CORPORACIÓN BANANERA NACIONAL, S.A.
PROVEEDURÍA GENERAL DE BIENES Y SERVICIOS ADMINISTRATIVOS

PROCEDIMIENTO DE COTIZACIÓN RESTRINGIDO
N°CORBANA-PGBS-PCR-0023-2024

CONTRATACIÓN DE SOLUCIÓN DE RESPALDO VEEAM

DICIEMBRE, 2024

CAPITULO I

CONDICIONES GENERALES

1. OBJETO

Corporación Bananera Nacional, S.A., (en adelante CORBANA), con cédula jurídica N°3-101-018968-18, presenta las especificaciones técnicas y condiciones generales del Procedimiento de Cotización Restringido N°CORBANA-PGBS-PCR-0023-2024, para la contratación de los servicios de la solución de Respaldo Veeam para la Dirección de Tecnología de Información, ubicada en Oficinas Centrales en Zapote, provincia de San José.

CAPITULO II

CONDICIONES PARTICULARES

2. DESCRIPCIÓN DE LA CONTRATACIÓN

El presente proceso corresponde a la contratación de la adquisición de solución de respaldo Veeam para mejorar el sistema de respaldos de CORBANA, agregando la protección de inmutabilidad para la protección avanzada ante el posible robo de información.

En el Capítulo III de Especificaciones Técnicas del presente cartel, se detallan todos los aspectos técnicos requeridos para esta solución.

CORBANA, para esta contratación, designará al MAP Alonso Rodríguez Arguedas, Director de Tecnología de Información, como encargado de la recepción de la solución de respaldo Veeam.

Por lo tanto, toda consulta debe ser dirigidas al señor MAP Alonso Rodríguez Arguedas, al correo electrónico arodriguez@corbana.co.cr con copia a la señora Luisa Castillo Mora, al correo lcastillo@corbana.co.cr

El oferente que resulte adjudicado deberá acatar todas las condiciones generales y especificaciones técnicas descritas en este cartel.

3. ASPECTOS GENERALES

3.1. El Procedimiento de Cotización Restringido N°CORBANA-PGBS-PCR-0023-2024 regulado en este cartel, se regirá por el Reglamento General de Contrataciones de CORBANA S.A.

3.2. CORBANA se reserva el derecho de adjudicar, declarar desierto o infructuoso, si considera que las ofertas presentadas no satisfacen los intereses perseguidos con esta contratación, por cualquier motivo. Asimismo, CORBANA se reserva el derecho de negociar una mejora en las condiciones de las ofertas que se presenten antes de la adjudicación.

3.3. En caso de que la oferta contenga defectos formales subsanables, CORBANA se reserva el derecho de solicitar corregir las omisiones y que se completen los documentos faltantes o que se aclaren elementos de forma.

3.4. Una vez entregada la oferta a CORBANA, ésta pasará a ser propiedad de CORBANA.

3.5. Formará parte de la propuesta tanto la oferta en sí, que se encuentre debidamente firmada por el representante legal, como cualquier documento que la acompañe.

3.6. En la oferta deberá indicarse el nombre completo del participante o la empresa oferente.

3.7. El oferente deberá indicar en su propuesta económica la vigencia, la cual no podrá ser inferior a **45 días naturales,** contados a partir del día de la apertura de las ofertas. Toda propuesta que no indique el plazo de vigencia será considerada con ajuste al plazo mínimo citado. De presentarse una indicación expresa de una vigencia inferior al plazo mínimo, no será admitida.

3.8. El oferente deberá indicar expresamente en su oferta el domicilio contractual (dirección exacta) y una dirección electrónica en las cuales, en una u otra a elección de CORBANA, podrá recibir notificaciones referentes a este Procedimiento de Cotización Restringido N°CORBANA-PGBS-PCR-0023-2024, así como un número de teléfono. Esta información deberá ser incluida en el FORMULARIO N°1 “INFORMACIÓN DEL OFERENTE” que forma parte de este cartel.

3.9. El participante debe indicar claramente el tiempo de entrega **en días naturales**, contemplando lo establecido en las especificaciones técnicas. El plazo de entrega empezará a regir a partir de enviada la Orden de Compra por parte de CORBANA, y recibida por parte del proveedor.

3.10. El participante debe indicar el plazo de garantía; así mismo, describir el procedimiento mediante el cual se solicitaría un eventual reclamo de la garantía. La garantía no debe ser menor a un (**1**) año.

3.11. En caso de que cumpla parcialmente lo deberá indicar claramente estableciendo lo que aplique, de no establecer claramente su cumplimiento parcial, significará un incumplimiento en la oferta.

3.12. La evaluación de las ofertas se hará de conformidad con el procedimiento de evaluación establecido en este cartel y la regulación normativa interna de CORBANA.

3.13. Para cada ítem solicitado en los requerimientos con los que el proveedor tenga un cumplimiento del 100%, deberá indicar "**Entendemos, Aceptamos y Cumplimos**".

4. ABREVIATURAS

Las siguientes abreviaturas corresponden a las señaladas en el presente cartel:

Caja Costarricense del Seguro Social	CCSS
Corporación Bananera Nacional, S.A.	CORBANA

5. PRESENTACIÓN Y RECEPCION DE OFERTAS

5.1. La oferta que se presente deberá estar ajustada en su totalidad a lo indicado en el Capítulo III de Especificaciones Técnicas de este cartel.

