 DEBIDA DILIGENCIA – POLÍTICA CONOZCA A SU PROVEEDOR	45
4 PARÁMETROS Y METODOLOGÍA DE EVALUACIÓN DE LAS OFERTAS	46
4.1 METODOLOGÍA CUMPLE / NO CUMPLE.....	46

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO		Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER		Página 3 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA		

A)	INTEGRIDAD DE LA OFERTA:	46
B)	EXPERIENCIA DE EL/LOS PARTICIPANTE/S	46
C)	PERSONAL TÉCNICO, RECURSO HUMANO, EQUIPO DE TRABAJO / RECURSOS. -.....	47
D)	OFERTA ECONÓMICA	49
E)	ANÁLISIS DE ÍNDICES FINANCIEROS:	49
F)	OTRO(S) PARÁMETRO(S) EXIGIDOS POR LOS ENTES DE CONTROL. -.....	49
4.2	METODOLOGÍA POR PUNTAJE	51
5	DOCUMENTOS ANEXOS.....	54
	FIRMA DE RESPONSABILIDAD:	55

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
	UNIDAD REQUIRENTE:	Página 4 de 55
	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

1. BASE LEGAL

1.1 NORMATIVAS RELACIONADAS AL OBJETO DE CONTRATACIÓN

CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR

“Art. 372.- (...) Los fondos provisionales públicos y sus inversiones se canalizarán a través de una institución financiera de propiedad del Instituto Ecuatoriano de Seguridad Social; su gestión se sujetará a los principios de seguridad, solvencia, eficiencia, rentabilidad y al control del órgano competente.”

CÓDIGO ORGÁNICO ADMINISTRATIVO

“Art. 3.- Principio de eficacia. Las actuaciones administrativas se realizan en función del cumplimiento de los fines previstos para cada órgano o entidad pública, en el ámbito de sus competencias”.

CÓDIGO ORGÁNICO MONETARIO Y FINANCIERO

“Art. 160.- Sistema financiero nacional. El sistema financiero nacional está integrado por el sector financiero público (...).”

“Art. 365.- Naturaleza. - Las entidades del sector financiero público se constituirán como personas jurídicas de derecho público, con autonomía administrativa, financiera y presupuestaria. En el ejercicio de sus actividades y servicios financieros se regirán por las disposiciones de este Código, las que emitan la Junta, los organismos de control, sus respectivos directorios, las aplicables a las instituciones financieras y en los demás, aplicarán la legislación que rige a las instituciones públicas”.

LEY DEL BANCO EL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL

“Art. 1.- Creación, denominación y naturaleza. - Créase el BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL, como una institución financiera pública con autonomía técnica, administrativa y financiera, con finalidad social y de servicio público, de propiedad del Instituto Ecuatoriano de Seguridad Social, denominada en adelante "el Banco", con personería jurídica propia, que se regirá por la presente Ley y por su Estatuto”.

“Art. 2.- Objeto social. - El objeto social del Banco será la prestación de servicios financieros bajo criterios de banca de inversión, para la administración de los fondos previsionales públicos del Instituto Ecuatoriano de Seguridad Social IESS; los Fondos Complementarios Previsionales Cerrados;

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO		Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER		
			Página 5 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA		

y, la prestación de servicios financieros, para atender los requerimientos de sus afiliados activos y jubilados (...)".

1.2 REGLAMENTO PARA LAS CONTRATACIONES DE GIRO ESPECÍFICO DEL NEGOCIO DEL BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL – BIESS.

1.2.1 DE LAS BASES DEL CONCURSO

“Art. 5. - Definiciones. - Para efectos de la aplicación del presente reglamento, se tendrán en cuenta las siguientes definiciones: (...) **5.2 Bases del concurso:** Documento que contiene las características técnicas y condiciones requeridas para la contratación, parámetros de evaluación, las obligaciones contractuales, el cronograma, la forma de presentación de ofertas; y, demás particularidades de la contratación. (...) **5.6 Fase preparatoria:** Incluye la elaboración y/o modificación del Plan Operativo Anual - POA; informe de necesidad; informes técnicos de ser el caso, estudio de mercado para definir el presupuesto referencial; bases del concurso (...) **5.10 Mejor oferta:** Oferta que brinde al BIESS, las mejores condiciones en los aspectos técnicos, económicos y legales, sin que el precio más bajo sea el único parámetro de selección. En todo caso, los parámetros de evaluación deberán constar obligatoriamente en las bases del concurso.”

“Art. 27. - Bases del concurso. - Para la contratación de adquisición de bienes y servicios, incluidos los de consultoría, el área requirente elaborará y aprobará las bases del concurso, tomando en cuenta los siguientes aspectos:

1. Deberán ser claras, completas e inequívocas; no deben presentar ambigüedades, ni contradicciones entre las mismas, que propicien o permitan diferentes interpretaciones.
2. Las áreas requirentes conjuntamente con la Dirección de Riesgo Operativo identificarán los bienes y servicios provistos por terceros que soportan los procesos críticos del negocio; de igual manera determinarán y evaluarán los riesgos a los que se expone el BIESS al contratar servicios provistos por terceros para determinar los factores y condiciones de mitigación a considerar en las bases de concurso.
3. El área requirente deberá observar y cumplir con todos los requisitos establecidos en las normas de control para la gestión del riesgo operativo vigente, emitidas por la Superintendencia de Bancos y demás normativa interna, particularmente en los que soportan los procesos críticos del BIESS, debiendo incorporar en las bases del concurso, los parámetros y procesos que aseguren la evaluación, calificación y selección de los proveedores; así como las condiciones requeridas para la prestación del servicio y las obligaciones del contratista, que se trasladarán a las cláusulas contractuales como obligaciones de las partes.
4. El área requirente, deberá establecer el proceso que asegure el control y monitoreo de los servicios contratados, mediante la evaluación, gestión y vigilancia de éstos, a fin de garantizar que se cumplan en todo momento con los niveles mínimos de servicio acordados y demás cláusulas establecidas en el contrato. La información utilizada para el monitoreo de los servicios contratados debe ser obtenida por la entidad controlada de manera independiente de aquella que proporcione el proveedor, para lo cual podrá utilizar los mecanismos técnicos que considere pertinentes, que le permita confirmar el cumplimiento de las condiciones contractuales.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 6 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

5. *Las Bases del concurso, deberán contener por lo menos, pero sin limitarse a: (...)*

Las bases del concurso, incluirán cualquier otra condición exigida por la Superintendencia de Bancos, o demás normativa que rige al sistema financiero, de acuerdo al objeto de contratación; y, serán aprobadas por el titular del área requirente; y, revisadas por las áreas técnicas que correspondan.

Las bases del concurso no podrán afectar el trato igualitario que se le debe dar a todos los participantes, ni establecer diferencias arbitrarias entre éstos.

27.1 Consideraciones particulares de las bases del concurso: *En cumplimiento de las disposiciones exigidas por la Superintendencia de Bancos, las áreas requirentes con el acompañamiento de las áreas técnicas deberán incorporar en las Bases del concurso, las disposiciones vigentes exigidas por el ente de control (...).*

“Art. 6.- Contratación sujetas al Giro Específico del Negocio. *La determinación de las contrataciones sujetas a la modalidad de Giro Específico del Negocio, deberá cumplir con las siguientes condiciones:*

- a) Que se encuentren reguladas por la normativa establecida para las instituciones del Sistema Financiero, y demás disposiciones exigidas por la Superintendencia de Bancos.*
- b) Que se encuentren planificadas y aprobadas en el Presupuesto Operativo Anual – POA del BIESS, del correspondiente ejercicio fiscal.*
- c) Los fundamentos de hecho y derecho que motiven la relación directa del objeto de contratación con la normativa aplicable.”*

“Art. 7.- Aprobación de las contrataciones de Giro Específico del Negocio. *Los titulares de las áreas requirentes emitirán un informe debidamente motivado que contenga la evaluación de las condiciones mínimas exigidas en este reglamento, pudiendo incluir otros aspectos técnicos de acuerdo a la naturaleza de la contratación que fundamenten la contratación como Giro Específico del Negocio. El mencionado informe será puesto a consideración del gerente general para su aprobación previo al inicio del proceso.”*

“Art. 10.- De las atribuciones y responsabilidades del gerente general. *- El gerente general además de las atribuciones y funciones conferidas en el ordenamiento jurídico, le corresponde: (...)*

- b) Aprobar la determinación de las contrataciones de Giro Específico del Negocio del BIESS (...).*

CODIFICACIÓN DE NORMAS DE LA SUPERINTENDENCIA DE BANCOS LIBRO I, NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIERO PÚBLICO Y PRIVADO; TÍTULO IX DE LA GESTION Y ADMINISTRACIÓN DE RIESGOS; Capítulo V. - NORMA DE CONTROL PARA LA GESTIÓN DEL RIESGO OPERATIVO, Artículo 2 de las definiciones, establece:

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 7 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

25. Factores de Riesgo Operativo. - Es la causa primaria o el origen de un evento de riesgo operativo. Los factores son: procesos, personas, tecnología de la información y eventos externos.

28. Incidente. - Es una interrupción no planificada de un servicio o la reducción de su calidad, que afecta el normal funcionamiento de sus servicios.

29. Información Crítica. – Es la información consideradas esencial para la continuidad del negocio y para la adecuada toma de decisiones.

43. Proceso crítico. - Es el conjunto de actividades indispensables para la continuidad del negocio y las operaciones de la entidad controlada, y cuya falta de identificación o aplicación deficiente puede generarle un impacto negativo.”

Los numerales 6 y 7, del segundo inciso del artículo 5, **SECCIÓN II “ADMINISTRACIÓN DEL RIESGO OPERATIVO”, CAPÍTULO V.- NORMA DE CONTROL PARA LA GESTIÓN DEL RIESGO OPERATIVO, TÍTULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, del LIBRO I.- NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO,** se dispone:

“ARTÍCULO 5.- Las entidades controladas deben identificar los riesgos operativos por la línea de negocio, tipo de evento, factor de riesgo operativo y las fallas o insuficiencias, utilizando para el efecto, una metodología debidamente documentada y aprobada que incorporará la utilización de herramientas que se ajusten a las necesidades de la entidad, tales como: autoevaluación, mapas de riesgos, indicadores, tablas de control (scorecards), bases de datos u otras.

Los tipos de eventos de riesgo operativo que deben considerarse, al menos, son los listados a continuación; para un mayor detalle referirse al Anexo No. 1, de la presente norma: ...

6. Interrupción del negocio por fallas en la tecnología de la información; y,

7. Deficiencias en el diseño y/o la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.”

Literales a), e) y g), del numeral 5, **ARTÍCULO 15.- Factor Tecnología de la Información, SECCIÓN III.- FACTORES DEL RIEGO OPERATIVO, CAPÍTULO V.- NORMA DE CONTROL PARA LA GESTIÓN DEL RIESGO OPERATIVO, TÍTULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, del LIBRO I.- NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO,** se dispone:

“(...) ARTÍCULO 15.- Factor Tecnología de la Información de las entidades controladas deben contar con tecnología de la información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna, confiable y segura; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, esté disponible para la toma de decisiones.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 8 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

Para considerar la existencia de un apropiado ambiente de gestión de riesgo tecnológico, las entidades controladas deben, como mínimo, pero sin limitarse a: (...)

5. Con el objeto de garantizar que la infraestructura tecnológica que soporta las operaciones sea administrada, monitoreada y documentada, las entidades controladas deben implementar, al menos, lo siguiente, pero sin limitarse a:

a) Infraestructura que soporta los procesos críticos con la redundancia necesaria para evitar puntos únicos de falla; de la cual se debe mantener el inventario y respaldos de la configuración actualizada e informes de su mantenimiento periódico; en el caso de los enlaces de comunicación, debe considerar que la trayectoria de los enlaces principal y alterno sean diferentes; ...

e) Centros de procesamiento de datos, principal y alterno, en áreas protegidas con los suficientes controles que eviten el acceso de personal no autorizado, daños a los equipos de computación y a la información en ellos procesada, almacenada o distribuida; y, condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la infraestructura de tecnología de la información. La ubicación del centro de procesamiento de datos alterno no debe estar expuesta a los mismos riesgos del sitio principal; ...

g) Para el caso de infraestructura provista por terceros, asegurar el cumplimiento de las disposiciones incluidas en los numerales precedentes (...)"

NORMAS DE CONTROL INTERNO DE LA CONTRALORÍA GENERAL DEL ESTADO (CGE)

410-10 Mantenimiento y control de la infraestructura tecnológica

La administración de la infraestructura tecnológica incluirá la adopción de políticas y procedimientos para el mantenimiento preventivo y correctivo, actualización, licenciamiento y control de los activos informáticos, con el fin de asegurar su óptimo funcionamiento, disponibilidad y la continuidad operativa de los servicios institucionales.

410-11 Seguridad de tecnología de información

Los responsables de la tecnología de la información definirán e implantarán políticas, normativas, procedimientos y mecanismos de seguridad físicos y lógicos, enfocados a salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información, bases de datos y sistemas de aplicación de la entidad, mitigando los riesgos tecnológicos y de ciberseguridad.

410-12 Plan de contingencias

Las entidades dispondrán de planes de contingencia y continuidad tecnológica debidamente documentados, aprobados, difundidos y probados periódicamente, que permitan la recuperación de

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 9 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

los servicios e infraestructura de tecnologías de la información ante situaciones de desastre o fallas disruptivas, garantizando la continuidad de las operaciones críticas.

LEY DE INNOVACIÓN Y DESARROLLO DE TECNOLOGÍA FINANCIERA (LEY FINTECH)

Art. 19.- De la tercerización de servicios tecnológicos. - Las entidades sujetas a las disposiciones de esta Ley que contraten con terceros la prestación de servicios tecnológicos, el procesamiento de datos, o el uso de plataformas e infraestructura digital para el desarrollo de actividades financieras tecnológicas, serán directamente responsables ante los organismos de control y los usuarios por la continuidad, seguridad y calidad de los servicios prestados. Los contratos respectivos deberán prever mecanismos de auditoría, acceso a la información y supervisión por parte de la autoridad competente.

REGLAMENTO PARA LAS CONTRATACIONES DE GIRO ESPECÍFICO DEL NEGOCIO DEL BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL – BIESS

1.2.2 DE LA MODALIDAD DE CONTRATACIÓN

“CAPÍTULO II

DE LAS MODALIDADES DE CONTRATACIÓN

Art. 23.-De selección. -Aquellas contrataciones de adquisición de bienes y servicios, incluidos los de consultoría que, cuenten con varios proveedores en el mercado, cuyo presupuesto referencial sea superior al resultado de multiplicar el monto del Presupuesto Inicial del Estado por el coeficiente 0,0000002, serán contratados por este procedimiento, a través de la convocatoria publicada en la página web institucional.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	Página 10 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

2. CARACTERÍSTICAS TÉCNICAS Y CONDICIONES REQUERIDAS PARA LA CONTRATACIÓN

2.1 INVITACIÓN O CONVOCATORIA:

Se convoca a las personas naturales, jurídicas, en asociación o consorcios; cuya actividad económica se encuentre relacionada directamente al objeto de contratación, legalmente capaces para contratar, a que presenten sus ofertas para la **“CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER”**

2.2 ANTECEDENTES:

Mediante Ley de Banco del Instituto Ecuatoriano de Seguridad Social – BIESS publicada en el Suplemento del Registro Oficial No. 587, de 11 de mayo del 2009, se crea el Banco del Instituto Ecuatoriano de Seguridad Social como una institución financiera pública, con personería jurídica propia y de carácter público, con finalidad social, con autonomía técnica, administrativa y financiera.

Mediante informe de la Contraloría General del Estado número DNAI-0087-2020, se recomienda a la Coordinación de Tecnología:

“(...)7. Dispondrá y supervisará a la comisión técnica encargada de la calificación de ofertas que el proveedor cumpla con los estándares de Data Center (Certificación TIER III o superior), servicios de Housing, Servicios de Cloud Computer, Servicios de Seguridad Informática, Servicios de Conectividad a nivel nacional e internacional para redes LAN / WAN con acceso a Internet y Sistemas de Almacenamiento, así también deberá, presentar un informe de factibilidad del proveedor para soportar todas las aplicaciones del Banco y un plan de migración técnico de la infraestructura tecnológica (moving).(...)”

Conforme el Estatuto Orgánico por Procesos del BIESS, establece como misión de la Coordinación de Tecnología del BIESS: *“Contribuir al logro de los objetivos estratégicos del Banco del Instituto Ecuatoriano de Seguridad Social mediante la provisión de servicios e infraestructura tecnológica necesarios que permitan asegurar las operaciones de la Institución aplicando las mejores prácticas de tecnologías de información y dando cumplimiento a las políticas de Tecnologías de la Información y Comunicación –TIC-”*.