5.2. La oferta debe ser presentada en idioma español y debe venir firmada digitalmente (certificado digital válido y vigente emitido por el Banco Central de Costa Rica) por el representante legal de la empresa, quien debe acreditar tal condición. Los formularios deberán cumplimentarse de acuerdo con lo que en estos se indica e igualmente deben entregarse firmados digitalmente.

5.3. La oferta se recibirá a más tardar el día **19 de diciembre de 2024** hasta las **16:00 horas**, por medio del correo electrónico a la dirección: lcastillo@corbana.co.cr.

5.4. Las ofertas deberán presentarse como un solo archivo, con el orden del cartel, con un índice de contenido, y todas las páginas deberán estar numeradas en secuencia. Dado que el expediente está soportado en formato digital, CORBANA se reserva el derecho de solicitar cualquier documento original que sea necesario revisar en físico.

5.5. Cotizar a nombre de Corporación Bananera Nacional, S.A. con cédula jurídica: 3-101-018968.

5.6. No se recibirá ninguna oferta, ni documentación adicional después de la hora fijada para la recepción de estas.

6. REQUISITOS DE ADMISIBILIDAD

6.1 El oferente y eventual adjudicado deberán encontrarse al día con el pago de las cuotas obrero-patronales de la CCSS, el día de la apertura de las ofertas, en la adjudicación y en los momentos de pagos.

6.2 El oferente y eventual adjudicado deberá estar inscritos ante la Dirección General de Tributación como contribuyentes y al día con sus obligaciones formales y materiales ante esta o en cualquier tipo de tributo, el día de la apertura de las ofertas, en la adjudicación y en los momentos de pagos.

7. REQUISITOS LEGALES

6.1 Podrán participar en la presente contratación las personas físicas o jurídicas en forma individual (no se aceptan ofertas conjuntas), que cuenten con plena capacidad de actuar debidamente acreditada, por intermedio de su representante legal, aportando los documentos que lo acrediten de conformidad con lo que se indica en los puntos siguientes de este apartado 6, y a quienes no les alcancen las prohibiciones establecidas en la Ley General de Contratación Pública, capítulo V y en el Reglamento General de Contrataciones de CORBANA, artículo 25 párrafo final. Además, deberán hacer transparente cualquier vinculación formal o informal con algún miembro de la Administración de CORBANA, so pena de nulidad de la adjudicación o del contrato. En consecuencia, todos los oferentes deberán presentar una declaración jurada firmada, con firma digital por el representante legal o, en su defecto, con la firma autenticada por abogado, en la cual manifiesten que no les alcanzan esas prohibiciones ni existen vínculos formales o informales con algún miembro de la Administración de CORBANA.

6.2 El oferente deberá **indicar expresamente en su oferta** que CORBANA queda libre de toda responsabilidad civil directa e indirecta o laboral como consecuencia de esta contratación, para lo cual deberá contratar los seguros necesarios ante la entidad correspondiente que lo proteja contra cualquier accidente, personal, daños a terceros y/o cualquier otro tipo de seguros vigente en el mercado.

6.3 El representante legal de la empresa oferente deberá presentar junto con su oferta, una **declaración jurada sencilla,** en la que se indique que cuenta con la disponibilidad de personal calificado subordinado a la empresa oferente para la presente contratación, así como los recursos humanos y materiales necesarios para garantizar el cumplimiento del objeto de esta contratación, en el plazo establecido, para lo cual deberá prever jornadas y cualesquiera otras situaciones que se requieran en materia laboral. Esta declaración jurada deberá tener la firma de la declarante autenticada por un abogado; sin embargo, en caso de ser firma digital no se requiere la autenticación.

8. DOCUMENTOS QUE DEBEN ACOMPAÑAR A LA OFERTA

Además de los requisitos indicados en otros apartados de este cartel, las ofertas se acompañarán de los siguientes documentos:

8.1 El oferente, en caso de persona jurídica, deberá aportar una certificación notarial que incluya certificación de personería y certificación de capital social con vista en el Registro Nacional y propiedad de las acciones (con vista en el libro de registro de accionistas), la cual no deberá tener más de un mes de emitida a la fecha de apertura de ofertas. En caso de que la certificación notarial no certifique el capital social con vista en el Registro Nacional, se podrá complementar con una certificación literal digital emitida por el Registro Nacional, con no más de quince (15) días naturales de emitida a la fecha de la apertura de las ofertas; sin embargo, ambas deberán indicar toda la información necesaria para describir a la persona jurídica oferente, tal como: citas de inscripción, número de su cédula jurídica, domicilio social, plazo de vigencia, representantes, sus facultades, e indicar las limitaciones del poder si las tuviere.

8.2 Copia simple de la cédula de identidad por ambos lados vigente del participante o del representante legal en caso de persona jurídica.

8.3 Declaración jurada de aceptación de los términos y condiciones incluidos en el presente cartel y que cumplen con cada uno de los puntos de la contratación.

9. PRECIO Y FORMA DE PAGO

9.1 El oferente debe indicar en forma clara el precio, con el detalle del monto que corresponde al impuesto sobre el valor agregado (IVA), debe desglosar el precio de la línea a comprar y deberá firmarlo digitalmente el representante legal de la empresa oferente o participante.

9.2 Los precios que contenga la oferta podrán ser expresados en dólares, moneda de curso legal de los Estados Unidos de América o en colones, moneda de curso legal de la República de Costa Rica. Para efectos de comparación de las ofertas, se tomará como referencia el tipo de cambio de venta vigente al momento de la recepción de las ofertas del Banco Central de Costa Rica. Los precios se entenderán firmes, definitivos e invariables.

9.3 Se debe indicar en forma clara el precio total cotizado en números y letras coincidentes, en caso de que haya diferencia entre los montos indicados, prevalecerá el precio más bajo.

9.4 CORBANA no realizará ningún ajuste de precios en la presente contratación, en ninguna circunstancia, salvo alguna excepción contenida en este cartel, por lo que la empresa adjudicada deberá cumplir en plazo y precio según la oferta presentada.

9.5 El participante deberá indicar la forma de pago, aclarándose que CORBANA no realiza pagos por adelantado.

9.6 El eventual oferente adjudicado deberá presentar su factura electrónica al correo facturaelectronica@corbana.co.cr a nombre de CORBANA con los siguientes datos:

Nombre de la razón social: CORPORACIÓN BANANERA NACIONAL S.A.
Cédula Jurídica: 3-101-018968
Provincia: San José
Cantón: San José
Distrito: Zapote
Dirección: 125 metros noreste de Casa Presidencial
Número de Teléfono: 4002-4700

9.7 El eventual oferente adjudicado debe considerar que la fecha máxima de recepción de comprobantes electrónicos es el día 28 del mes en que se emita la factura. La factura que sea emitida con posterioridad al día indicado será rechazada de oficio y corresponderá que se emita la nota de crédito correspondiente. La emisión de la nueva factura deberá realizarse a partir del día 1 del mes siguiente.

9.8 Los pagos se realizarán en la moneda cotizada en la oferta.

9.9 CORBANA verificará, al momento de recibir la solicitud de pago debidamente aprobada por la Administración, que se encuentra al día en el pago de las obligaciones obrero-patronales de la CCSS o que existe, en su caso, el correspondiente arreglo de pago debidamente aceptado y extendido por el Departamento de Cobros Administrativos de la CCSS. Además, deberá estar al día en el cumplimiento de deberes formales y materiales ante la Administración Tributaria y estar al día con el pago correspondiente.

9.10 El oferente que resulte adjudicado deberá considerar que, de acuerdo con la reforma del inciso 3) del artículo 74 de la Ley N° 17 Ley Constitutiva de la Caja Costarricense del Seguro Social (CCSS), en el caso que durante la ejecución del contrato adquiera la condición de morosidad y tenga pagos pendientes por parte de CORBANA, esta podrá retener dichos recursos y girar lo que corresponda a la CCSS. Si, una vez efectuado el pago de las cuotas obrero-patronales, quedara algún remanente a favor del adjudicado, CORBANA le hará entrega de éste.

9.11 De conformidad con lo establecido en la Ley del Impuesto sobre la Renta, artículo 23, inciso g), se retendrá el DOS POR CIENTO (2%) del monto total de este contrato (o el monto que establezca la ley en su momento), en cada pago que se realice, el cual será transferido a la Dirección General de Tributación.

10. EVALUACIÓN DE LAS OFERTAS

10.1 Las ofertas que cumplan con la parte formal serán elegibles para el estudio técnico.
10.2 Las ofertas que cumplan con la aprobación técnica serán elegibles para el estudio final (Estudio de Precios).
10.3 El estudio final dará la adjudicación del proceso a la oferta de menor precio.

10.4 En caso de empate: De producirse un empate, se solicitará a las empresas que mantienen el empate, una nueva oferta que debe venir en sobre cerrado en la fecha y hora que se indicará. De persistir el empate, la Administración de CORBANA, queda en libertad de decidir lo que a su criterio considere oportuno, una vez considerados y evaluados los puntos antes citados.

11. MULTAS Y SANCIONES

11.1. Si existiera atraso en la entrega del proyecto y este atraso no fuera justificado y aceptado satisfactoriamente ante CORBANA, el contratista deberá pagar a CORBANA por concepto de multa, un 0.5% (cero punto cinco por ciento) del valor total del monto adjudicado, por cada día natural de atraso en la entrega a entera satisfacción de CORBANA.

11.2. Se analizará como días de atraso a justificar únicamente aquellos que hayan sido causados por motivos de fuerza mayor o caso fortuito, contados en forma objetiva, para lo cual el oferente adjudicado deberá presentar la documentación y prueba que respalde los hechos alegados.

11.3. CORBANA se reserva el derecho de hacer efectivas las multas por entrega tardía contra el monto de la garantía de cumplimiento.

12. RECLAMOS CONTRA CORBANA

12.1. No se atenderán reclamos ni se compensará en forma alguna los precios pactados, ya que el hecho de presentar la oferta implica plena aceptación de todas las cláusulas, condiciones, instrucciones y especificaciones de este servicio.