Mediante Memorando Nro. BIESS-DIRB-2026-0251-MM, se informa a, la Coordinación de Tecnología la aprobación del Plan Estratégico de Tecnologías de la Información (PETI) para el período 2026-2030. Este instrumento de planificación institucional traduce los objetivos estratégicos en capacidades tecnológicas concretas, encontrándose alineado de forma directa al Objetivo Estratégico Institucional OEI 5: "Incrementar la eficiencia institucional en procesos y uso de recursos, bajo criterios de seguridad y gestión integral de riesgos, innovación tecnológica y confiabilidad de sistemas".

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
	UNIDAD REQUIRENTE:	Página 11 de 55
	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

En el diagnóstico de la situación actual (AS-IS) plasmado en el referido PETI, se identificó como un riesgo operativo e institucional prioritario la obsolescencia de componentes lógicos y físicos que soportan las aplicaciones centrales del Banco. El documento estratégico determina que, para mitigar las brechas de ciberseguridad, infraestructura y los tiempos objetivos de recuperación), es indispensable viabilizar la ejecución del portafolio de proyectos definidos en los Objetivos Estratégicos de TI.

En cumplimiento al Oficio Nro. CNTEP-GNNEG-2024-0058-O de 20 de noviembre de 2024, la Coordinación de Tecnología actuó de manera oportuna y diligente, remitiendo a CNT E.P. la totalidad de los insumos técnicos habilitantes requeridos en dicho pronunciamiento (inventarios, arquitectura y RVTools) con el fin de viabilizar el análisis de factibilidad para los servicios de housing y moving. No obstante, el despliegue planificado de las mesas técnicas conjuntas y la continuidad de este proceso de transición no se ejecutaron de manera fluida debido a los constantes cambios administrativos y de autoridades del Nivel Jerárquico Superior ocurridos dentro de la institución. Estas sucesivas transiciones organizacionales interrumpieron el cronograma de trabajo e implicaron recurrentes periodos de inducción, revisión de antecedentes e informes de riesgos por parte de las nuevas administraciones, impidiendo avanzar con el plan de reubicación planificado en ese entonces. Una vez estabilizada la gobernanza institucional y reactivadas formalmente las mesas de evaluación técnica, según consta en el reciente Oficio Nro. CNTEP-GNNEG-SC-SO-2026-0573-O de fecha 15 de mayo de 2026, CNT E.P. ratificó oficialmente que la infraestructura central del Banco mantiene complejidades estructurales, de obsolescencia y de soporte de terceros que impiden una transición inmediata. El operador público concluyó de manera definitiva que proceder con la reubicación física o virtualización en el escenario actual comprometería gravemente la estabilidad operativa, la disponibilidad y la seguridad de los servicios críticos del banco. Por lo tanto, para precautelar de forma obligatoria la continuidad de los servicios financieros y de seguridad social del BIESS, se justifica la contratación de contingencia con el proveedor actual (TELCONET) como la única alternativa viable en el mercado.

Con fecha 29 de julio de 2025, el Banco del Instituto Ecuatoriano de Seguridad Social y la compañía TELCONET S.A., suscribieron el Contrato Nro. BIESS-CJUR-GE-006-2025 por Giro Específico del Negocio para la “CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATA CENTER”, por un valor de \$784.400,00 más IVA, con un plazo de ejecución de 365 días a partir de la fecha de suscripción del contrato, con vigencia hasta el 29 de julio de 2026.

Con oficio No. BIESS-CTEC-2026-0018-OF, de 06 de mayo de 2026, el Sr. Coordinador de Tecnología, solicitó a la Corporación Nacional de Telecomunicaciones – CNT E.P.

“(..) Como antecedente relevante, se hace referencia al Oficio Nro. CNTEP-GNNEG-2024-0058-O, mediante el cual la Corporación Nacional de Telecomunicaciones – CNT E.P. emitió un criterio técnico respecto de la infraestructura tecnológica del BIESS, señalando la conveniencia de mantener la operatividad con el proveedor actual, en atención a la complejidad de la infraestructura física del

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO		Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER		
			Página 12 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA		

Banco y a los riesgos asociados a un eventual traslado o moving de equipos con condiciones limitadas de soporte técnico.

Considerando que el BIESS debe garantizar la continuidad, disponibilidad, integridad y estabilidad de los servicios tecnológicos que soportan sus productos financieros, entre ellos Préstamos Quirografarios, Préstamos Hipotecarios y Préstamos Prendarios, resulta necesario contar con un pronunciamiento técnico actualizado que permita evaluar la factibilidad de provisión del servicio de Data Center más allá de junio de 2026. En virtud de lo expuesto, solicito a usted se sirva emitir un pronunciamiento formal respecto de si CNT E.P. se encuentra técnica y operativamente en capacidad de brindar los servicios de Data Center bajo las condiciones actuales de la infraestructura tecnológica del BIESS, considerando los riesgos de obsolescencia, continuidad operativa, disponibilidad de servicios, integridad de la información y soporte especializado requerido.

En caso de que CNT E.P. determine la factibilidad técnica y operativa para brindar los servicios de Data Center bajo las condiciones actuales de la infraestructura tecnológica del BIESS, se solicita que dicho criterio sea expresamente señalado en su respuesta formal. Asimismo, de ser procedente, se requiere coordinar y conformar las mesas técnicas necesarias entre CNT E.P. y el BIESS, a fin de analizar el alcance del servicio, condiciones técnicas, riesgos, requerimientos de continuidad, mecanismos de transición y demás aspectos necesarios para una eventual provisión del servicio.

De igual manera, se solicita indicar si CNT E.P. ratifica, actualiza o modifica el criterio técnico emitido mediante el oficio antes referido, particularmente en relación con la recomendación de mantener la continuidad operativa con el proveedor actual, en caso de que un eventual traslado de infraestructura represente riesgos relevantes para la operación tecnológica del Banco.

El pronunciamiento solicitado permitirá al BIESS contar con los elementos técnicos necesarios para la toma de decisiones institucionales orientadas a precautelar la continuidad de los servicios financieros, la seguridad de la información y la estabilidad operativa de la infraestructura tecnológica, durante el período de transición hacia la renovación tecnológica institucional. (..)"

En seguimiento al requerimiento institucional, mediante oficio No. BIESS-CTEC-2026-0018-OF de 08 de mayo de 2026, el Sr. Coordinador de Tecnología presentó una insistencia ante la Corporación Nacional de Telecomunicaciones (CNT E.P.). Dicha entidad remitió su pronunciamiento técnico oficial mediante el Oficio Nro. CNTEP-GNNEG-SC-SO-2026-0573-O de 15 de mayo de 2026, señalando textualmente lo siguiente:

(..) Frente a la persistencia de las brechas tecnológicas y la falta de avance en las actividades preparatorias por parte del BIESS, CNT E.P. ratifica que, mientras la entidad solicitante no solvante los requerimientos de su competencia, se mantendrá un alto nivel de riesgo para la ejecución de los servicios de housing y moving. Proceder con la reubicación física o virtualización de la

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO		Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER		Página 13 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA		

infraestructura en el escenario actual comprometería gravemente la estabilidad operativa, la disponibilidad y la seguridad de los servicios críticos del banco, así como la protección de la información ciudadana e institucional (...)

Con fecha 8 de mayo de 2026, se llevó a cabo una reunión de trabajo entre los equipos técnicos del Banco del Instituto Ecuatoriano de Seguridad Social (BIESS) y la Corporación Nacional de Telecomunicaciones (CNT EP).

Durante la reunión, se analizó detalladamente la alta criticidad del servicio y se identificaron los riesgos de nivel extremo a los que se expondría la infraestructura tecnológica de la institución en caso de un eventual traslado físico de los equipos hacia un centro de datos diferente. Entre las principales alertas técnicas evaluadas, se destacaron la potencial inestabilidad y los posibles daños mecánicos o lógicos en los componentes de hardware que se encuentran en estado de obsolescencia o fin de vida útil, lo que provocaría una interrupción en la continuidad de las operaciones financieras y los servicios transaccionales dirigidos a los afiliados.

Con el objetivo de salvaguardar la seguridad de la información y mitigar cualquier impacto operativo o económico, ambas entidades acordaron establecer mesas de trabajo interinstitucionales. Este espacio técnico conjunto permitirá estructurar y planificar de forma segura la viabilidad de futuros proyectos tecnológicos y de conectividad, garantizando siempre el cumplimiento de las normativas vigentes del ente de control. Conforme lo manifestado en el Oficio Nro. BIESS-CTEC-2026-0028-O de 29 de mayo de 2026, mismo que manifiesta.

(...) Con el objetivo de salvaguardar la seguridad de la información y mitigar cualquier impacto operativo o económico, ambas entidades acordaron establecer mesas de trabajo interinstitucionales. Este espacio técnico conjunto permitirá estructurar y planificar de forma segura la viabilidad de futuros proyectos tecnológicos y de conectividad, garantizando siempre el cumplimiento de las normativas vigentes del ente de control.

Conforme lo indicado en el Oficio Nro. CNTEP-GNNEG-SC-SO-2026-0573-O, mismo que manifiesta la necesidad indispensable de subsanar los requerimientos técnicos antes de definir la entrega formal del servicio.

En tal virtud, esta Coordinación concluye que la Corporación Nacional de Telecomunicaciones (CNT E.P.) no brindará al momento, los servicios gestionados de Data Center (Housing y Moving) solicitados por nuestra institución, debido a que proceder con la reubicación en el escenario actual comprometería gravemente la estabilidad operativa, la disponibilidad y la seguridad de los servicios críticos del banco.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
	UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA

Con este pronunciamiento, el BIESS procederá con las acciones administrativas pertinentes dentro de su competencia para asegurar la continuidad de los servicios de Data Center con el proveedor actual y evitar la indisponibilidad de la banca pública (...)

Por lo expuesto, y con el fin de salvaguardar la continuidad operativa, la seguridad de la información y la estabilidad de los servicios financieros del Banco, se vuelve imperativo y crítico dar inicio el proceso para la Contratación de Servicios Gestionados de Data Center.

Mediante el Informe Nro. INF-CTEC-2026-057 de 09 de junio de 2026, la Coordinación de Tecnología emitió la justificación técnica y legal para determinar este proceso bajo la modalidad de Giro Específico del Negocio. Dicho instrumento demostró la subsunción absoluta del servicio en las condiciones del Artículo 6 del Reglamento interno, al comprobarse que: a) se encuentra regulado por la Norma de Riesgo Operativo de la Superintendencia de Bancos; b) cuenta con asignación en la Partida Presupuestaria 520706 (Servicios Tecnológicos) del POA vigente; y, c) se fundamenta en la dependencia absoluta del Banco de un Data Center externo de categoría TIER III para operar el core bancario (IBS Producción) y viabilizar los Préstamos Quirografarios, Hipotecarios y Prendarios. El informe concluyó que esta modalidad es el mecanismo idóneo para garantizar los niveles de servicio (SLA), redundancia y ciberdefensa (AntiDDoS, NGFW, WAF) exigidos por el ente de control, salvaguardando la continuidad de la banca pública.

Con memorando Nro. BIESS-CTEC-2026-0386-MM de 10 de junio de 2026, el Sr. Coordinador DE TI, solicitó la aprobación para la determinación de la **“Contratación de Servicios Gestionados de Data Center”**, por Giro Específico del Negocio; y, conforme memorando BIESS-GGEN-2026-0682-MM, de 11 de junio de 2026, el Gerente General dispuso: (...) *en cumplimiento al artículo 7 del “Reglamento para las contrataciones del giro específico de negocio del Banco del Instituto Ecuatoriano de Seguridad Social – BIESS” vigente, aprueba el objeto de contratación, para que gestione el proceso como Giro Específico del Negocio, bajo la modalidad que aplique de acuerdo a su reglamentación (...).*

2.3 OBJETIVOS

Incrementar la eficiencia institucional en procesos y uso de recursos, bajo criterios de seguridad y gestión integral de riesgos, innovación tecnológica y confiabilidad de sistemas

2.4 ALCANCE:

Contar con el Servicio Gestionado de Data Center en un Data Center Principal situado en la ciudad de Guayaquil y un Data Center Alterno ubicado en la ciudad de Quito para el BIESS, por un periodo de 365 días, según necesidades del Banco, en horario 24/7/365.

Los servicios que se deben cubrir son:

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 15 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

- Alquiler de espacio físico de Data Center en modalidad Housing (con todas las facilidades solicitadas en las especificaciones técnicas) para el Centros de Datos principal y alterno, con características mínimas de Certificación mínimo TIER III del certificado por Uptime Institute.
- Servicio de networking para conectividad de todo el equipamiento tecnológico del BIESS
- Servicio de gestión de Next Generation Firewall.
- Servicio Web Application Firewall (WAF).
- Servicios de Balanceo de carga para plataformas y/o aplicativos web del banco.
- Servicio AntiDdos (incluye scrapping)
- Servicio de Almacenamiento
- Servicio de Manos Remotas de Data Center.
- Servicio de Datos de Canal L2.
- Servicios gestionados bajo demanda.

2.5 METODOLOGÍA DE TRABAJO

Para la ejecución del presente proceso, el contratista adjudicado y la institución se registrarán bajo los siguientes lineamientos metodológicos estructurados en dos componentes esenciales:

Prestación del Servicio

El contratista será el responsable absoluto del correcto funcionamiento y de la provisión continua de los servicios contratados, debiendo sujetarse al siguiente esquema operativo:

Planificación e Inventario Inicial: El contratista, por medio de su Gerente o Líder de Proyecto, elaborará y entregará en un plazo máximo de quince (15) días calendario a partir de la firma del contrato, un plan de trabajo detallado que incluya:

- Inventario pormenorizado de todo el equipamiento y elementos del BIESS alojados en los Centros de Datos actuales.
- Plan de organización de equipamiento (distribución óptima en racks, mapeo físico, *port mapping* y *power mapping*).
- Matriz de riesgos operativos asociados a la infraestructura de red.

Gestión de Cambios y Continuidad: El contratista coordinará y gestionará con el Administrador de Contrato la aprobación de las ventanas de mantenimiento requeridas para cualquier actividad programada. La solicitud se realizará conforme a los Métodos de Procedimiento (MOP) aprobados, garantizando la validación previa de los servicios para evitar incidentes, encolamientos, caídas o la degradación de la estabilidad transaccional.

Entregables de Estabilización: Una vez reorganizados los componentes físicos o lógicos, el contratista elaborará un informe técnico que contenga: diagramas detallados de conexión (LAN,

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 16 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

WAN, racks, SAN), inventario de configuraciones activas (Firewall, WAF, Balanceador de Carga, DDoS), *power mapping* actualizado y el acta de entrega-recepción parcial de funcionamiento técnico.

Evidenciables Mensuales de Operación: Para justificar la ejecución del servicio y dentro de los primeros cinco (5) días calendario de cada mes, el contratista entregará al Administrador del Contrato de manera obligatoria:

- Informes individuales de disponibilidad por cada uno de los servicios de seguridad perimetral, balanceo, WAF y DDoS.
- Reportes consolidados de alertas, bloqueos e incidentes de ciberseguridad mitigados.
- Reporte mensual de consumo de horas de soporte y manos remotas.
- Reporte de tickets levantados en la mesa de servicios.

Control y Monitoreo del Servicio (*Cumplimiento Obligatorio Superintendencia de Bancos*)

En estricto cumplimiento del Artículo 23 de la Norma de Control para la Gestión del Riesgo Operativo de la Superintendencia de Bancos, el Administrador del Contrato del BIESS ejercerá las facultades de evaluación, gestión y vigilancia de manera autónoma, utilizando mecanismos de verificación **independientes** a los reportes que proporcione el proveedor, bajo la siguiente metodología:

Validación Tecnológica Independiente (Cimiento del Control): Para no depender exclusivamente de los informes del contratista, el BIESS —a través de sus equipos técnicos de monitoreo de infraestructura y la Dirección de Seguridad Informática— implementará y consumirá herramientas propias y de terceros para auditar de forma externa el cumplimiento de las condiciones contractuales:

- **Monitoreo Perimetral Externo:** El Administrador utilizará las herramientas institucionales de monitoreo de disponibilidad (*pings* continuos, pruebas sintéticas de carga y escaneos lógicos) para verificar de manera independiente el tiempo de respuesta y la disponibilidad del *Housing* y de las IPs públicas asignadas.
- **Auditoría de Logs en Tiempo Real:** El proveedor se encuentra obligado a brindar las facilidades técnicas para derivar en tiempo real los registros (*logs*) de auditoría generados por el Firewall, WAF, DDoS y balanceador hacia el repositorio centralizado o consola interna del BIESS. El personal técnico del banco extraerá y auditará estos datos para contrastar la efectividad de las firmas, parches aplicados y bloqueos reportados.
- **Monitoreo:** El BIESS medirá de forma independiente la disponibilidad de sus canales electrónicos (PQ, PH y Prendarios) correlacionando de forma directa las ralentizaciones o alertas internas con las caídas o degradaciones del servicio de balanceo o WAF gestionado por el tercero.