12.2. Cualquier reclamo contra CORBANA relacionado con esta contratación por diferencias en la forma de ejecución, deberá ser presentado, por escrito y ante la Proveeduría General de Bienes y Servicios Administrativos de CORBANA, a los correos wmunoz@corbana.co.cr del señor William Muñoz Rodríguez, Proveedor General con copia al correo lcastillo@corbana.co.cr de la señora Luisa Castillo Mora, encargada de la compra y al señor Alonso Rodríguez Arguedas, Director de Tecnología de Información de CORBANA, al correo arodriguez@corbana.co.cr **dos (2) días naturales** posteriores a que el oferente adjudicado conozca o deba conocer la causa que les dio origen. Pasado este término, se entenderá que el oferente adjudicado no tiene ninguna reclamación contra CORBANA.

13. RENUNCIA A INTERESES

13.1. CORBANA no tendrá obligación de pagar intereses y el oferente adjudicado, por consiguiente, desiste del derecho de recuperarlos con respecto a dineros que CORBANA es obligado a retener por razones de juicios, órdenes, decretos, procesos judiciales y depósitos de garantía o cumplimiento.

CAPITULO III

ESPECIFICACIONES TECNICAS

VEEAM DATA PLATFORM FOUNDATION

Se debe de incluir el Software de respaldos necesario para 10 máquinas virtuales que cumpla con las siguientes características:

1. Software de Respaldos

1.1 La solución ofrecida debe licenciarse bajo un esquema de suscripción que incluya licencias y soporte, debe licenciarse con el formato de cargas de trabajos y debe permitir proteger 10 cargas de trabajo que pueden ser máquinas físicas, máquinas virtuales o en nube con el mismo esquema de licenciamiento, los sistemas operativos de las 10 cargas de trabajo se distribuyen en Windows Server 2022 y 2019.

1.2 Las cargas de trabajo se distribuyen en 1.6 TB Onpremise y 6.1 TB en nube de OCI.

- Onpremise: VM1: 128GB, VM2: 300GB, VM3:128GB, VM4: 550GB, VM5: 200GB, VM6 128GB, VM7:128GB

- Nube OCI: VM1: 5.8 TB, VM2:150GB, VM3:150 GB

1.3 La consola de administración debe de estar alojada en una máquina virtual en nube, la cual será suministrada por Corbana.

1.4 La solución ofrecida debe proporcionar una copia de seguridad eficiente 'incremental para siempre' e incluir opciones de copias de seguridad completas y ad-hoc.

1.5 La solución ofrecida debe detectar automáticamente el espacio libre del datastore productivo y evitar el snapshot de copia de seguridad si el espacio está por debajo del umbral definido.

1.6 La solución ofrecida debe monitorear automáticamente la latencia del datastore productivo durante la copia de seguridad y reducir la velocidad de la copia de seguridad si la latencia del datastore supera un umbral definido.

1.7 La solución ofrecida debe permitir la exclusión de discos de máquinas virtuales y archivos de intercambio (swap) en copias de seguridad basadas en snapshots.

1.8 La solución ofrecida debe permitir la exclusión de archivos y carpetas de la copia de seguridad basada en snapshots.

1.9 La solución ofrecida debe permitir la exclusión de los bloques marcados como eliminados para reducir el tamaño de la copia de seguridad y aumentar el rendimiento del respaldo.

1.10 Conocer si la solución ofrecida requiere o no agentes implementados en máquinas virtuales o físicas.

1.11 La solución ofrecida no debe necesitar realizar copias de seguridad de sistema operativo separadas de las copias de seguridad de datos de la aplicación en máquinas virtuales para facilitar la recuperación granular de elementos de la aplicación.

1.12 La copia de seguridad sin agente de máquinas virtuales debe truncar los registros de transacciones o archivos de Microsoft SQL, Microsoft Exchange y Oracle Database.

1.13 La copia de seguridad sin agente de máquinas virtuales debe proporcionar copias de seguridad de registros o archivos de transacciones de Microsoft SQL, Oracle Database y PostgreSQL junto con copias de seguridad basadas en snapshots.

1.14 La solución ofrecida debe permitir la recuperación de archivos y elementos de aplicaciones sin instalar Agentes o plugins en Máquinas Virtuales.

1.15 La solución ofrecida debe integrarse con los sistemas de almacenamiento y utilizar snapshots de almacenamiento para las operaciones de respaldo.

1.16 La solución ofrecida deberá proporcionar la capacidad de explorar máquinas virtuales en snapshots de almacenamiento y recuperar instantáneamente la máquina virtual, el archivo del sistema operativo o la carpeta o los elementos de la aplicación directamente desde el snapshot de almacenamiento. Esta capacidad también debe aplicarse a los snapshots de almacenamiento creados independientemente de la aplicación de respaldo.

1.17 La solución ofrecida deberá poder utilizar snapshots de almacenamiento para crear una copia de la máquina virtual en un entorno de red aislado para fines de prueba.

1.18 La solución ofrecida debe admitir copias de seguridad físicas de sistemas operativos Windows, Linux, UNIX y MAC.

1.19 La solución ofrecida debe facilitar la copia de seguridad a nivel de imagen y de archivo de entornos físicos o basados en la nube.

1.20 La solución ofrecida debe utilizar la tecnología Changed Block Tracking para copias de seguridad incrementales de cargas de trabajo físicas o basadas en la nube.

1.21 La solución ofrecida debe admitir la copia de seguridad de los servidores de Windows configurados como clúster.

1.22 La solución ofrecida debe proporcionar complementos de respaldo para las aplicaciones MS SQL, Oracle RMAN y SAP HANA, permitiendo la centralización de repositorio.

1.23 La solución ofrecida debe proporcionar conocimiento de la aplicación al realizar copias de seguridad de MySQL y PostgreSQL que se ejecutan en Linux.

1.24 La solución ofrecida debe permitir mover los archivos de respaldo entre cualquier tipo de repositorio de respaldo (aun cuando el repositorio destino sea de un tipo distinto al del origen) sin necesidad de usar la gestión regular de archivos (copiar/pegar)

1.25 La solución ofrecida debe permitir mover los respaldos entre las tareas y copiar los respaldos entre repositorios.

1.26 La solución ofrecida debe proporcionar una portabilidad completa en cualquier archivo de respaldo propietario y no debe depender de ninguna infraestructura de respaldo como, por ejemplo, el catálogo central, para la recuperación.

1.27 La solución ofrecida debe proporcionar la tecnología de recuperación Changed Block Tracking para máquinas virtuales VMware, Hyper-V.

1.28 La solución ofrecida debe permitir que las copias de seguridad de máquinas virtuales en la nube puedan ser restauradas en cualquier nube pública o volver a una máquina virtual en un hipervisor local en las instalaciones.

1.29 La solución ofrecida debe escanear los datos de la máquina virtual con un software antivirus antes de restaurar la máquina al entorno de producción. La solución ofrecida debe abortar la operación de recuperación si se detecta malware.

1.30 La solución ofrecida debe proporcionar la capacidad de iniciar la máquina virtual en un entorno de red aislado durante el proceso de recuperación e inyectar un script en el sistema operativo invitado que permita que el servidor se modifique para fines de cumplimiento antes de la recuperación.

1.31 La solución ofrecida debe proporcionar una recuperación completa de la copia de seguridad basada en el Agente con la capacidad de crear un medio de arranque para el servidor específico, del tipo bare metal.

1.32 La solución ofrecida debe permitir la recuperación instantánea de copias de seguridad basadas en agentes para VMware o máquinas virtuales Hyper-V.

1.33 La solución ofrecida debe convertir automáticamente UEFI a BIOS durante la operación de recuperación de Amazon AWS.

1.34 La solución ofrecida debe facilitar las operaciones de recuperación a nivel de archivo sin la necesidad de implementar un agente o plugin de recuperación en un servidor virtual o físico.

1.35 La solución ofrecida debe poder recuperar archivos en un sistema operativo invitado de máquina virtual incluso cuando no haya conexión de red entre el servidor de respaldo y la máquina virtual.

1.36 La solución ofrecida debe permitir delegar operaciones de restauración y proporcionar una interfaz de usuario de autoservicio basada en la web y la capacidad de buscar máquinas, recursos compartidos de archivos y archivos específicos en todas las copias de seguridad.

1.37 La solución ofrecida debe permitir restaurar las listas de control de acceso (ACL) de archivos y carpetas sin la necesidad de sobre escribir los archivos.

1.38 La solución ofrecida debe admitir la recuperación granular de las aplicaciones de Microsoft Active Directory, Exchange, SQL, SharePoint y PostgreSQL.

1.39 La solución ofrecida debe admitir la recuperación granular de bases de datos Oracle a partir de copias de seguridad basadas en imágenes u Oracle RMAN.

1.40 La solución ofrecida no debe usar un producto de terceros para la recuperación granular de elementos de la aplicación.

1.41 La solución ofrecida debe proporcionar una interfaz de usuario de autoservicio basada en la web y la capacidad de examinar y recuperar elementos de Microsoft Exchange y bases de datos SQL u Oracle.

1.42 La solución ofrecida debe permitir la recuperación instantánea de base de datos SQL u Oracle desde la copia de seguridad al último estado o a un punto anterior en el tiempo a cualquier servidor de base de datos de producción o clúster (físico o virtual) en minutos, independientemente de su tamaño.

1.43 La solución ofrecida debe estar definida por software y ser capaz de ejecutarse localmente o en cualquier plataforma en la nube.

1.44 La solución ofrecida debe ser independiente del almacenamiento y debe contar con tecnología integrada de duplicación y compresión.

1.45 La solución ofrecida deberá asegurar las copias de seguridad en repositorios reforzados a prueba de malware y hackers con copias de seguridad inmutables, para prevenir el cifrado o eliminación por ransomware y debe admitir credenciales que se usan una sola vez y no ser almacenadas en la infraestructura de respaldo, así si el servidor de respaldo se ve comprometido, un atacante no puede obtener las credenciales y conectarse al repositorio reforzado.

1.46 La solución ofrecida debe poder escalar tanto horizontal como verticalmente.

1.47 La solución ofrecida debe proporcionar un mecanismo fácil para expandir o contratar el almacenamiento de respaldo de destino.

1.48 La solución ofrecida debe ofrecer la flexibilidad para ajustar el tamaño del bloque deduplicación de datos y el nivel de compresión de datos.

1.49 La solución ofrecida debe admitir de forma nativa la copia del respaldo a cinta y no debe requerir software adicional para su administración.