Gestión de Pruebas de Contingencia Co-administradas: El Administrador de Contrato ejecutará de forma conjunta con el proveedor, al menos dos (2) veces al año, las pruebas integrales de Continuidad del Negocio y activación del Plan de Recuperación ante Desastres (DRP) hacia el

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	Página 17 de 55
	UNIDAD REQUIRENTE: COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

Sitio Alternativo de Quito, evaluando de forma independiente si el contratista cumple con el umbral de contingencia operativa y continuidad tecnológica.

OTRAS CONSIDERACIONES PARA LA CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER

1. En caso de que el BIESS requiera finalizar el uso de un servicio, la institución notificará al contratista, el cual dispondrá de 15 días calendario para elaborar el Método de Procedimiento (MOP), realizar los respaldos necesarios (en caso de que el BIESS lo requiera) y ejecutar la ventana de mantenimiento. Al finalizar el plazo se dejará de facturar por el servicio revocado. Todos los servicios solicitados en el presente proceso son bajo demanda, por lo tanto, la entidad contratante se reserva el derecho de finalizar cualquiera de ellos cuando deje de necesitarlo.
2. En el caso de requerir funcionalidades adicionales que soportan los equipos de los servicios gestionados y que sean requeridos por la institución, el Administrador de Contrato notificará al contratista, el cual dispondrá de máximo 15 días calendario para realizar la factibilidad técnica. Informe que será presentado al Administrador de Contrato para su aprobación. El contratista dispondrá de hasta 60 días calendario dependiendo de la complejidad para elaborar el Método de Procedimiento MOP (El MOP será elaborado solamente en caso de que la complejidad del servicio lo requiera), implementar el servicio y ejecutar la ventana de mantenimiento para puesta en marcha siempre y cuando se cuente con la autorización del Administrador de Contrato del BIESS. Terminada esta implementación, el contratista notificará al Administrador de contrato, el cual realizará la verificación y buen funcionamiento del nuevo servicio.
3. En el caso de requerirse nueva infraestructura se ubicará en los racks, el Administrador de contrato notificará y acompañará al contratista, el cual verificará la existencia del espacio adecuado en los racks y notificará al Administrador de Contrato el espacio asignado con las tomas requeridas para energización y puertos de red. El BIESS entregará el nuevo equipamiento al contratista mediante la firma de acta entrega recepción del equipo que ingresará al Data Center correspondiente y realizará la actualización del inventario. Esta actividad no tendrá costo para el BIESS.
4. En el caso de requerirse el desmontaje de equipamiento, el BIESS solicitará al contratista y este se encargará del desmontaje y embalaje del equipamiento con acompañamiento de técnicos del BIESS, terminado este procedimiento se elaborará la respectiva acta entrega/recepción y remitirá el inventario actualizado al Administrador de Contrato. El contratista deberá sustituir el espacio libre con Blanking Panels. Esta actividad no tendrá costo para el BIESS.
5. Si el BIESS requiere tener acceso en tiempo real a la información de logs de los servicios, el proveedor debe brindar las facilidades y realizar las configuraciones para la integración con equipos de propiedad del BIESS o de terceros.
6. Servicio de Monitoreo proactivo de seguridad el mismo que se encuentra enfocado en el monitoreo de suplantación de identidad en el internet, con lo cual, el proveedor puede realizar búsquedas asociados a palabras clave que identifiquen al BIESS con el fin de alertar y

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	Página 18 de 55
	UNIDAD REQUIRENTE: COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

posteriormente tomar acciones (ya sea por el proveedor o por el BIESS) para evitar una posible suplantación de identidad que afecte a la ciudadanía.

2.6 INFORMACIÓN QUE DISPONE EL BIESS:

El BIESS cuenta actualmente con su infraestructura y servicios alojados en los Centros de Datos de la empresa Telconet. El Data Center Principal se encuentra ubicado en la ciudad de Guayaquil en el sector de la Prosperina (Junto a la ESPOL).

El Data Center Alterno se encuentra en la ciudad de Quito en la calle De los Aceitunos E5-85 y Av. Eloy Alfaro.

El BIESS prestará todas las facilidades necesarias para obtener la información técnica que se dispone para la ejecución del contrato, previa suscripción de los acuerdos de confidencialidad el BIESS entregará al menos:

- El inventario de la infraestructura tecnológica ubicada en los Datacenter.
- Diagramas de la infraestructura tecnológica.
- Diagramas de port mapping.
- Estado actual de las configuraciones de FW, WAF, Balanceador de Carga, DDos
- Diagramas de aplicaciones del BIESS

2.7 PRODUCTOS O SERVICIOS ESPERADOS:

A continuación, se detalla de forma macro los ítems generales esperados a recibir en el proceso contractual denominado “CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER”

ÍTEM	SERVICIO	CANTIDAD	UNIDAD	CARACTERÍSTICA TÉCNICA
HOUSING CENTRO DE DATOS				LAS CARACTERÍSTICAS TÉCNICAS SON DETALLADAS EN EL SIGUIENTE CUADRO
1	Centro De procesamiento de Datos Principal (Guayaquil) y Componentes (RACK).	4	UNIDAD (SERVICIO RACK)	
2	Centro de procesamiento de datos alterno (Quito) y componentes (RACK)	2	UNIDAD (SERVICIO RACK)	
3	Interconexión LAN CPDP – CPDA (100Mbps)	1	UNIDAD (ENLACE)	
4	Cintoteca CPDP	1043	UNIDAD (SERVICIO)	
5	Servicio de horas de manos remotas	2	UNIDAD (SERVICIO)	
6	Servicio de mailling(Antispam), dominio biess.info.ec	1	UNIDAD (SERVICIO)	
7	Servicio de Seguridad Perimetral (Next Generation Firewall)	1	UNIDAD (SERVICIO)	
8	Servicio de Balanceo de Aplicaciones	1	UNIDAD (SERVICIO)	

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO		Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER		Página 19 de 55
UNIDAD REQUIRENTE:		COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

9	Servicio de Web Application Firewall (WAF)	1	UNIDAD (SERVICIO)
10	Servicio de DDoS	1	UNIDAD (SERVICIO)
11	Servicio de Storage (STaaS), capacidad 10TB	10TB	SERVICIO ESPACIO DE ALMACENAMIENTO
12	Servicio de Backup (BaaS), capacidad de 50 TB	50TB	SERVICIO ESPACIO DE ALMACENAMIENTO
13	Servicio de Deep & Dark Web (1 dominio)	1	UNIDAD (SERVICIO)
14	Servicio de Brand Protection (1 dominio)	1	UNIDAD (SERVICIO)
15	Servicio de Data Leakage (1 dominio)	1	UNIDAD (SERVICIO)
SERVICIOS BAJO DEMANDA ***			
16	Puntos de red cobre	30	UNIDAD (SERVICIO)
17	Puntos de red fibra a 1GB	5	UNIDAD (SERVICIO)
18	Puntos de red fibra a 10GB	5	UNIDAD (SERVICIO)
19	Cintas (Espacio en cintoteca)	738	UNIDAD (SERVICIO)
20	Servicio de Storage (STaaS), capacidad 59 TB	59TB	SERVICIO (ESPACIO DE ALMACENAMIENTO)
21	Servicio de Backup (BaaS), capacidad de 39 TB	39TB	SERVICIO (ESPACIO DE ALMACENAMIENTO)
*** LOS ÍTEMS LISTADOS CORRESPONDIENTES A LOS SERVICIOS BAJO DEMANDA, ÚNICAMENTE SERÁN EJECUTADOS, PREVIA AUTORIZACIÓN DEL ADMINISTRADOR DE CONTRATO Y DE ACUERDO A LA NECESIDAD INSTITUCIONAL Y FACTURADOS POSTERIOR A CONFIRMACIÓN DE LA NECESIDAD DE LOS MISMOS POR PARTE DEL BIESS, SERVICIOS QUE ESTARÁN VIGENTES POR 5 MESES.			

A continuación, los detalles de las especificaciones técnicas son:

1. CENTRO DE PROCESAMIENTO DE DATOS PRINCIPAL (Guayaquil)	
2. CENTRO DE PROCESAMIENTO DE DATOS ALTERNO (Quito)	
Categoría y ubicación de los data centers	TIER III o superior tanto para el Data Center Principal (DCP) en Guayaquil y el Data Center Alterno (DCA) en Quito. El proveedor deberá demostrar documentadamente, ser propietario de la Infraestructura de Data Center, de Guayaquil y Quito.
Estándares Internacionales	Los Data Center deberán cumplir con todos los estándares de la industria de TI basado en la certificación mínimo de TIER III o superior del Uptime Institute.
	El proveedor deberá presentar al menos una certificación en diseño, construcción u operación, por cada uno de los data centers.
Ubicación física	El DCP se ubicará en la ciudad de Guayaquil, y el DCA, en la ciudad de Quito.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

Energización	Todo el equipamiento rackeado debe estar energizado correctamente y deberá soportar la carga eléctrica demandada por el equipamiento tecnológico.
	El contratista deberá incluir las PDU, regletas y conectores necesarios para energizar el equipamiento alojado.
	El servicio de housing debe garantizar que los equipos a ser alojados en los DCP y DCA contarán con sistemas redundantes mínimo tipo N+1 para suministro de energía eléctrica, a través de generadores y UPS.
	El reporte mensual del contratista deberá incluir el consumo eléctrico de cada rack en referencia a la capacidad instalada
Sistemas de Enfriamiento	Sistema de enfriamiento redundante mínimo tipo N+1.
	Sistema de climatización mediante pasillos fríos/calientes, con pasillo frío auto contenido.
Sistemas de detección de incendio	Debe disponer de sistema de detección temprana, detección convencional y extinción de incendios.
	El sistema de extinción de incendios debe estar basado en agentes no contaminantes y que no afecten el funcionamiento de los equipos ni a las personas.
Sistemas de control de accesos	Sistemas de seguridad para el acceso con al menos 5 niveles de protección de acceso, desde el control de ingreso del personal hasta la jaula o POD del BIESS (DCP y DCA).
	Seguridad Física a través de sistemas de video vigilancia, control de acceso con tarjeta de proximidad o biométrico, y personal de seguridad.
	El contratista debe garantizar el acceso al personal técnico del BIESS o sus contratistas, en un esquema 7x24x365, para la administración y gestión de equipos alojados en modo housing.
Sistema ATS (Automatic Transfer Switch)	Proveer mínimo de 2 ATS (1 en el Data center de Guayaquil y 1 en el Data Center de Quito) de energía eléctrica de 110V con 6 tomas mínimo, que se instalarán en los racks dentro del Espacio contratado que el BIESS indique, los cuales se utilizarán para conectar equipos que cuenten con una sola fuente de poder, indicados previamente por el BIESS
Disponibilidad	La disponibilidad que deben brindar los Data Centers es de mínimo 99,982% en modalidad 7x24x365 para servicio de Housing.
Servicio de Infraestructura de Red	El contratista debe contar en el DCP y DCA, con equipos de red que proporcionen al BIESS los servicios de conectividad. La red de data center del proveedor debe estar diseñada e implementada en un marco de redes de última generación, conforme a las tendencias de la industria.
	A fin de gestionar los servicios publicados del BIESS, se requiere un pool de al menos 96 direcciones IP públicas.
	El contratista deberá implementar la topología que demande el BIESS mediante esquemas redundantes, y que garanticen altas velocidades, estabilidad, escalabilidad, disponibilidad, seguridad, segmentación del networking interno, conectividad entre racks y la interconexión a los enlaces de datos e internet para los equipos a ser alojados.
	Los servicios de conectividad serán administrados por el contratista bajo las necesidades y lineamientos del BIESS.
	El contratista deberá proveer de todo el equipamiento de networking y demás elementos requeridos para garantizar la conectividad de toda la infraestructura del BIESS en el data center, entre data centers y sus oficinas remotas por medio de los contratistas de enlaces de datos.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 21 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

	La red debe asegurar una topología libre de loops, sin la utilización de protocolos que introducen inestabilidad y complejidad, entregando, conexiones seguras, estables y consistentes, además debe soportar la conectividad a dependencias que demande el BIESS.
	Se debe asegurar una arquitectura global del centro de datos que soporte avanzados mecanismos de calidad de servicio (QoS) para priorizar tráfico, para el transporte de diferentes aplicaciones como real time, sistemas de misión crítica, storage traffic tanto en el Fabric como en la interconexión con la WAN y LAN.
	La configuración de switches CORE del contratista serán independientes de otros clientes, para ello se configurará un tenant exclusivo para el BIESS o el que aplique según la tecnología.
	El contratista deberá proveer de puntos de red para la conexión de todo el equipamiento conforme la tecnología ethernet y velocidades que requieran para su normal operación.
	El contratista deberá mantener el direccionamiento y segmentación IP que tiene el BIESS en la actualidad.
	Se debe brindar servicio de interconexión para permitir la conectividad hacia la infraestructura alojada en el Centro de Datos del contratista, con otro contratista de servicios externo tipo carrier, por lo que se deberá proveer de al menos de dos mangas para el acceso de la fibra de otros proveedores en cada data center.
Jaula o PODs para Racks	Los racks requeridos para los DCP y DCA, deben estar dentro de jaulas o PODs para alojamiento de equipamiento y de racks exclusivos para el BIESS, por lo cual, el acceso a las mismas debe ser asegurado con un sistema de tarjeta de proximidad o biométricos.
Rackeo de equipos	El rackeo de equipos y el cableado debe cumplir con estándares de la industria para etiquetado, distribución, instalación de cableado, así como rackeo de equipos.
	El contratista debe proveer como parte del servicio de Housing, los Blanking Panels para cubrir todos los espacios libres donde no se alojen equipos, en todos los racks requeridos en el servicio de Housing y en función de la distribución de equipos establecida por el BIESS, con el fin de evitar el retorno de aire caliente.
	El contratista debe proveer como parte del servicio de Housing, de organizadores de acuerdo con la necesidad de la organización (peinado) de los cables de cobre y fibra para los racks asignados.
Espacio de Racks	Todas las unidades de rack deben ser utilizables.
	El contratista deberá proporcionar espacio en jaula mínimo de 4 (cuatro) Racks de 42 U tipo gabinete para servidores en el DCP y un espacio de jaula mínimo de 2 (dos) racks de 42 U en el DCA, exclusivos para el BIESS, que incluya mecanismos de seguridad física y lógica.
	El DCP debe contar con un espacio vacío adicional dentro de la jaula o pod equivalente a un rack de 42 unidades para ubicar un sistema de librería TS3500 del BIESS

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	Página 22 de 55
	UNIDAD REQUIRENTE: COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

	El DCA debe contar con un espacio vacío adicional dentro de la jaula o POD, de dimensiones aproximadas a un rack de 42 unidades para ubicar un armario para almacenamiento de cintas del BIESS.
	El contratista deberá realizar la organización de nuevos equipos basada en las mejores prácticas y distribución uniforme de energía.
	En base a la necesidad el BIESS podrá aumentar o disminuir espacios físicos de rack en las jaulas, para lo cual el proveedor deberá realizar el respectivo peinado y organización en el rack intervenido
	Los racks deberán contar con los patch panels necesarios para interconexión de acuerdo a la topología y ubicación de los equipos del BIESS.
3. INTERCONEXIÓN LAN CPDP – CPDA (100MBPS)	
	Se requiere la provisión y gestión de un canal o enlace de conectividad LAN to LAN para la conexión de los 2 Data center (Tipo L2), y mantener los mismos direccionamientos IP con la propagación de todas las VLANs definidas por el BIESS en ambos data centers. Con un ancho de banda de al menos 100Mbps.
4. CINTOTECA CPDP	
	Espacio en Cintoteca para mínimo 1043 cintas en el Data Center de la ciudad de Guayaquil
	Las cintas deberán estar vigiladas por una cámara de seguridad, con una retención videos por el lapso de al menos 3 meses.
	Los videos deberán ser entregados en medio digital cada mes, como parte del servicio
	El contratista será responsable de realizar los ingresos y retiros de cintas desde las librerías hacia la cintoteca o viceversa de acuerdo a las solicitudes del BIESS. De igual manera, de la recepción de nuevas cintas.
	Estas interacciones no serán cargadas al servicio de manos remotas y serán parte del servicio.
	El Biess Cancelará por la cantidad de cintas alojadas en la cintoteca
5. SERVICIO DE HORAS DE MANOS REMOTAS	
Soporte Técnico	El Centro de Datos Físico deberá brindar soporte técnico especializado en un esquema de 24x7x365 en los componentes y servicios del Centro de Datos de acuerdo con el SLA establecido.
	El contratista asignará al menos un técnico VIP por cada Centro de Datos, mismo que se encargará de la gestión y atención rápida de los requerimientos técnicos solicitados por el BIESS.
	El contratista deberá disponer de canales de soporte para solicitar servicio de asistencia y jerarquización de problemas y fallos.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	Página 23 de 55
	UNIDAD REQUIRENTE:	
	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