1.50 La solución ofrecida debe admitir de forma nativa como repositorio y el traslado de archivos de respaldo a Amazon S3 (con inmutabilidad), IBM Cloud Object Storage, Azure Blob Cloud Storage (con inmutabilidad), Google Cloud Storage, y otras plataformas de almacenamiento en la nube compatibles con S3.

1.51 La solución ofrecida debe admitir de forma nativa el traslado de archivos de respaldo a Amazon S3 Glacier (incluido Deep Archive) con capacidad de inmutabilidad, y Microsoft Azure Blob Storage Archive Tier para archivado a largo plazo de copias de seguridad

1.52 La solución ofrecida debe proporcionar una recuperación incremental y granular del almacenamiento de objetos basado en la nube.

1.53 La solución ofrecida debe proporcionar soporte para el almacenamiento de objetos en las instalaciones.

1.54 La solución ofrecida debe ofrecer un movimiento incremental de datos hacia y desde el almacenamiento basado en objetos.

1.55 La solución ofrecida debe ofrecer inmutabilidad en el almacenamiento de objetos S3 a nivel de depósito.

1.56 La solución ofrecida debe tener la opción de copiar o mover datos al almacenamiento de objetos al finalizar la copia de seguridad. Idealmente, ambas opciones se pueden combinar.

1.57 La solución ofrecida debe encriptar los archivos de respaldo usando el encriptado AES de 256 bits. El cifrado no debe depender de la plataforma de almacenamiento de respaldo.

1.58 La solución ofrecida debe proporcionar un cifrado AES de 256 bits con tecnología de protección de pérdida de contraseña, por lo que los datos se pueden descifrar si se pierde la contraseña operativa.

1.59 Todos los componentes de La solución ofrecida de respaldo deben admitir autenticación Kerberos.

1.60 La solución ofrecida debe integrarse con autenticación de credenciales del tipo gMSA.

1.61 La solución ofrecida debe permitir autenticación multifactor (MFA) para una verificación adicional de usuario en la consola de administración de la solución.

1.62 La solución ofrecida debe integrarse con SAML 2.0 para la autenticación extendida.

1.63 La solución ofrecida debe proporcionar control de acceso basado en roles a través de una interfaz de usuario web para la mayoría de las operaciones de recuperación y respaldo.

1.64 La solución ofrecida debe leer y verificar automáticamente la consistencia de los datos de producción en el archivo de copia de seguridad una vez completada la copia de seguridad. En caso de que se detecte corrupción de datos, La solución ofrecida debe reconstruir automáticamente el bloque dañado con datos de producción.

1.65 La solución ofrecida deberá iniciar automáticamente las máquinas virtuales de VMware y Hyper-V Windows y Linux así como de agentes de nube y físicas a partir de copias de seguridad y verificar el sistema operativo y la disponibilidad de la aplicación. Esta prueba no debe tener impacto en la red de producción. La solución ofrecida debe proporcionar un informe de verificación de recuperación.

1.66 La solución ofrecida debe escanear automáticamente los datos de producción en busca de virus durante la verificación de respaldo.

1.67 La solución ofrecida debe poder utilizar la copia de seguridad o réplica de la máquina virtual para crear una copia de la máquina virtual en un entorno de red aislado para fines de prueba.

1.68 La solución ofrecida debe incluir un mecanismo de copia de seguridad fuera del sitio con la capacidad de seleccionar individualmente los conjuntos de copias de seguridad que deben copiarse y definir una retención diferente de las copias de seguridad en el almacenamiento secundario de copias de seguridad.

1.69 La solución ofrecida debe presentar tecnología de aceleración WAN incorporada para la replicación de datos con la capacidad de limitar la utilización del ancho de banda.

1.70 La solución ofrecida debe proporcionar una copia de seguridad eficiente basada en archivos incrementales.

1.71 La solución ofrecida debe admitir recursos compartidos de archivos basados en NFS, SMB, Windows y Linux.

1.72 La solución ofrecida debe aprovechar los snapshots de VSS cuando sea posible

1.73 La solución ofrecida debe proporcionar una recuperación incremental a cualquier plataforma objetivo-heterogénea

1.74 La solución ofrecida debe proporcionar la capacidad de archivo granular de archivos, archivando tipos de archivos específicos.

1.75 La solución ofrecida debe estar desarrollada para tareas de protección y recuperación ante desastres para entornos Amazon Elastic Compute Cloud (EC2), Amazon Relational Database Service (RDS) y Amazon Elastic File System (EFS). También debe permitir respaldar y restaurar las configuraciones de Amazon Virtual Private Cloud (VPC).

1.76 La solución ofrecida debe poder realizar las siguientes operaciones de protección de datos: crear instantáneas nativas de la nube de instancias EC2, crear instantáneas nativas de la nube de los recursos de RDS, crear copias de seguridad a nivel de imagen de instancias EC2 y crear copias de seguridad de los sistemas de archivos EFS.

1.77 La solución ofrecida debe poder realizar las siguientes operaciones de recuperación de datos respaldados: restaurar instancias EC2 completas, restaurar volúmenes de instancias EC2, restaurar archivos y carpetas de instancia EC2, restaurar instancias de base de datos

de RDS, restaurar sistemas de archivos EFS completos, así como archivos y directorios EFS, configuraciones completas y elementos específicos de configuraciones de VPC.

1.78 La solución ofrecida debe estar desarrollada para tareas de protección y recuperación ante desastres para entornos de Microsoft Azure.

1.79 La solución ofrecida de poder realizar las siguientes operaciones: crear copias de seguridad a nivel de imagen e instantáneas nativas de la nube de máquinas virtuales de Azure, crear copias de seguridad a nivel de imagen de las bases de datos de Azure SQL, crear instantáneas nativas en la nube de recursos compartidos de archivos de Azure, restaurar archivos individuales de recursos compartidos de archivos de Azure, bases de datos específicas de Azure SQL, máquinas virtuales de Azure completas, discos virtuales individuales y archivos y carpetas del sistema operativo invitado.

1.80 La solución debe permitir el escaneo in-line de los backups con bajo impacto utilizando análisis de entropía con Machine Learning para detectar datos encriptados por un malware.

1.81 El escaneo in-line también debe detectar onion links, cambios en el file system, comparar metadatos como grado de compresión de los archivos y cambios masivos en la extensión de estos.

1.82 La solución debe permitir escanear los backups en los repositorios bajo demanda o de manera agendada para detectar los backups limpios y sospechosos.

1.83 La solución debe poder invocar al antivirus instalado en el Mount Server de Veeam.

1.84 La solución debe permitir aplicar búsquedas con regla YARA para detectar malware o cumplir con compliance.

1.85 La solución debe generar sus eventos en formato SYSLOG y ser capaz de enviar dichos eventos a herramientas SIEM como SPLUNK, Crowdstrike, Palo Alto, Microsoft Sentinel, Fortinet, IBM Qradar y otros.

1.86 La solución debe hacer seguimientos de eventos durante los escaneos y marcar las imágenes de backup como sospechosas para evitar la reinfección en producción.

1.87 La solución debe ofrecer una Incident API que pueda ser consumida por cualquier herramienta de seguridad que al detectar un ataque o incidente pueda avisarle a Veeam del incidente y poder hacer un quick backup del equipo que está bajo ataque.

1.88 La solución debe integrarse con ServiceNow en forma bidireccional para otorgar visibilidad de los backups en la consola de ServiceNow, poder crear y resolver automáticamente tickets de incidentes en ServiceNow, ofrecer un Backup Dashboard en la consola de ServiceNow y templates de backup para ser aplicados al momento de provisionar VMs desde ServiceNow.

1.89 La solución debe poder realizar las siguientes operaciones de recuperación de datos respaldados: restaurar instancias EC2 completas, restaurar volúmenes de instancias EC2, restaurar archivos y carpetas de instancia EC2, restaurar instancias de base de datos de RDS, restaurar sistemas de archivos EFS completos, así como archivos y directorios EFS, configuraciones completas y elementos específicos de configuraciones de VPC.

1.90 La solución debe estar desarrollada para tareas de protección y recuperación ante desastres para entornos de Microsoft Azure protegiendo Azure VMs, AzureSQL, Azure File Share y Azure Virtual Network Configuration.

1.91 La solución debe poder realizar las siguientes operaciones: crear copias de seguridad a nivel de imagen e instantáneas nativas de la nube de máquinas virtuales de Azure, crear copias de seguridad a nivel de imagen de las bases de datos de Azure SQL, crear instantáneas nativas en la nube de recursos compartidos de archivos de Azure, restaurar archivos individuales de recursos compartidos de archivos de Azure, bases de datos específicas de Azure SQL, máquinas virtuales de Azure completas, discos virtuales individuales y archivos y carpetas del sistema operativo invitado

1.92 La solución debe proporcionar información del estado de protección de cargas de trabajo virtuales, físicas o basadas en nube.

1.93 La solución debe alertar sobre trabajos de respaldo fallidos y trabajos que exceden la ventana de respaldo

1.94 La solución debe alertar por adelantado si el objetivo de la copia de seguridad se acerca a la capacidad.

1.95 La solución debe proporcionar alertas proactivas para eliminar problemas. Estos problemas deben detectarse automáticamente, abarcar la configuración y el rendimiento, y el proveedor debe actualizar dinámicamente la detección.

1.96 La solución debe proporcionar un informe de evaluación de Infraestructura VMware para asegurar que el entorno esté preparado para las operaciones de respaldo basadas en snapshots y detectar máquinas virtuales que requieren implementación de respaldo basada en agente.

1.97 La solución debe proporcionar un informe de autoevaluación. El informe debe detectar si la solución se implementa de acuerdo con las mejores prácticas.

1.98 La solución debe proporcionar un informe sobre máquinas virtuales que no están protegidas por copia de seguridad y un informe de cumplimiento de RPO (Objetivo del punto de recuperación) para las máquinas virtuales protegidas.

1.99 La solución debe proporcionar planificación de capacidad y pronosticar la utilización del espacio de almacenamiento de respaldo.

1.100 La solución debe proporcionar un informe automatizado sobre todas las operaciones de recuperación para fines de auditoría.

1.101 La solución debe proporcionar una infraestructura de respaldo y un informe de cambios de política para fines de auditoría.

1.102 La solución debe permitir definir dashboards de monitoreo personalizados e integraciones con sistemas ITSM con la ayuda de REST APIs.