Servicio de manos remotas	El oferente debe proporcionar bajo demanda el servicio de manos remotas en un esquema 24x7x365, que incluirá realizar tareas simples, que incluyan: • Reseteo del equipo o reseteo de tarjetas, • Descripción y reporte de indicadores (display) de los equipos o consolas, • Conexiones sencillas. • Rackeo y/o desrackeo de equipos. • Observación básica del entorno. • Gestión básica de cables de red y eléctricos. Para ello el BIESS entregará las actividades que deberá ejecutar el contratista por cada evento requerido.
	Cada interacción será definida por intervalos de duración de 15 minutos.
	Se requiere un pool de horas de 24 horas por año de servicio, lo que corresponde a 2 horas mensuales.
	El pago se realizará por horas completadas de 60 minutos.
	En el caso de los servicios gestionados, serán administrados por el contratista y remitirá al BIESS reportes de incidentes, funcionamiento, estadísticas de uso, informes, boletines de seguridad de manera periódica según lo requiera el BIESS.
	La administración de estos servicios implica según corresponda el manejo total de la tecnología incluida la gestión de requerimientos, el contratista deberá atender en cumplimiento del SLA todas las solicitudes realizadas por el BIESS.
	El contratista entregará a la firma de contrato el procedimiento para apertura de tickets y los niveles de escalamiento conforme lo solicitado en las especificaciones técnicas.
6. SERVICIO DE MAILING (Antispam), dominio biess.info.ec	

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 24 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

	Se requiere proteger el servicio de correo electrónico de notificaciones del BIESS, con un Sistema Antispam que debe funcionar detectando y alertando a la entidad de manera proactiva un incidente ante la presencia de correos Spam que afecten al servicio de mail. El equipo deberá operar en cualquiera de las siguientes modalidades: • Modo Gateway • Modo Transparente • Modo Servidor Disponer de certificación “VBSpam” de Virus Bulletin que mide el porcentaje de captura de spam vs el porcentaje de falsos positivos, el cual verifica si la solución anti-spam es capaz de: • Bloquear un gran porcentaje de correos electrónicos en un tráfico real de spam. • Una correcta identificación de todo spam, en un tráfico real donde existen correos electrónicos legítimos. Escuchar Leer fonéticamente Diccionario – Debe ser capaz de proteger correo electrónico entrante (desde Internet) y correo saliente (hacia Internet) en el protocolo SMTP. • Permitir la conexión en tiempo real a una base de datos centralizada en el fabricante para descargar actualizaciones de Antispam de forma continua. Protección contra ataques de denegación de servicio (DoS) y ataques de directorio. • Verificaciones de DNS reverso para proveer protección tipo anti-spoofing (anti-engaño) de fuentes válidas de correo. • Debe proveer mecanismos de identificación basados en un servicio de reputación global provistos por el Fabricante, capaz de rechazar conexiones SMTP desde fuentes no confiables y evitar así gran cantidad de tráfico basura, es decir, tener la capacidad de limitar conexiones SMTP a servidores no confiables o de mala reputación. • Lista de la reputación del remitente local con base en: - o Número de correos con virus - o Cantidad de correo no deseado - o Número de destinatarios inválidos o no existentes. • Posibilidad de definir listas blancas/negras por dominio o cuentas específicas, IP's públicas, listas de terceros, capacidad de prevenir ataques de virus y ataques de directorio. • Capacidad de aseguramiento para el envío masivo de correo de tipo notificaciones de al menos una transaccionalidad de 280.000 mails diarios.
7. SERVICIO DE SEGURIDAD PERIMETRAL (Next Generation Firewall)	
	Se requiere contar con el servicio de seguridad perimetral (Firewalls), que permita el aseguramiento de la red para la infraestructura del BIESS. Características Generales El servicio deberá contar con al menos las siguientes capacidades y/o funcionalidades: Firewall (QoS, NAT/PAT) Filtrado Web IPS/IDS, Antivirus /AntiMalware /Antibot IPsec VPN VPN SSL Protección DNS Soporte del fabricante. El servicio deberá ser provisto con equipamiento de marca que conste en el cuadrante de Gartner como líder durante al menos los últimos tres años previos a la fecha de publicación del presente proceso. Los equipos firewall deben contener la última versión de software estable lanzado por el fabricante. Debe permitir derivar los registros (logs) hacia la solución de reportería y correlación de eventos de la misma marca del firewall.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 25 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

	Módulo IPS Inspección profunda de paquetes, incluido el tráfico encriptado con el último TLS. Actualizaciones de firmas diarias de protección, automáticas provistas por el fabricante. Capacidad de contar con varios perfiles de protección personalizados, para protección de servicios específicos de la red.
	Filtrado Web
	Control de aplicaciones WEB.
	Integración con directorio activo para controles por usuarios, grupos, y/o equipos.
	Actualizaciones continuas de bases de datos por el fabricante u otras fuentes
	Categorización manual o personalizable de sitios web y/o aplicaciones.
	Controlar el acceso al contenido web bloqueando páginas web que contengan palabras o patrones específicos, mediante el uso de comodines, expresiones regulares, etc.
	Optimiza el uso del ancho de banda en la red al priorizar, despriorizar o bloquear el tráfico según la aplicación.
	Inspección de tráfico HTTPS
	Antivirus/AntiMalware/AntiBot
	Antivirus perimetral para protección de amenazas y ataques informáticos.
	Protección contra los últimos virus, spyware y otras amenazas conocidas a nivel de contenido.
	Motores de detección avanzados para detener malware conocido y polimórfico.
	Prevenir ataques exitosos a través de múltiples vectores de amenaza.
	Actualizaciones de bases de datos diarias del fabricante.
	Realiza la detección posterior a la infección de bots en hosts.
	Previene los daños de los bots al bloquear las comunicaciones de C&C (Comando y control) de los bots.
	Se actualiza continuamente desde una red colaborativa para combatir el cibercrimen.
	IPsec VPN y VPN SSL
	Capacidad para creación de VPN tipo IPSEC
	Se requiere de al menos 800 usuarios concurrentes VPN SSL BIESS, sin costo adicional para la institución.
	Red
	Los equipos del servicio de manera individual deben contar con al menos el siguiente Performance:
	- IPS Throughput: 13 Gbps
	- GW: 80 Gbps
	La solución debe soportar un throughput de prevención de amenazas de mínimo 7 Gbps medido con todas las características activadas.
	El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links
	802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	Página 26 de 55
	UNIDAD REQUIRENTE: COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

	El contratista deberá dimensionar las interfaces físicas que se requiera y con base en las mejores prácticas del fabricante y velocidades de operación a nivel de red.
	Consola de administración
	Consola de administración de los equipos, misma que puede estar embebida en los firewalls o en un equipo diferente, appliance físico o virtual. En este caso, la consola de administración debe contar con el licenciamiento para uso, actualizaciones y soporte de fabricante durante el tiempo que dure el servicio.
	Log y Correlacionador
	La solución debe permitir almacenar por al menos 6 meses los logs generados por el firewall, correlacionar eventos y generar reportes automáticos (al menos 3) y bajo demanda.
	Los registros logs deben ser trasladados a un repositorio externo una vez que el disco del equipo de logs requiera liberar su espacio y serán almacenados por todo el tiempo que dure el contrato, y serán entregados al BIESS
	Los logs generados por el firewall son de propiedad exclusiva del BIESS y no podrán ser copiados, modificados o eliminados por el contratista para otros fines.
	Licenciamiento
	El servicio de seguridad perimetral (firewalls) deberá contar con licenciamiento de todas las características señaladas en las especificaciones y su vigencia será la misma del tiempo del contrato.
	En caso de solicitarse más características que soporten los firewalls, el contratista será encargado de agregar licenciamiento y adecuación del servicio, según lo indicado en las especificaciones generales y la metodología de trabajo.
	Otras Consideraciones
	El servicio de seguridad perimetral (firewall) deberá brindar la protección de la red LAN, WAN y DMZ del BIESS
	El contratista se encargará de realizar al menos 2 mantenimientos anuales de software sobre el servicio de seguridad perimetral (firewall). Por lo que el contratista instalará los parches de seguridad recomendados por el fabricante y en el caso de actualizaciones o upgrades de sistema operativo, se realizará siempre y cuando sea recomendado por el fabricante. Todas las operaciones de updates y upgrades serán aprobados por el BIESS.
	De ser requerido, el personal autorizado por el BIESS podrá solicitar al contratista (sin costo alguno extra), que realice configuraciones en los equipos que conforman el cluster, referente a reglas de: Firewall, NATs/PATs, control de navegación, VPN SSL, VPN IPSec, AntiBot, activación/configuración de funcionalidades propias que se encuentren licenciadas en el servicio.
	El contratista deberá realizar respaldos periódicos diarios de las configuraciones y políticas del firewall. Los respaldos deberán ser almacenados en un repositorio propio del contratista y también se entregará una copia al BIESS para su almacenamiento.
	La herramienta será administrada en conjunto por el contratista y el personal del BIESS, sin embargo, el contratista no podrá realizar ningún cambio de configuraciones, políticas, afinamientos, sin consentimiento del área responsable del BIESS.
	El contratista llevará una bitácora de cambios realizados sobre las políticas y/o configuraciones y será presentada de manera mensual al BIESS.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 27 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

	Las políticas de firewall serán de uso exclusivo para el BIESS y no podrá contar con reglas, configuraciones u objetos para uso de terceros.
	Las reglas de firewall serán creadas siguiendo las buenas prácticas, con nombres de reglas estandarizadas, comentarios y demás parámetros que sean necesarios para este fin.
	El contratista deberá garantizar el buen funcionamiento de la solución, sin que se generen congestión de tráfico, sobre procesamiento de recursos u otros problemas que puedan generar un bajo performance de la solución.
	Servicio de Administración bajo los tiempos establecidos en el documento SLA
	De ser el caso el BIESS, podrá solicitar al contratista la reestructuración de las reglas configuradas en los diferentes módulos/blades que posee el firewall.
	De ser el caso el BIESS, podrá solicitar al contratista que realice una rearquitectura que involucre la conectividad de las diferentes vlans que convergen a los equipos que conforman el cluster y que se encuentran dentro de la LAN, WAN y DMZ del BIESS
	El contratista entregará al menos 5 usuarios nombrados con el rol de auditor con permisos de lectura únicamente para monitoreo de la solución, así como los accesos a los Dashboard generados para este servicio (modo visualización).
	El contratista entregará al BIESS la reportería de forma mensual y bajo demanda del servicio.
Contingencia.	Los servicios especializados pueden ser provistos en el sitio principal o en el sitio alterno, de acuerdo a la necesidad del BIESS.
Actualizaciones	Los servicios especializados provistos por el proveedor, deben pasar por el mantenimiento, actualizaciones o gestión de cambios, con base en las mejores prácticas, con el fin de garantizar la continuidad de los servicios.
8. SERVICIO DE BALANCEO DE APLICACIONES	
	CARACTERÍSTICAS FÍSICAS Y DE RENDIMIENTO
	Se requiere contar con el servicio de balanceo de aplicaciones
	Disponibilidad: El servicio deberá tener la posibilidad de detectar y compensar la sobrecarga de solicitudes a los servidores para no evidenciar lentitud y/o indisponibilidad de servicio.
	Throughput: La solución debe soportar al menos un Throughput Nominal de 1 Gbps para balanceo en condiciones de máxima carga.
	Crecimiento Throughput: Los equipos ofertados deben tener la Capacidad de crecimiento a por lo menos 2 Gbps por licenciamiento sin necesidad de cambiar/modificar el equipo.
	Peticiones HTTP x segundo: La solución debe soportar al menos 200.000 HTTP request por segundo.
	Crecimiento Peticiones HTTP x segundo: La solución debe tener la capacidad de crecimiento sin necesidad de cambiar el modelo/sistema, para soportar mínimo 300,000 HTTP request por segundo.
	FUNCIONES DE ADMINISTRACIÓN DE TRÁFICO
	Balanceo de Tráfico: La solución ofertada deberá realizar funciones de Balanceo de Tráfico de aplicaciones basadas en IP (TCP, UDP) y Servicios Web.
	Algoritmos balanceo: La solución debe permitir hacer control de balanceo de tráfico local con varios tipos de algoritmos especializados definidos en la solución de balanceo:
	• Round Robin

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	Página 28 de 55
	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	
UNIDAD REQUIRENTE:		

	• Respuesta rápida
	• Conexiones mínimas
	• Análisis de carga
	• Hash de URL
	Monitoreo Servidores: La solución debe realizar monitoreo de la salud de los Servidores que gestione el equipo de Balanceo de tráfico, por medio de:
	• Ping.
	• Chequeo a nivel de TCP y UDP a puertos específicos
	• Monitoreo HTTP y HTTPS
	• Verificación de la salud de una combinación de servicios, permitiendo tomar la decisión del estado de salud aplicando varios monitores simultáneos.
	• Configurar monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red.
	• Monitoreo en línea, donde el funcionamiento de la aplicación determine el estado de salud de la misma.
	Monitoreo Aplicaciones: La solución deberá soportar mínimo el Monitoreo de aplicaciones/protocolos del mercado: LDAP, FTP, DNS, SMTP, POP3, RADIUS, SIP, SNMP.
	Persistencia conexiones: Deberá permitir hacer persistencia de conexiones hacia la aplicación con base en cualquier información contenida en cualquier parte del paquete completo, esto para poder adaptar la solución a las necesidades de las diferentes aplicaciones. El control de persistencia de las conexiones se debe realizar por los siguientes métodos:
	• Dirección IP origen
	• Dirección IP destino
	• Cookies
	• SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia
	• Sesiones SSL
	FUNCIONES DE ACCELERACIÓN DE TRÁFICO
	Compresión: La solución debe ofrecer Características de Compresión de tráfico a nivel de aplicaciones:
	• El sistema deberá permitir compactar el tráfico http a través del estándar GZIP, Deflate y compatible con browsers MS Internet Explorer, Google Chrome, Mozilla Firefox, Safari, etc.
	• Debe incluir compresión de tráfico con capacidad de crecimiento
	FUNCIONES DE SEGURIDAD
	Seguridad SSL: La solución debe incluir el soporte de Aceleración SSL:
	La solución debe soportar al menos 3.000 transacciones por segundo
	Compatibilidad para conexiones SSL con claves de 2048 y 4096 bits con capacidad de crecimiento por licenciamiento hasta de 5.000 sin necesidad de cambiar el equipo
	Encriptación: La solución ofertada debe manejar mínimo AES256; SHA1/MD5 y soporte a algoritmos de llave pública: RSA, Diffie-Hellman
	ADMINISTRACIÓN DEL SISTEMA

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 29 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

	CLI, WEB: La solución debe permitir el acceso para la administración de la solución vía CLI
	(Interfaz de línea de comandos) por SSH2, interfaz de administración gráfica basada en Web seguro (HTTPS)
	REPORTES Y VISIBILIDAD
	Reportes: La solución debe permitir dar visibilidad del balanceo del tráfico web, para identificar las aplicaciones más utilizadas, las URLs accedidas, los usuarios con más accesos y los servidores más requeridos.
	Se debe entregar al menos 5 usuarios para monitoreo y lectura al BIESS.
	Visibilidad:
	La herramienta que forme parte de la solución debe proporcionar la información de manera gráfica, de tal forma que permita identificar de manera más rápida y oportuna, alguna falla/anomalía en la entrega del servicio al usuario final.
	La solución ofertada debe disponer de una consola de administración centralizada en donde se puedan ver y administrar los equipos que se encuentren en el ambiente de la entidad.
	Soportar las últimas versiones de TLS y SSL
	SOPORTE PARA BALANCEADO DE APLICACIONES LEGACY
	Debe soportar la publicación de las actuales aplicaciones legacy del BIESS, que trabajan con TLS v1 y v1.1.
	El contratista deberá garantizar el buen funcionamiento de la solución, sin que se generen congestión de tráfico, encolamiento, sobreprocesamiento de recursos u otros problemas que puedan generar un bajo performance de la solución.
	METODOLOGIA: El BIESS entregará el listado de aplicaciones, las cuales deberán ser configuradas por el contratista para el balanceo de carga.
	El contratista entregará al administrador de contrato la reportería de forma mensual y bajo demanda del servicio.
Contingencia.	Los servicios especializados pueden ser provistos en el sitio principal o en el sitio alternativo, de acuerdo a la necesidad del BIESS.
Actualizaciones	Los servicios especializados provistos por el proveedor, deben pasar por el mantenimiento, actualizaciones o gestión de cambios, con base en las mejores prácticas, con el fin de garantizar la continuidad de los servicios.
9. SERVICIO DE WEB APPLICATION FIREWALL (WAF)	
	Características Generales
	Servicio de Firewall de Aplicaciones Web
	Tener características de by-pass o conmutación automática en caso de falla, permitiendo de esta manera la continuidad del servicio.
	Contar con los puertos Ethernet necesarios, que soporten el correcto funcionamiento de los componentes.
	Debe soportar al menos 10 sitios del BIESS.
	Ser escalable en caso de la institución lo requiera.
	Detallar el procedimiento para el escalamiento de los componentes.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 30 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

	Presentar una arquitectura que permita definir un nivel de contingencia en caso de que se presente un incidente en los componentes, considerando que no debería impactar en el funcionamiento de las aplicaciones y que por la criticidad de los servicios debe recuperarse en un tiempo no mayor a 2 horas.
	Características Específicas
	Mantener características de proxy reverso para que por medio de una misma IP y puerto poder exponer varios servicios/sistemas
	Soportar aplicaciones WEB desarrolladas al menos en lenguajes java, php, html, con servidores de aplicaciones JBOSS, Tomcat, apache, etc.
	Soportar el bloqueo de las transacciones cuyo contenido corresponde a las firmas de los ataques conocidos, dejando pasar todo lo demás.
	Soportar la detección basada en el Modelo de Seguridad Negativa (modelo explícito basado en firma de ataques conocidos).
	Adicionar y/o modificar las firmas a través del usuario administrador.
	Actualizar de forma automática, por medio de una base de conocimiento propia o de terceros de las firmas de ataques, con el objetivo de mantenerse al día, respecto de las últimas amenazas.
	Detectar ataques multi-nivel incluyendo, red, sistema operativo, Web Server Software, y ataques en la capa de aplicación.
	Incluir técnicas utilizadas dentro del estándar OWASP to 10.
	Contar con un modo de aprendizaje dinámico que permita definir cuáles son las acciones esperadas y aceptadas para los usuarios que utilizan las aplicaciones. Si estas operaciones no están contempladas en lo que se espera como "normal" debe alterar y/o bloquear.
	Contar con políticas de seguridad pre-configuradas de acuerdo a las mejores prácticas de seguridad en aplicaciones WEB que le permitan a la entidad proteger de una forma sencilla las aplicaciones desde el primer momento de la implementación de la solución.
	Detectar la estructura y elementos de la aplicación, esta información podrá ser utilizada para la configuración del modelo positivo de seguridad.
	Incluir un proceso de aprendizaje dinámico de tal forma que se tenga una línea base que considere mínimo los siguientes elementos de la aplicación: Host válidos, URLs, métodos sin importar si su origen es sobre protocolos.
	Preservar la integridad de conexiones entre cliente y el servidor (no permitir modificaciones de conexiones) y asegurar que los paquetes sean los mismos antes y después de ser analizados por el WAF.
	Definir reglas para el modelo de seguridad positivo o negativo y permitir la creación de reglas de correlación con múltiples criterios.
	Proteger las aplicaciones que utilicen protocolos http y https.
	Descifrar el tráfico SSL, de las aplicaciones web cliente-servidor y reencriptarlo antes de su reenvío.
	Descifrar el tráfico SSL para inspección en los modos: puente o sniffer. Sin terminar o cambiar la conexión.
	Contar con protección para rastrear e identificar las fuentes de ataques originadas desde proxies anónimos, direcciones IP maliciosas, botnets, y sitios de phishing.
	Permitir ajustar las fuentes de ataque para identificar y bloquear tráfico considerado malicioso.
	Ajustar dinámicamente las políticas de seguridad con base en la identificación de las fuentes de ataque o de las fuentes que denoten actividad sospechosa.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 31 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

	Bloquear solicitudes de acceso basado en reputación de la fuente del tráfico, como direcciones IP conocidas por su comportamiento malicioso por BotNet, DDoS, Phishing o redes de anonimización.
	El contratista deberá garantizar el buen funcionamiento de la solución, sin que se generen congestión de tráfico, encolamiento, sobreprecesamiento de recursos u otros problemas que puedan generar un bajo performance de la solución.
	El contratista entregará al Administrador de contrato la reportería de forma mensual y bajo demanda del servicio.
Contingencia.	Los servicios especializados pueden ser provistos en el sitio principal o en el sitio alternativo, de acuerdo a la necesidad del BIESS.
Actualizaciones	Los servicios especializados provistos por el proveedor, deben pasar por el mantenimiento, actualizaciones o gestión de cambios, con base en las mejores prácticas, con el fin de garantizar la continuidad de los servicios.
10. SERVICIO DE DDOS	
	Servicio de protección DDoS. Se debe contar con protección contra ataques de denegación de servicio volumétricos que atenten contra la infraestructura del BIESS. Este sistema debe contar con capacidad de contención de ataques volumétricos de hasta 1 Gbps con origen internacional o local. El sistema debe contar con los siguientes requisitos:
	La contención del ataque se debe realizar de forma automática, sin que el servicio se vea afectado
	El sistema Anti DDoS debe funcionar fuera de línea (off-line) con detección basada en flow collector y snmp.
	Tiempos y umbrales de detección personalizables
	Detección de ataques distribuidos.
	El contratista entregará dos usuarios nombrados con el rol de auditor con permisos de lectura únicamente para monitoreo de la solución, así como los accesos a los Dashboard generados para este servicio (modo visualización)
	Este servicio deberá poder ser usado tanto en el Data Center de Guayaquil o en el Data Center de Quito, según la necesidad del BIESS, por lo que el contratista realizará las gestiones necesarias para su provisión.
	El contratista deberá garantizar el buen funcionamiento de la solución, sin que se generen congestión de tráfico, encolamiento, sobreprecesamiento de recursos u otros problemas que puedan generar un bajo performance de la solución.
	El contratista entregará al Administrador de contrato la reportería de forma mensual y bajo demanda del servicio.
Contingencia.	Los servicios especializados pueden ser provistos en el sitio principal o en el sitio alternativo, de acuerdo a la necesidad del BIESS.
Actualizaciones	Los servicios especializados provistos por el proveedor, deben pasar por el mantenimiento, actualizaciones o gestión de cambios, con base en las mejores prácticas, con el fin de garantizar la continuidad de los servicios.
11. SERVICIO DE STORAGE (STaaS), Capacidad 10 TB	
- El contratista deberá proveer el servicio de espacio de almacenamiento (storage) en una nube local privada (Storage as a Service), en el Data Center Principal, con una capacidad mínima de 10 TB; el protocolo de conexión entre el ambiente del BIESS y el servicio de storage será por NFS o S3, mediante una vlan dedicada entre los ambientes del proveedor y el o los ambientes del BIESS. -El almacenamiento deberá estar alojado en infraestructura física ubicada dentro del territorio ecuatoriano, operada directamente por el contratista. No se requiere replicación al Data Center Alterno (DCA). Se deberá asignar un espacio de 1TB en el servicio de StaaS para almacenamiento de videos de cintoteca.	

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	Página 32 de 55
	UNIDAD REQUIRENTE: COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

12. SERVICIO DE BACKUP (BaaS), Capacidad 50 TB
El contratista deberá proveer el servicio de respaldo de datos administrado en la nube local privada (Backup as a Service), con una capacidad mínima de 50 TB, alojado en territorio ecuatoriano. El servicio deberá ser brindado 24x7 incluyendo monitoreo y soporte durante la vigencia del contrato.
- La solución deberá cumplir con las siguientes características técnicas mínimas: - Protección de cargas de trabajo de servidores virtuales desde una única consola centralizada y que sea administrada por la entidad - Definición de políticas de frecuencia y retención configurables por el administrador del BIESS. - Respaldo y recuperación de máquinas virtuales completas para ambiente vmware versión 6.5 y 7.x.

13.SERVICIO DE DEEP & DARK WEB (1 dominio)
El componente de visibilidad en la internet profunda deberá proveer inteligencia accionable mediante los siguientes requerimientos: Infiltración y Monitoreo de Canales Cerrados: Rastreo continuo de menciones de la marca, palabras clave e infraestructura de la institución dentro de foros de cibercriminales, mercados de la Darknet (redes TOR, I2P, Freenet), así como en grupos y comunidades privadas de mensajería instantánea (Telegram, WhatsApp y Discord). Alertas Tempranas de Ransomware y Vulnerabilidades: Notificación inmediata ante campañas coordinadas por grupos de Ransomware activos que identifiquen a la institución o a sus proveedores críticos como víctimas. Servicio De Scraping Con la finalidad de incorporar mecanismos para detectar la copia de los diferentes componentes de los sitios web del BIESS, el servicio deberá incorporar una funcionalidad avanzada de recolección, extracción y procesamiento automatizado de datos procedente de fuentes externas a la red institucional (incluyendo Clear Web, Deep Web y Dark Web), orientada a la identificación proactiva y continua (24/7) de riesgos digitales específicos contra el BIESS, tales como fugas de credenciales de correos institucionales, suplantación de identidad digital de la marca (phishing y typosquatting) y filtración de información confidencial o código fuente." Alertas de Anomalías y Resúmenes con IA Generativa: Capacidad de generar alertas automáticas ante picos inusuales de menciones de la institución (detección de anomalías) y resúmenes ejecutivos utilizando modelos de Inteligencia Artificial Generativa entrenados en el lenguaje del cibercrimen
14. SERVICIO DE BRAND PROTECTION (1 dominio))
El servicio contratado no debe limitarse a la detección, sino que debe garantizar la remediación efectiva de las amenazas externas bajo las siguientes condiciones: Desmantelamiento Multivector: Capacidad de ejecutar solicitudes de remoción efectivas contra portales de <i>Phishing</i>, abuso de marca en anuncios de motores de búsqueda pagados (Google Ads), aplicaciones móviles falsas en tiendas oficiales/no oficiales, ataques de <i>Typosquatting</i> (dominios maliciosos similares) y perfiles falsos en redes sociales principales (Facebook, Instagram, LinkedIn, X, TikTok, YouTube). Garantía de Persistencia (Re-up Protection): Monitoreo continuo post-remediación que asegure que si un contenido malicioso o sitio fraudulento previamente dado de baja vuelve a aparecer en un periodo de al menos quince (15) días, sea detectado y mitigado de forma automática como un re-incidente sin generar costos adicionales. Protección Integral y Detección de Clonación de Sitios Web: capacidad de inspección y rastreo avanzado mediante tecnología de balizamiento digital OnePixel mediante la inserción de un recurso técnico imperceptible y automatizado dentro del código fuente del sitio web oficial
15. SERVICIO DE DATA LEAKAGE (1 dominio)

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 33 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

	El servicio/plataforma deberá cumplir obligatoriamente con las siguientes capacidades de monitorización en tiempo real
	Monitoreo Continuo de Credenciales Corporativas: Capacidad de identificar credenciales institucionales expuestas (dominios específicos de la entidad) provenientes de brechas de datos masivas (<i>Big Leaks</i>) y repositorios públicos o privados.
	Detección de Credenciales por Infostealers: Identificación precisa de credenciales de usuarios, empleados o clientes comprometidas a través de malware especializado de tipo <i>infostealer</i> , recolectando metadatos del contexto de la infección (fecha aproximada, país, IP del equipo infectado y URLs afectadas).
	Detección de Secretos y Llaves de Código: Capacidad de escanear y alertar sobre la exposición involuntaria de llaves de configuración, contraseñas en texto plano, tokens y llaves criptográficas/privadas expuestas en repositorios de código público como GitHub, plataformas de commits o sitios de intercambio de texto (<i>Paste sites</i> como Pastebin, Ghostbin, ControlC, entre otros).
	Validación de Exposición de Bases de Datos: Capacidad de insertar registros o tokens simulados (<i>Tracking Tokens</i>) dentro de las bases de datos de la institución para detectar de manera proactiva si la información interna ha sido filtrada, facilitando el proceso de auditoría y aislamiento de la fuente de la fuga.
	Monitoreo de Datos Sensibles en Almacenamiento Cloud: Vigilancia activa de archivos institucionales o información confidencial expuesta en plataformas colaborativas o repositorios de almacenamiento en la nube.

CONDICIONES GENERALES	
Tiempo del servicio	La duración del servicio deberá ser de 365 días calendario
Responsabilidad	Cualquier inconveniente que pudiera suscitarse por problemas relacionados a los servicios de Data Center (condiciones físicas), será responsabilidad del contratista, para ello debe contar con técnicos especialistas que residan en la ciudad de Quito y Guayaquil respectivamente.
SLA	El Oferente adjudicado deberá entregar el SLA elaborado por el BIESS, firmado previa suscripción del contrato.
Varios	El contratista debe notificar al BIESS las ventanas de mantenimiento programadas para su infraestructura y se comprometerá a notificar con la debida anticipación (no menor a 7 días calendario), indicando los tiempos de inicio, indisponibilidad y finalización de la operación. Como parte del servicio, el BIESS requiere realizar al menos 2 veces al año, Pruebas de continuidad del Negocio u otras pruebas técnicas de contingencia, por lo tanto, se requiere que el contratista del soporte necesario para realizar estas pruebas y activación del Sitio Alterno sin que esto represente un costo adicional para la institución. En caso de que el BIESS requiera de alguna característica que soporten los equipos utilizados de los servicios gestionados, el contratista será encargado de verificar la factibilidad técnica, y configurar el servicio conforme lo indique la metodología de trabajo. Se realizará los ajustes en los valores con base en el valor convenido. Todos los servicios gestionados deben acoplarse a la arquitectura y modo de funcionamiento requeridos por el BIESS. Por lo que el contratista podrá y/o deberá realizar adecuaciones en el/los Data Centers, configuraciones, o inclusive incorporar elementos de hardware o software de ser necesario para este fin, sin que esto represente costo adicional para el BIESS. El oferente deberá realizar una visita técnica, a los centros de procesamiento Principal y Alterno, con el fin de identificar los componentes y recursos necesarios para la correcta energización, re acondicionamiento, controles ambientales y otros necesarios para el correcto funcionamiento de la infraestructura en cumplimiento a las prácticas de datacenter TIER III. El contratista debe realizar una evaluación para validar compatibilidad de los aplicativos del BIESS con la solución propuesta de balanceo y protección de seguridad WAF de servicios gestionados; misma que será registrada en una acta que avala que las actividades aquí solicitadas fueron realizadas. Debido a que el presente proceso involucra el manejo de tecnología especializada en los Centros de Procesamiento de Datos Principal y Alterno, el personal técnico del BIESS requiere la transferencia de conocimiento mínimo de 8 ó 12 horas por cada una de las soluciones en servicios gestionados como Firewall, Balanceadores, WAF, AntiDDoS.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 34 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

	Adicionalmente, el contratista deberá proporcionar plataformas de acceso web bajo demanda que permitan al personal técnico consultar contenidos, cursos y materiales complementarios en línea, asegurando la disponibilidad continua de recursos de capacitación más allá de las sesiones presenciales. Los instructores designados deberán contar con certificación oficial del fabricante en la tecnología impartida. Al finalizar la transferencia, se entregará un certificado de participación respaldado por la empresa, garantizando que la capacitación cumple con los estándares de actualización periódica exigidos por el fabricante. Esta transferencia de conocimiento se realizará en las fechas y horas acordadas entre las partes. Todos los gastos de materiales correrán por parte del contratista. El contratista entregará un temario por cada solución para revisión y aprobación del administrador de contrato. El temario se basará en el temario oficial del fabricante para la certificación equivalente a administración de la solución. Él o los instructores deberán estar certificados en la tecnología de la cual estén brindando la transferencia de conocimientos. Se deberá entregar un certificado con respaldo de la empresa al culminar la misma.
--	---

SERVICIOS BAJO DEMANDA
16. Puntos de red cobre
Posterior al inicio del servicio, el BIESS a través del Administrador de Contrato, solicitará bajo demanda nuevos puntos de red, para lo cual, El contratista debe proporcionar los patch cords de Cbre que se requieran para la conectividad desde los switches del contratista hacia los equipos a ser alojados. Todos los patch cords utilizados en nuevas solicitudes de conexión deben ser nuevos y certificados de fábrica.
17. Puntos de red fibra a 1GB
Posterior al inicio del servicio, el BIESS a través del Administrador de Contrato solicitará bajo demanda nuevos puntos de red, para lo cual, El contratista debe proporcionar los patch cords de fibra que se requieran para la conectividad desde los switches del contratista hacia los equipos a ser alojados. Todos los patch cords utilizados en nuevas solicitudes de conexión deben ser nuevos y certificados de fábrica.
18. Puntos de red fibra a 10GB
Posterior al inicio del servicio, el BIESS a través del Administrador de Contrato solicitará bajo demanda nuevos puntos de red, para lo cual, El contratista debe proporcionar los patch cords de fibra que se requieran para la conectividad desde los switches del contratista hacia los equipos a ser alojados. Todos los patch cords utilizados en nuevas solicitudes de conexión deben ser nuevos y certificados de fábrica.
19. Cintas (Espacio en cintoteca)
el BIESS a través del Administrador de Contrato solicitará bajo demanda de espacio adicional de almacenamiento de cintas en cintoteca, con las mismas condiciones descritas anteriormente en el punto 4 "Cintoteca CPDP". El contratista deberá llevar el reporte de cintas adicionales en el informe mensual de Housing.
20. SERVICIO DE STORAGE (STaaS), Capacidad 59 TB
La entidad solicitará bajo demanda del servicio de Storage (STaaS) adicional, con las mismas condiciones descritas anteriormente en el punto 11 "Servicio de Storage (STaaS)".

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 35 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

21. SERVICIO DE BACKUP (BaaS), Capacidad 39 TB
el BIESS a través del Administrador de Contrato solicitará bajo demanda del servicio de Backup (BaaS) adicional, con las mismas condiciones descritas anteriormente en el punto 12 "Servicio Backup (BaaS)".

Para la prestación del servicio, se ha determinado que el BIESS al ser una entidad de banca pública que administra información financiera y transaccional crítica, cuya disponibilidad, integridad y confidencialidad son indispensables para la prestación ininterrumpida de los servicios institucionales, la ejecución de operaciones financieras crediticias y el cumplimiento de las disposiciones regulatorias en materia de gestión de riesgos y continuidad del negocio, se requiere que el proveedor del servicio sea propietario tanto del Data Center Principal como del Data Center Alterno. Esta condición garantiza el control directo, permanente e integral sobre la infraestructura física y tecnológica que soportará los servicios contratados, eliminando la dependencia de terceros para la administración, mantenimiento, ampliación, acceso y recuperación de la infraestructura crítica. Asimismo, mitiga riesgos operativos asociados a la terminación o modificación de contratos de uso o arrendamiento, restricciones de acceso, controversias, cambios de condiciones operativas, insolvencia o decisiones comerciales de terceros que puedan comprometer la disponibilidad de los servicios. La propiedad de ambos Data Centers fortalece la capacidad del proveedor para ejecutar de manera inmediata los planes de continuidad del negocio y recuperación ante desastres, garantizando la disponibilidad permanente de la infraestructura, la atención oportuna de incidentes críticos y la resiliencia operativa requerida para soportar los servicios tecnológicos esenciales de la institución, reduciendo significativamente la exposición a riesgos que podrían afectar la estabilidad de la operación y la prestación de los servicios institucionales.

2.8 DEFINICIÓN DE PRESUPUESTO REFERENCIAL:

Del resultado del Estudio de Mercado se ha definido que el presupuesto referencial para esta contratación es de USD \$869.525,00 (Ochocientos sesenta y nueve mil quinientos veinte y cinco 00/100 dólares de los Estados Unidos de América) más IVA, desglosados de la siguiente manera:

ÍTEM	SERVICIO	CANTIDAD	VALOR UNIT.	VALOR MENSUAL	MESES DEL SERVICIO	VALOR TOTAL ANUAL
HOUSING CENTRO DE DATOS						
1	Centro De procesamiento de Datos Principal(Guayaquil)y Componentes (RACK).	4	\$4.400,00	\$17.600,00	12	\$211.200,00
2	Centro de procesamiento de datos alterno (Quito)y componentes (RACK)	2	\$5.650,00	\$11.300,00	12	\$135.600,00
3	Interconexión LAN CPDP – CPDA (100 Mbps)	1	\$1.600,00	\$1.600,00	12	\$19.200,00
4	Cintoteca CPDP	1043	\$7,50	\$7.822,50	12	\$93.870,00
5	Servicio de horas de manos remotas	2	\$80,00	\$160,00	12	\$1.920,00
6	Servicio de Mailling (Antispam), dominio biess.info.ec	1	\$1.650,00	\$1.650,00	12	\$19.800,00
7	Servicio de Seguridad Perimetral (Next Generation Firewall)	1	\$7.530,00	\$7.530,00	12	\$90.360,00
8	Servicio de Balanceo de Aplicaciones	1	\$6.310,00	\$6.310,00	12	\$75.720,00

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO		Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER		Página 36 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA		

9	Servicio de Web Application Firewall (WAF)	1	\$5.460,00	\$5.460,00	12	\$65.520,00
10	Servicio de DDoS	1	\$2.390,00	\$2.390,00	12	\$28.680,00
11	Servicio de Storage (STaaS), capacidad 10 TB	10	\$20,00	\$200,00	12	\$2.400,00
12	Servicio de Backup (BaaS), capacidad 50 TB	50	\$90,00	\$4.500,00	12	\$54.000,00
13	Servicio de Deep & Dark Web (1 dominio)	1	\$700,00	\$700,00	12	\$8.400,00
14	Servicio de Brand Protection (1 dominio)	1	\$600,00	\$600,00	12	\$7.200,00
15	Servicio Data Leakage (1 dominio)	1	\$250,00	\$250,00	12	\$3.000,00
			SUBTOTAL	\$68.072,50		\$816.870,00
SERVICIOS BAJO DEMANDA						
16	Puntos de red cobre	30	\$15,00	\$450,00	5	\$2.250,00
17	Puntos de red fibra a 1GB	5	\$17,00	\$85,00	5	\$425,00
18	Puntos de red fibra a 10GB	5	\$28,00	\$140,00	5	\$700,00
19	Cintas (Espacio en cintoteca)	738	\$7,00	\$5.166,00	5	\$25.830,00
20	Servicio de Storage (STaaS), capacidad 59 TB	59	\$20,00	\$1.180,00	5	\$5.900,00
21	Servicio de Backup (BaaS), capacidad de 39 TB	39	\$90,00	\$3.510,00	5	\$17.550,00
			SUBTOTAL	\$10.531,00		\$52.655,00
			SUBTOTAL			\$869.525,00
			IVA			\$130.428,75
			TOTAL			\$999.953,75

2.9 PLAZO DE EJECUCIÓN:

El plazo de ejecución de esta contratación es de 365 días calendario a partir de la notificación de la autorización de inicio del servicio, la cual será emitida por el administrador del contrato.

2.10 FORMA Y CONDICIONES DE PAGO:

El BIESS realizara pagos trimestrales al contratista por el 100% del valor de los servicios efectivamente prestados a entera satisfacción de la contratante, posterior a la suscripción del Acta Entrega Recepción Parcial/Definitiva correspondiente.

Los documentos habilitantes de pago son los siguientes:

- Informe del Contratista
- Acta Entrega Recepción Parcial/Definitiva
- Prefactura.

Para los casos de los servicios bajo demanda, se considerarán los siguientes documentos habilitantes para el pago:

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
	UNIDAD REQUIRENTE:	Página 37 de 55
	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

- Autorización del Administrador de contrato
- Proforma del nuevo servicio a ser implementado
- Informe del Contratista
- Acta Entrega Recepción

2.11 GARANTÍAS

Garantía de fiel cumplimiento: La garantía de fiel cumplimiento del contrato se rendirá por un valor igual al cinco por ciento (5%) del monto total del mismo, la que deberá ser presentada previo a la suscripción del contrato.

Esta garantía será devuelta luego de la suscripción del acta entrega recepción definitiva.

2.12 RIESGOS ASOCIADOS A LOS SERVICIOS PROVISTOS POR TERCEROS

Conjuntamente con la Dirección de Riesgo Operativo del BIESS, se realizó la identificación asociada a los riesgos provistos para contratación, la matriz de riesgos se adjunta como Anexo 1.

3 CONDICIONES PARTICULARES DE LA CONTRATACIÓN

3.1 OBLIGACIONES DEL CONTRATISTA:

El contratista adjudicado se obliga de manera vinculante al estricto cumplimiento de las siguientes condiciones durante toda la vigencia de la relación contractual:

- **Cumplimiento de Pliegos y Oferta:** Dar cumplimiento cabal, oportuno e irrestricto a todas las características técnicas, metodológicas y administrativas establecidas en las presentes bases del concurso y en su oferta técnica adjudicada.
- **Facilidades de Control y Auditoría:** Prestar de forma inmediata y obligatoria todas las facilidades logísticas, físicas y tecnológicas para la revisión, inspección y seguimiento del servicio prestado por parte del Administrador del Contrato del BIESS, así como de la Unidad de Auditoría Interna, auditores externos y delegados de la Superintendencia de Bancos.
- **Control de Lavado de Activos (UAFE):** En caso de que el contratista realice una actividad económica catalogada como sujeto obligado a reportar ante la Unidad de Análisis Financiero y Económico (UAFE), deberá presentar de forma obligatoria el Certificado de Cumplimiento de la UAFE vigente al momento de la suscripción del contrato y mantenerlo actualizado durante la ejecución contractual.
- **Blindaje de Confidencialidad:** Suscribir obligatoriamente el Acuerdo de Confidencialidad y No Divulgación de Información proporcionado por el BIESS, de manera conjunta y simultánea a la firma del contrato principal.
- **Tratamiento y Custodia de Datos Personales (LOPD):** Dar fiel y estricto cumplimiento a la Ley Orgánica de Protección de Datos Personales (LOPD) vigente y a las normas emitidas por la

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO		Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER		
			Página 38 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA		

Superintendencia de Bancos dentro del ámbito de competencia del servicio prestado. El contratista asume la figura jurídica de **Encargado del Tratamiento de Datos**, siendo responsable administrativo y penal por cualquier fuga, alteración, pérdida o acceso no autorizado a los datos del banco.

- El contratista podrá cambiar el personal técnico durante la ejecución del contrato, para lo cual deberá notificar al administrador quien evaluará que cumpla con la experiencia y demás condiciones exigidas para el personal técnico y aprobará su respectivo remplazo.

3.2 OBLIGACIONES ADICIONALES DEL CONTRATISTA:

a) CONFIDENCIALIDAD DE LA INFORMACIÓN:

Prohibición Absoluta de Divulgación: El contratista y la totalidad de sus colaboradores, asesores o subcontratistas quedan expresamente prohibidos de reproducir, publicar, transferir o difundir la información institucional o bases de datos lógicas del BIESS que lleguen a su conocimiento con ocasión del servicio, por ser considerada información confidencial y de propiedad exclusiva del Banco. El incumplimiento debidamente probado de esta obligación constituirá causal de terminación unilateral y anticipada del contrato por parte del Administrador del Contrato, sin perjuicio de las acciones civiles, administrativas y penales a las que hubiere lugar.

Cumplimiento de Políticas Internas de Ciberseguridad: El contratista y el personal asignado para la prestación del servicio se obligan formalmente a cumplir y hacer cumplir la Política, Reglamento, Manual e instructivos de Seguridad de la Información y Gestión de Accesos lógicos vigentes en el BIESS.

Formalización del Convenio: Constituye una obligación de obligatorio cumplimiento la suscripción del Convenio de Confidencialidad y No Divulgación de Información de forma simultánea a la firma del contrato principal.

Rol de Encargado del Tratamiento (LOPD): De conformidad con la Ley Orgánica de Protección de Datos Personales (LOPD), el contratista asume de manera vinculante la figura de **Encargado del Tratamiento** sobre los datos lógicos alojados, procesados o respaldados en la infraestructura de *Housing* y servicios de nube provistos. Por tanto, se obliga a tratar los datos personales única y exclusivamente bajo las instrucciones documentadas emitidas por el BIESS y con el solo fin de ejecutar el objeto contractual.

Control de Datos Generales, Sensibles y Financieros: En concordancia con el informe técnico de identificación de datos del proceso, el contratista reconoce que la infraestructura custodia datos generales (identificativos, localización, laborales), datos financieros (cuentas bancarias, historiales crediticios) y datos sensibles (discapacidades y sustitutos) correspondientes a afiliados, jubilados, pensionistas, servidores y trabajadores del banco. En consecuencia, implementará obligatoriamente las siguientes medidas mínimas de seguridad:

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 39 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

- **Control de Acceso Físico y Lógico:** Autenticación robusta de usuarios, perfiles con mínima autorización, segregación estricta de funciones y restricción física porPODs/jaulas mediante tarjetas de proximidad o biometría.
- **Cifrado de Extremo a Extremo:** Cifrado de datos en tránsito y en reposo para salvaguardar la integridad de las bases de datos transaccionales (IBS Producción) y la suite de correo masivo info.fin.ec.
- **Trazabilidad de Logs:** Conservación de bitácoras (*logs*) inalterables de accesos por un período mínimo de seis (6) meses y desvío en tiempo real hacia la consola interna del BIESS.

Plazo Perentorio de Notificación de Brechas: El contratista deberá notificar obligatoriamente al Administrador del Contrato y al equipo de Seguridad de la Información del BIESS cualquier incidente de ciberseguridad, vulneración, alteración o violación a la seguridad de los datos personales de manera inmediata a su detección, fijándose un término máximo improrrogable de **dos (2) días contados a partir de su conocimiento**, adjuntando la matriz de impacto y asumiendo los costos íntegros de contención y remediación.

Obligación de Destrucción Segura Post-Contrato: Concluida la vigencia contractual, el contratista transferirá los respaldos lógicos al BIESS y ejecutará un borrado definitivo e irreversible de todo remanente de datos en sus sistemas de almacenamiento (*STaaS*) y esquemas de *Backup (BaaS)*, utilizando metodologías que impidan su reconstrucción. El proveedor entregará una certificación formal suscrita por su representante legal detallando el método técnico utilizado, el cual será un requisito habilitante e indispensable para proceder con la firma del Acta de Entrega-Recepción Definitiva.

b) PLAN DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO:

El contratista debe entregar un “Plan de Continuidad del Negocio” sobre su infraestructura a nivel de Data Center que garantice la continuidad de los servicios ofertados según la necesidad del BIESS. El plan contendrá como mínimo lo siguiente:

- Plan de mantenimiento de los componentes de datacenter enfocado a la continuidad
- Informe del último Plan de Recuperación de Desastres (DRP) del datacenter

En el plazo de 30 días a partir de la suscripción del contrato, el contratista deberá presentar al Administrador del Contrato, el plan de contingencia del servicio contratado, el mismo que permanecerá vigente durante la prestación del servicio y será sometido a pruebas con las áreas pertinentes y aprobado por la Dirección de Riesgo Operativo del BIESS.

c) DERECHOS DE PROPIEDAD INTELECTUAL:

No aplica, los productos/servicios del objeto de contratación no involucran la consideración de este apartado.

d) ETAPA DE TRANSICIÓN:

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
	UNIDAD REQUIRENTE:	Página 40 de 55
	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

Para la contratación de servicios determinados como críticos por las áreas requirentes, estas deberán considerar una etapa de transición, en el caso de que el BIESS decida hacerse cargo del servicio o a su vez contratar con algún otro proveedor del servicio, para lo cual deben considerar todos los aspectos y tiempo necesario para que se cumpla esta condición.

e) CUMPLIMIENTO NORMATIVO INTERNA:

El Contratista deberá cumplir con la normativa interna del Banco relacionada a la norma expedida por la Superintendencia de Bancos, aplicable en función del servicio a ser contratado, por tanto, para la ejecución, el Administrador de Contrato socializará los documentos normativos y sus actualizaciones sobre la Gestión de Configuración, Documentación de Políticas, Reglamento de Seguridad de la Información y otros que por la naturaleza de las actividades se deban aplicar.

f) EQUIPO DE LA CONTRAPARTE CALIFICADO PARA BRINDAR EL SERVICIO EN LOS NIVELES REQUERIDOS:

El Contratista, al inicio de la ejecución del contrato deberá entregar el listado del equipo de contraparte técnica y/o administrativa al Administrador del Contrato para la oportuna ejecución del servicio.

g) ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN

En cumplimiento de las normativas de control del sector financiero y las políticas institucionales co-establecidas con la Dirección de Seguridad de la Información, el contratista deberá garantizar los siguientes parámetros mínimos de protección física y lógica sobre los servicios gestionados:

- **Línea Base de Configuración Segura (*Hardening*):** El contratista implementará políticas de endurecimiento técnico (*hardening*) en todos los componentes lógicos provistos (Firewall, WAF, DDoS y balanceador). Esto incluye la desactivación obligatoria de protocolos obsoletos, cambio de credenciales por defecto de los administradores y la habilitación exclusiva de puertos necesarios para la operación transaccional del BIESS.
- **Gestión de Vulnerabilidades y Parches:** El contratista ejecutará de manera permanente el monitoreo de alertas de seguridad del fabricante aplicables a las plataformas de hardware y software del Data Center. Se obliga a aplicar los parches de seguridad y actualizaciones críticas de forma planificada, previa autorización del Administrador del Contrato del BIESS, para mitigar debilidades que expongan el perímetro del banco.
- **Integridad y Resguardo de Bitácoras (*Logs*):** Toda actividad de administración, modificación de reglas perimetrales, accesos de usuarios VPN o alertas de ciberseguridad perimetral deberá quedar registrada de forma automática en bitácoras (*logs*) inalterables. El contratista garantizará el almacenamiento seguro de estos registros por todo el tiempo que dure el contrato, asegurando que la información sea de propiedad exclusiva del BIESS y se encuentre disponible para auditorías técnicas.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO		Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER		Página 41 de 55
	UNIDAD REQUIRENTE: COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA		

- **Cumplimiento de Estándares Internacionales:** Como pilar de seguridad proactiva y viabilidad operativa, el contratista demostrará durante la ejecución del servicio el mantenimiento de sus certificaciones vigentes en el esquema de seguridad ISO 27001 (Seguridad de la Información), ISO 27017 (Seguridad en la Nube) e ISO 27018 (Protección de Datos Personales en la Nube) aplicables a la infraestructura física y tecnológica que soporta la operación del banco.

h) TRANSFERENCIA DE CONOCIMIENTO

- El contratista deberá realizar la respectiva transferencia de conocimiento del/los servicio ofertados, en el término de 30 días a partir del inicio del servicio objeto de esta contratación. El administrador de contrato determinará los técnicos que participaran en esta capacitación.
- El contratista deberá realizar la entrega de toda la documentación asociada a manuales de los servicios ofertados

J) ACUERDO DE NIVELES DE SERVICIO

Ver el Documento de Acuerdo de Niveles de Servicio, que se incluye como Anexo 2.

k) INFORMES DE AUDITORIA EXTERNA APLICABLE AL SERVICIO A SER CONTRATADO

El contratista a partir del inicio de ejecución del contrato, en un término de 5 días deberá presentar como evidenciable el último informe de auditoría realizado por un ente externo, asociado a los siguientes puntos:

- Seguridad de la Información
- Continuidad del negocio

Dichos puntos se encuentran asociados al servicio de Housing de centro de datos y a su vez a la seguridad para el manejo de la información del cliente

Dichos informes deberán estar vigentes durante la prestación del servicio.

3.3 OTRAS CONDICIONES CONTRACTUALES EXIGIDAS POR LOS ENTES DE CONTROL.

En cumplimiento de lo dispuesto en los *ítems 1 al 5, ARTÍCULO 23, SECCIÓN VII.- SERVICIOS PROVISTOS POR TERCEROS, CAPÍTULO V.- NORMA DE CONTROL PARA LA GESTIÓN DEL RIESGO OPERATIVO, TÍTULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, del LIBRO I.- NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO,*

g) La gestión de riesgos asociados a los servicios críticos provistos por terceros, que garanticen la gestión de seguridad de la información incluyendo ciberseguridad y la gestión de la continuidad del negocio, en función a la naturaleza del servicio contratado.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 42 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

3.4 OBLIGACIONES DEL CONTRATANTE Y ADMINISTRADOR DE CONTRATO

El Banco del Instituto Ecuatoriano de Seguridad Social (BIESS) y el Administrador que sea designado para el control del servicio, ejercerán de manera obligatoria las siguientes atribuciones y responsabilidades contractuales:

- **Designación del Administrador:** se designará formalmente al Administrador del Contrato, quien asumirá la responsabilidad de velar por la ejecución cabal de todas las cláusulas vigentes.
- **Planificación de Pruebas de Continuidad:** El Administrador de Contrato, en coordinación técnica con el Gerente de Proyecto del proveedor, estructurará el cronograma para la validación, ejecución y soporte de las pruebas de contingencia del Plan de Recuperación ante Desastres (DRP) hacia el Sitio Alterno de Quito, gestionando su respectiva aprobación y validación ante la Dirección de Riesgo Operativo institucional.
- **Oportunidad y Tiempos de Respuesta:** Cumplimiento de los plazos de atención y resolución de incidencias según la criticidad informada. Se evaluará mecánicamente el desempeño bajo criterios cuantitativos de cumplimiento técnico, efectividad de la mesa de soporte (tickets cerrados a tiempo) y la oportuna entrega de los evidenciables mensuales de ciberseguridad dentro de los plazos contractuales estipulados. El resultado de este proceso se formalizará mediante la emisión del Certificado de Evaluación.
- **Resolución oportuna de peticiones:** Atender y dar solución formal a los requerimientos, consultas técnicas o problemas administrativos escritos que sean presentados por el contratista en el desarrollo del servicio, en un término máximo de diez (10) días contados a partir de su recepción oficial.
- **Suscripción de actas de conformidad:** Suscribir las actas de entrega-recepción parciales y definitiva de los servicios gestionados recibidos, siempre que se verifique técnicamente que el proveedor ha cumplido con los parámetros de calidad del servicio y las obligaciones de ley conexas.
- **Aplicación de Control Independiente:** El Administrador del Contrato aplicará de forma estricta la Metodología de Control y Monitoreo Independiente de los servicios contratados, conforme a los lineamientos imperativos detallados en el apartado de la Metodología de Trabajo de estas bases, asegurando el desvío de *logs* en tiempo real para mantener la soberanía de los datos de la banca pública.
- **Transparencia y Soportes de Auditoría:** Mantener un expediente físico y digital íntegro y debidamente foliado con todas las actuaciones, reportes independientes de SLAs y memorandos del proceso, garantizando el libre acceso a la información y brindando las facilidades del caso a los auditores internos, externos y delegados de la Superintendencia de Bancos, ; misma que se encontrará publicada en la página web institucional

3.5 TRATAMIENTO DE DATOS PERSONALES

En virtud de haberse determinado que el presente procedimiento de contratación involucra el uso y custodia incidental o controlada de información de la institución, se desarrollan los contenidos obligatorios que regirán la ejecución del servicio:

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 43 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

- **Identificación del tipo o naturaleza del tratamiento:** Corresponde a las actividades de recolección, almacenamiento, conservación, custodia, transmisión y eliminación segura de bases de datos lógicas y respaldos institucionales alojados en la infraestructura física provista por el contratista.
- **Identificación de la información a proporcionar objeto del tratamiento de datos:** Datos identificativos como nombres, apellidos, números de cédula, firmas y direcciones; datos de localización y direcciones IP; datos de contacto profesional; datos laborales; y categorías especiales de información que abarcan datos crediticios, financieros, económicos, patrimoniales, así como datos de personas con discapacidad y sustitutos.
- **Identificación de los Titulares de los datos personales tratados:** Afiliados activos, jubilados, pensionistas, beneficiarios, usuarios financieros, así como servidores, exservidores, trabajadores y extrabajadores del Banco del Instituto Ecuatoriano de Seguridad Social (BIESS).
- **Alcance y fin del objeto de contratación:** Proporcionar servicios gestionados de Data Center, alojamiento de infraestructura tecnológica en modalidad *Housing*, almacenamiento, conectividad, seguridad perimetral, monitoreo, respaldo, recuperación ante desastres y soporte técnico que permitan garantizar la continuidad operativa, disponibilidad, integridad, confidencialidad y seguridad de la información institucional.
- **Descripción de los medios utilizados para permitir los accesos a datos personales:** El contratista proveerá el entorno físico y la capa de red segura en centros de procesamiento de datos de categoría TIER III. El envío, transmisión o intercambio de información se realizará exclusivamente a través de medios tecnológicos seguros autorizados por el BIESS, incluyendo redes privadas, enlaces dedicados, canales cifrados, conexiones VPN y protocolos seguros de comunicación. El acceso lógico a las bases de datos transaccionales será de uso exclusivo del personal técnico del BIESS, quedando restringida la manipulación de datos por parte del personal del proveedor al ámbito estrictamente necesario para el soporte de la infraestructura.
- **Finalidad del Tratamiento:** Garantizar la continuidad, disponibilidad, estabilidad e integridad de las plataformas y sistemas lógicos que soportan los productos financieros misionales del banco, específicamente la precalificación, aprobación y desembolso de Préstamos Quirografarios, Préstamos Hipotecarios y Préstamos Prendarios a nivel nacional.
- **Responsable del Tratamiento:** Banco del Instituto Ecuatoriano de Seguridad Social (BIESS).
- **Obligaciones del Encargado de Tratamiento:**
 - Tratar los datos personales única y exclusivamente conforme a las instrucciones documentadas emitidas por el BIESS y para los fines de la ejecución del objeto contractual.
 - Garantizar la confidencialidad de la información y restringir el acceso a la misma únicamente al personal estrictamente autorizado.
 - Implementar y mantener las medidas técnicas, organizativas, físicas y administrativas apropiadas determinadas en los estándares internacionales ISO 27001, ISO 27017 e ISO 27018 para proteger la información frente a accesos no autorizados, pérdida, alteración o destrucción ilícita.
 - Notificar al Administrador del Contrato del BIESS cualquier incidente de seguridad, vulneración o brecha de los datos personales de manera inmediata y a más tardar dentro del término de dos (2) días contados a partir de su conocimiento.
 - Colaborar con el BIESS en la atención de requerimientos de los titulares, auditorías o requerimientos de las autoridades de control competentes.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO		Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER		
			Página 44 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA		

- No transferir, comunicar, divulgar o utilizar los datos personales para fines propios o de terceros.
- **Obligaciones del Responsable del Tratamiento:**
 - Determinar las finalidades, medios y condiciones bajo las cuales se realizará el tratamiento de los datos personales.
 - Proporcionar al contratista únicamente la información y los accesos lógicos estrictamente necesarios para el desarrollo del objeto contractual.
 - Emitir las instrucciones, lineamientos y directrices técnicas necesarias para el tratamiento seguro de la información conforme a la normativa legal vigente.
 - Supervisar, controlar y auditar el cumplimiento de las obligaciones técnicas, organizativas y de seguridad de la información asumidas por el contratista.
 - Verificar al término de la relación contractual la devolución, eliminación o destrucción segura de la información puesta a disposición del proveedor.
- **Subcontratación del Tratamiento:** El contratista no podrá subcontratar la ejecución de actividades que impliquen el tratamiento de datos personales, a menos que reciba autorización previa y expresa por escrito por parte del Administrador del Contrato del BIESS. En caso de autorizarse, el subcontratista asumirá de forma vinculante las mismas obligaciones de protección y confidencialidad que el encargado principal.
- **Derecho de repetición contra el encargo:** El BIESS se reserva el derecho de repetir contra el contratista por el valor total de las indemnizaciones, multas, sanciones administrativas o pérdidas económicas que la institución deba asumir como consecuencia directa de fallas, omisiones, negligencia o incumplimientos del proveedor en sus obligaciones como Encargado del Tratamiento de Datos Personales o debido a incidentes de seguridad que le sean imputables.
- **Derechos de titulares de datos:** El BIESS, como Responsable del Tratamiento, será el único canal encargado de gestionar y atender el ejercicio de los derechos de acceso, eliminación, rectificación, actualización, oposición y portabilidad de los titulares de los datos personales. El contratista se obliga a prestar toda la colaboración técnica que el Administrador del Contrato le requiera para dar atención oportuna a dichos requerimientos.
- **Plazo de conservación, devolución o eliminación de datos:** El contratista conservará los datos únicamente durante la vigencia del contrato. Concluida la relación contractual, el contratista estará obligado a realizar la entrega total de los respaldos lógicos y la información al BIESS. Una vez verificada la integridad de la devolución por parte del Banco, el contratista procederá a la eliminación segura, destrucción o borrado definitivo e irreversible de todas las copias de la información en sus ambientes de producción, contingencia, almacenamiento temporal y respaldos, emitiendo una certificación formal suscrita por su representante autorizado que detalle el método técnico utilizado.

3.6 MULTAS Y PENALIZACIONES:

En los casos de incumplimiento de las obligaciones contractuales por parte del contratista, se aplicará por cada día de retraso en la ejecución, una multa del 1 x 1.000 del valor del contrato, conforme las condiciones establecidas en el contrato.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO		Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER		Página 45 de 55
	UNIDAD REQUIRENTE: COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA		

Penalizaciones. – En caso de incumplimiento de los Acuerdos de Niveles de Servicio (ANS), se aplicarán las penalidades establecidas para cada incumplimiento, de conformidad con lo previsto en dichos acuerdos. En caso de aplicarse una multa y/o penalización, ésta deberá ser contemplada en la respectiva acta entrega recepción para el descuento en el pago del periodo actual.

3.7 VIGENCIA DE LA OFERTA:

Conforme el numeral 33.1 del artículo 33 del Reglamento para las Contrataciones de Giro Específico del Negocio del Banco del Instituto Ecuatoriano de Seguridad Social – BIESS: *“Las ofertas se entenderán vigentes hasta la fecha de la suscripción del contrato”*.

3.8 SUBCONTRATACIÓN

- El/la contratista podrá subcontratar la ejecución parcial del contrato con personas naturales o jurídicas, bajo su riesgo y responsabilidad.
- El/la contratista podrá subcontratar determinados trabajos debidamente justificados, previa autorización del administrador del contrato siempre que el monto de la totalidad de lo subcontratado no supere el 30% del valor del contrato principal.
- El/la contratista será la única responsable ante el contratante por los actos u omisiones de sus subcontratistas y de las personas directa o indirectamente empleadas por ellos.

3.9 DEBIDA DILIGENCIA – POLÍTICA CONOZCA A SU PROVEEDOR

Los Formularios de Perfil Conozca a su Proveedor deberán ser presentados solo por el **OFERENTE FINALISTA DEL PROCESO, PREVIO A LA ADJUDICACIÓN**, según corresponda (persona natural o jurídica).

El proveedor deberá llenar y presentar el formulario que le corresponda más la documentación de respaldo solicitada por el BIESS.

DECLARACIONES:

- **Declaración de No Aplicabilidad de Servicios Cloud:** El área requirente aclara expresamente que el objeto de la presente contratación no contempla la adquisición, arrendamiento ni suscripción de servicios de infraestructura, plataforma o software en la nube (*IaaS, PaaS, SaaS*) con proveedores nacionales ni extranjeros. En consecuencia, se determina que **NO APLICA** la presentación de los informes específicos ni el procedimiento de notificación obligatoria previa normados en el Artículo 23, numeral 6 de la Resolución SB-2023-01901 de la Superintendencia de Bancos.
- **Ratificación de la Naturaleza del Servicio:** Las obligaciones del presente proceso se circunscriben estrictamente a la modalidad de *Housing* físico, almacenamiento local y ciberseguridad perimetral gestionada sobre el equipamiento e infraestructura centralizada del proveedor. La totalidad de los datos lógicos, bases de datos

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	Página 46 de 55
	UNIDAD REQUIRENTE: COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

transaccionales y respaldos del BIESS se mantendrán alojados de forma exclusiva en los centros de procesamiento de datos físicos, independientes y geodiferenciados ubicados dentro del territorio ecuatoriano (Data Center Principal en Guayaquil y Data Center Alternativo en Quito), operados directamente por el contratista adjudicado bajo estándares de categoría TIER III.

4 PARÁMETROS Y METODOLOGÍA DE EVALUACIÓN DE LAS OFERTAS

Para realizar la evaluación de la capacidad del servicio solicitado, la instalación y/o soporte e historial de desempeño, capacidad logística, instalaciones y recursos humanos, de conformidad con lo establecido en el Artículo 23 de la Norma de Control para la Gestión del Riesgo Operativo de la Superintendencia de Bancos, el oferente deberá acreditar documentadamente el cumplimiento de los siguientes requisitos mínimos, a través de los medios de verificación detallados a continuación:

4.1 METODOLOGÍA CUMPLE / NO CUMPLE

Para la verificación del cumplimiento de los requisitos mínimos, se empleará la metodología cumple/no cumple y por puntaje.

1. CUMPLIMIENTO DE REQUISITOS MÍNIMOS

A) INTEGRIDAD DE LA OFERTA:

El BIESS verificará la presentación de los formularios previstos en las bases del concurso, que se encuentre debidamente firmado y completos conforme a los formatos establecidos.

B) EXPERIENCIA DE EL/LOS PARTICIPANTE/S

La empresa oferente debe demostrar de manera obligatoria la siguiente experiencia general:

No.	Tipo	Descripción	Temporalidad	Número de proyectos similares	Valor del Monto mínimo de experiencia	Valor del Monto mínimo de cada proyecto
1	General	Experiencia en implementar proyectos de Data Center.	Últimos 5 años	Al menos 1	\$300.000,00	\$200.000,00

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO		Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER		Página 47 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA		

2	Específica	Experiencia en proveer servicios de housing y servicios gestionados de Data Center a instituciones bancarias del sector financiero (solo bancos)	Últimos 5 años	Al menos 1	\$150.000,00	\$115.000,00
---	------------	--	----------------	------------	--------------	--------------

Medio de comprobación: Podrá presentar certificados, actas de entrega recepción parcial o definitiva de contratos liquidados y/o copias de contratos vigentes.

C) PERSONAL TÉCNICO, RECURSO HUMANO, EQUIPO DE TRABAJO / RECURSOS. -

Ítem	Función/Cargo	Cantidad	Nivel de estudio	Título Académico
1	Gerente o Líder de Proyecto	1	Tercer nivel con título	- Ingeniero ó Licenciado en Sistemas - Ingeniero Tecnólogo computación. Ingeniero ó Licenciado Electrónica Telecomunicaciones - Ingeniero ó Licenciado Telemática. - Ingeniero ó Licenciado Informática. - Ingeniero ó Licenciado en Redes y Telecomunicaciones - Ingeniero ó Licenciado en sistemas y redes. - Ingeniero ó Licenciado administración empresas. - O equivalentes.
2	Técnico de Soporte de Nivel 3	3	Tercer nivel con título	- Ingeniero o Licenciado Sistemas. - Ingeniero o Licenciado computación. - Ingeniero o Licenciado en Electrónica o Telecomunicaciones. - Ingeniero o Licenciado en Telemática. - Ingeniero o licenciado en informática o Licenciado en Redes y Telecomunicaciones - Ingeniero o Licenciado en sistemas y redes - O equivalentes
3	Técnico de Soporte de Nivel 2	3	Tercer nivel con título	- Ingeniero o Licenciado Sistemas. - Ingeniero o Licenciado computación. - Ingeniero ó Licenciado Electrónica Telecomunicaciones - Ingeniero ó Licenciado Telemática. - Ingeniero ó Licenciado Informática. - Ingeniero o Licenciado en Redes Telecomunicaciones - Ingeniero ó Licenciado en sistemas y redes.
4	Técnico Soporte Nivel 1 de servicio	3	Tercer nivel con título	- Licenciado ó Tecnólogo Sistemas. - Licenciado ó Tecnólogo computación. - Licenciado Tecnólogo Electrónica y Telecomunicaciones. - Licenciado o Tecnólogo en Telemática. - Licenciado o Tecnólogo en Informática. - Licenciado o Tecnólogo en Redes y Telecomunicaciones. - Licenciado o Tecnólogo en sistemas y redes.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO		Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER		Página 48 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA		

Medio de verificación: La Comisión de contratación verificará en la página del Ministerio Educación, Deporte y Cultura para lo cual el oferente deberá incluir los datos: Nombre y Número de Cédula del personal.

EXPERIENCIA DEL PERSONAL TÉCNICO. -

No.	Función/Cargo	Experiencia requerida	Tiempo de experiencia	Número de Proyectos	Monto de Proyectos
1.1	Gerente o Líder de Proyecto	Deberá acreditar experiencia acumulada como Gerente en administración de proyectos en áreas tecnológicas.	2 años	Al menos 1 (uno)	0
2.1	1 Técnico de Soporte de Nivel 3	Deberá acreditar experiencia acumulada en Ciberseguridad y/o seguridad. informática.	2 años	Al menos 1 (uno)	0
2.2	Los otros dos Técnicos de Soporte de Nivel 3	Deberá acreditar experiencia acumulada en administración de las tecnologías que soportan los servicios gestionados (WAF, Balanceador o Firewall)	2 años	Al menos 1 (uno)	0
3.1	Un Técnico de Soporte de Nivel 2	Deberá acreditar experiencia acumulada en administración y operación del Firewall.	2 años	Al menos 1 (uno)	0
3.2	Los otros Técnicos de Soporte de Nivel 2	Deberá acreditar experiencia acumulada en administración y operación de servicios de Balanceador o WAF.	2 años	Al menos 1 (uno)	0
4.1	El personal técnico de Soporte a Nivel 1	Deberá acreditar experiencia acumulada en operación de Data Center.	1 año	Al menos 1 (uno)	0
4.2	Al menos un Técnico de Soporte a Nivel 1	Deberá acreditar experiencia acumulada en la operación de Networking a nivel LAN y WAN y/o Administración y operación de la red.	1 año	Al menos 1 (uno)	0

Medio de comprobación:

La empresa oferente deberá demostrar la relación de dependencia laboral directa del personal técnico, para lo cual entregará las planillas de afiliación al IESS de los últimos seis meses.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	Página 49 de 55
	UNIDAD REQUIRENTE: COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

Deberán incluir en su oferta la HOJA DE VIDA de cada profesional que conforme el equipo de trabajo, adjuntando los certificados que acrediten la experiencia requerida, mismos que deben especificar como mínimo:

- Nombre o razón social.
- Nombre de quien expide o firma la certificación
- Señalar la experiencia en el cargo
- Tiempo de experiencia
- Fecha de expedición de la certificación

D) OFERTA ECONÓMICA

EL BIESS verificará la presentación y entrega de la oferta económica, y esta será evaluada en la calificación por puntaje

E) ANÁLISIS DE ÍNDICES FINANCIEROS:

Los índices financieros requeridos, su análisis se registrará conforme el detalle a continuación:

Índice	Indicador solicitado	Observaciones
Solvencia	mayor o igual a 1,0	Activo corriente / Pasivo corriente
Endeudamiento	menor a 1,5	Pasivo Total / Patrimonio neto

Los factores para su cálculo estarán respaldados en la correspondiente declaración de impuesto a la renta del ejercicio fiscal inmediato anterior y/o los balances presentados al órgano de control respectivo, que deberán adjuntar a la oferta.

El incumplimiento de los indicadores mínimo solicitados en las bases del concurso, serán causal de rechazo de la oferta.

F) OTRO(S) PARÁMETRO(S) EXIGIDOS POR LOS ENTES DE CONTROL. -

Otros Parámetros	Descripción/Identificador	Medio de comprobación
Certificaciones Gerente o Líder de Proyecto	✓ Certificación en Metodología del PMI - PMP, o maestría en gestión de proyectos	Presentar copias de los certificados solicitados.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO		Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER		Página 50 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA		

Certificaciones para 1 técnico de soporte nivel 3	✓ Certificación en Gestión de seguridad, certificados de forma conjunta; - CEH; o CISM; - EC-Council Licensed Penetration Tester LPT Master; o Certificados de administrador o experto de alguna de las marcas que soportan los servicios gestionados requeridos.	Presentar copias de los certificados emitidos por el fabricante. Los certificados deben encontrarse vigentes, no se aceptarán certificados caducados.
Certificaciones para los otros dos técnicos de soporte nivel 3	✓ Certificaciones de administrador, especialista o experto (o su equivalente) de al menos 1 marca de las plataformas de los servicios de DDoS, WAF, Firewall o Balanceador de Carga. De manera individual por cada técnico.	Presentar copias de los certificados emitidos por el fabricante. Los certificados deben encontrarse vigentes, no se aceptarán certificados caducados.
Certificaciones para un técnico de soporte nivel 2	✓ Certificación en Administración y operación de la red. ✓ Certificados de administrador de la marca que soportan la solución de firewall.	Presentar copias de los certificados emitidos por el fabricante. Los certificados deben encontrarse vigentes, no se aceptarán certificados caducados.
Certificaciones para los otros técnicos de soporte nivel 2	✓ Certificaciones de Administración en la marca de balanceador o waf que será ofertada en los servicios gestionados.	Presentar copias de los certificados emitidos por el fabricante. Los certificados deben encontrarse vigentes, no se aceptarán certificados caducados.
Certificaciones para los técnicos de soporte nivel 1	✓ Al menos un curso o certificación en operación de Data Center. ✓ Certificación que avalen conocimientos en redes.	Presentar copias de los certificados solicitados.
Certificación de empresa	✓ Certificación internacional en la que se establecen los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI), enfocándose en identificar y gestionar sus riesgos de seguridad de la información de manera efectiva	Certificado de seguridad de la información relacionado al servicio a contratarse emitido por una entidad certificadora.

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	Página 51 de 55
	UNIDAD REQUIRENTE: COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

Certificación TIER III	✓ Certificado emitido por el Up Time Institute de cumplimiento de norma de data center TIER III o superior.	Certificado o link del sitio web oficial del Uptime Institute en donde se verifique el cumplimiento de lo solicitado.
Propiedad del Data Center	✓ Documentos legales del oferente, en el cual indique ser propietario tanto del Data Center Principal como del Alterno.	Título de propiedad o pago de los predios urbanos municipales.
Traslado de la infraestructura a otro Data Center.	✓ En el caso que el proveedor adjudicado brinde los servicios en una ubicación diferente en la que actualmente está configurada la infraestructura del BIESS, el oferente debe incluir todos los recursos técnicos, humanos y otros, que permitan que minimicen los riesgos de pérdida de información e incidentes con la infraestructura y aplicaciones, de tal manera que los servicios del BIESS mantengan la continuidad del negocio. Para lo cual deberá entregar un Plan de Migración en el que al menos conste las siguientes actividades • Servicio de validación de estado actual de sistemas. • Aseguramiento y garantía de equipos. • Proceso de backup de equipos. • Servicio de embalaje y mapeo de equipos. • Servicio de traslado de la infraestructura. • Servicio de seguridad de escolta. • Reconexión de equipos. • Configuración de servicios de seguridad y conectividad. • Prueba de funcionamiento de las aplicaciones en el sitio destino. • Análisis y calificación de riesgo • Ventanas de indisponibilidad de los servicios productivos que no superen las 48 horas.	Plan de Migración del proveedor.

2. METODOLOGÍA POR PUNTAJE

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 52 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

Aquellas ofertas que cumplan integralmente con los requisitos mínimos pasarán a la etapa de evaluación de ofertas por puntaje, caso contrario serán descalificadas por cuanto los requisitos mínimos constituyen parámetros de cumplimiento obligatorio.

Se han definido los siguientes parámetros de calificación, los cuales serán evaluados en base a la metodología por puntaje.

PARÁMETRO	DESCRIPCIÓN DE LA METODOLOGÍA DE EVALUACIÓN	PUNTAJE
Experiencia General	No se otorgará puntaje a la experiencia general mínima requerida, por ser de cumplimiento obligatorio. Para que la experiencia general presentada sea susceptible de calificación por puntaje, ésta deberá ser mayor a la establecida como requisito mínimo. El valor total de la experiencia general solicitada adicional al requisito mínimo que será puntuada, no podrá superar el valor del presupuesto referencial del procedimiento de contratación. Se otorgará el máximo puntaje a la o las ofertas que presenten como experiencia general adicional el monto más alto y, a las demás ofertas se asignará un puntaje directamente proporcional.	10 PUNTOS
Experiencia Específica	No se otorgará puntaje a la experiencia específica mínima requerida, por ser de cumplimiento obligatorio. Para que la experiencia específica presentada sea susceptible de calificación por puntaje, ésta deberá ser mayor a la establecida como requisito mínimo. El valor total de la experiencia específica solicitada adicional al requisito mínimo que será puntuada, no podrá superar el valor del presupuesto referencial del procedimiento de contratación. Se otorgará el máximo puntaje a la o las ofertas que presenten como experiencia específica adicional el monto más alto y, a las demás ofertas se asignará un puntaje directamente proporcional	20 PUNTOS

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

Experiencia del Personal Técnico	Para que la experiencia presentada sea susceptible de calificación por puntaje, ésta deberá ser mayor a la establecida como requisito mínimo. Puntaje máximo a otorgarse a: Gerente o Líder de Proyecto: 4 (cuatro). (por cada año completo adicional a los años solicitados como requisito mínimo, se asignará un puntaje adicional de 1 puntos, hasta llegar a un máximo de 4 puntos). Técnicos de soporte nivel 3: 2 (dos). (Por cada año completo adicional de experiencia a los años solicitados como requisito mínimo, para cada personal técnico de Nivel, se asignará un puntaje adicional de 0,25 puntos, hasta llegar a un máximo de 2 puntos). La acreditación de la experiencia podrá ser individual o en conjunto. Técnicos de soporte nivel 2: 2 (dos). (Por cada año completo adicional de experiencia a los años solicitados como requisito mínimo, para cada personal técnico de Nivel, se asignará un puntaje adicional de 0,25 puntos, hasta llegar a un máximo de 2 puntos). La acreditación de la experiencia podrá ser individual o en conjunto. Técnicos de soporte nivel 1: 2 (dos). (Por cada año completo adicional de experiencia a los años solicitados como requisito mínimo, para cada personal técnico de Nivel, se asignará un puntaje adicional de 0,25 puntos, hasta llegar a un máximo de 2 puntos). La acreditación de la experiencia podrá ser individual o en conjunto.	10 PUNTOS						
Otro(s) parámetro(s) resuelto(s) por la entidad: Bonificación por certificaciones de empresa respecto a Gestión de calidad, Seguridad de la Información y Continuidad del Negocio.	Se otorgará 10 puntos al oferente que cuente con certificaciones vigentes de Seguridad de la Información y Continuidad de Negocio, conforme la siguiente tabla: <table><tr><th>CERTIFICACIÓN</th><th>PUNTAJE</th></tr><tr><td>En Seguridad de la Información (ISO 27001)</td><td>5</td></tr><tr><td>Gestión de la Continuidad de Negocio (ISO 22301)</td><td>5</td></tr></table> Para la verificación de lo indicado, los oferentes deberán presentar los certificados vigentes e indicar puntualmente en su oferta.	CERTIFICACIÓN	PUNTAJE	En Seguridad de la Información (ISO 27001)	5	Gestión de la Continuidad de Negocio (ISO 22301)	5	10 PUNTOS
CERTIFICACIÓN	PUNTAJE							
En Seguridad de la Información (ISO 27001)	5							
Gestión de la Continuidad de Negocio (ISO 22301)	5							

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	
		Página 54 de 55
UNIDAD REQUIRENTE:	COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

Oferta Económica	La oferta económica se evaluará aplicando un criterio inversamente proporcional; a menor precio, mayor puntaje. Se otorgará el máximo puntaje a la o las ofertas que presenten el mejor costo, y a las demás ofertas se asignará un puntaje directamente proporcional. Para la puntuación proporcional de la oferta económica se utilizará la siguiente fórmula: $\text{Puntaje} = \frac{\text{Oferta económica menor} \times 50}{\text{Oferta económica presentada por cada oferente}}$	50 PUNTOS
------------------	---	-----------

Para la valoración se observarán los siguientes parámetros:

Parámetro	Valoración por puntaje
Experiencia General	10
Experiencia específica	20
Experiencia del personal técnico	10
Otro(s) parámetro(s) resuelto(s) por la entidad: Bonificación por certificaciones de empresa respecto a Gestión de calidad. Continuidad del Negocio.	10
Oferta económica	50
TOTAL	100

5 DOCUMENTOS ANEXOS

- Anexo 1. Matriz de Riesgos
- Anexo 2. Identificación de La Existencia De Tratamiento De Datos Personales en el Objeto Contractual
- Anexo 3. Acuerdo de Niveles de Servicio
- Anexo 4. Verificación de Requisitos Normativa SB
- Anexo 5. Cronograma del Proceso de Giro Especifico del Negocio
- Anexo 6. Forma de Presentación de Ofertas
- Anexo 7. Formularios de la Oferta

 GSBS-PA-P08-S01-FO-03	BASES DEL CONCURSO	Fecha: JULIO 2026
	PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATACENTER	Página 55 de 55
	UNIDAD REQUIRENTE: COORDINACIÓN DE TECNOLOGÍA / DIRECCION DE INFRAESTRUCTURA TECNOLÓGICA	

FIRMA DE RESPONSABILIDAD:

NOMBRES Y APELLIDOS	CARGO	FIRMA
Elaborado por: Ing. Carla Corrales	Analista Senior de Infraestructura	
Elaborado por: Ing. Fernando Silva	Especialista de Aseguramiento de la calidad	
Revisado por: Ing. Tatiana Aldaz	Directora de Infraestructura Tecnológica.	
Revisado por: Ing. Juan Pablo Jácome	Director de seguridad Informática y Aseguramiento de la Calidad (E)	
Aprobado por: Ing. Richard Osorio	Coordinador de Tecnología	