1.103 La solución debe permitir programar la entrega automática de dashboards, informes y carpetas de informes. Se debe poder optar por recibir dashboards e informes por correo electrónico, guardar dashboards e informes en una carpeta local o recurso compartido de red.

1.104 La solución debe notificar a los usuarios sobre eventos importantes, cambios y posibles problemas en el entorno virtual y de copia de respaldo.

1.105 La solución debe ser capaz de tomar acciones de remediación como por ejemplo ejecutar un script que encienda una VM, o ejecutar un script que agregue una VM a un trabajo de respaldo existente o ejecutar un script que elimine el último snapshot en VMware o que elimine el último checkpoint en HyperV.

2. Almacenamiento o repositorio

2.1 La solución debe de contemplar el costo del almacenamiento en X nube.

2.2 Se debe de indicar bajo dos (2) escenarios el costo del almacenamiento en la nube de Veeam y el costo en X nube publica (Azure, OCI, AWS, Google).

2.3 El almacenamiento inicial será de 5 TB, indicando el costo con la posibilidad de aumentar durante el año 2025 1 TB.

3. Servicios de implementación, configuración, soporte y capacitación

El oferente debe ofrecer los siguientes servicios:

3.1 Servicio de Instalación, configuración y documentación de la solución ofertada.

- 3.1.1 El oferente deberá de indicar el código de licenciamiento ofrecido.
- 3.1.2 El oferente deberá de indicar en una línea especifica el costo por instalación y el tiempo de esta.
- 3.1.3 Planificación y Diseño: definición de la estrategia de respaldo y recuperación.
- 3.1.4 Instalación y despliegue de la solución ofrecida.
- 3.1.5 Configuración de repositorio de datos en almacenamiento definido.
- 3.1.6 Configuración Notificaciones al personal definido en la estrategia de respaldo y recuperación para el control de los respaldos.
- 3.1.7 Configuración de políticas de respaldo para cargas de trabajo, utilizando el esquema de full sintético los fines de semana e incrementales entre semana.
- 3.1.8 Validación de funcionamiento: pruebas de respaldo de las 1 cargas de trabajo y de la recuperación de archivos.

3.1.9 Diagrama de la solución brindada.

3.1.10 Documentación.

3.1.11 Revisión ejecución de respaldos una vez al mes durante el periodo del contrato.

3.1.12 Identificación de errores y resolución en conjunto con personal de la dirección de tecnología de información.

3.1.13 Análisis de crecimiento mensual de los respaldos durante el periodo del contrato.

3.1.14 Identificación de limitaciones en las operaciones de respaldos y propuesta de mitigación una vez al mes

3.1.15 Reporte y corrección de vulnerabilidades en forma trimestral

3.1.16 Capacitación de la solución oferta, de al menos 8 horas para 6 personas del Departamento de Tecnología de la Corporación Bananera Nacional

3.1.17 Soporte correctivo en la solución implementada (2 horas por mes) por el periodo del contrato.

3.1.18 Mantenimiento preventivo semestral con actualización por el periodo del contrato

3.1.19 Validaciones de los respaldos en forma trimestral.

4. Requisitos de Admisibilidad para la solución de respaldos

4.1 El oferente debe aportar certificación extendida por el fabricante de la marca ofertada, en la que haga constar que el oferente es canal autorizado de la marca ofrecida y que está autorizado para la venta, soporte y distribución del objeto ofertado.

4.2 El oferente debe contar con al menos 3 años de relación comercial con el fabricante, por lo que la certificación extendida por el fabricante debe indicar claramente la fecha desde que el oferente es canal autorizado de la marca ofrecida para la venta, soporte y distribución del objeto ofertado, con el fin de verificar los años de relación con el fabricante.

4.3 El oferente de la solución de protección de datos debe ser un “Distribuidor”, con el máximo nivel de Partner del Fabricante de la solución de respaldos.

4.4 La certificación debe de tener un máximo de tres meses de emitida, contados a partir de la fecha de la apertura de ofertas, debe indicar, la fecha de emisión y nombre, número de teléfono y correo electrónico del contacto del fabricante.

4.5 El oferente debe haber realizado en los últimos 3 años, previo a la apertura de la oferta, al menos 2 ventas con su respectiva implementación, finalizadas o en ejecución del objeto ofertado en el país con la solución de respaldo ofertada.

4.6 Para acreditar dicha información, el oferente deberá aportar al menos dos cartas o declaraciones juradas de referencias de clientes donde se certifique dicha condición, y se contemplen los siguientes puntos:

4.6.1 La carta o declaración jurada debe ser de dos proyectos diferentes recibidos a satisfacción por el cliente y debe incluir los siguientes ítems:

- Nombre de la empresa o institución donde se realizó la implementación.
- Nombre del proyecto.
- Breve descripción del proyecto, especificando la cantidad de máquinas virtuales que se respaldan.
- Fecha de inicio y final del proyecto.
- Información de contacto del encargado o autorizado del proyecto: Nombre, número de teléfono y correo electrónico.
- Firma del encargado o autorizado del proyecto.

FORMULARIO N°1

INFORMACIÓN DEL OFERENTE

,____de_____del 2024

Señores
Corporación Bananera Nacional S.A.

Estimados señores:

Por este medio brindo la información de resumen en mi condición de oferente:

Nombre o razón social del oferente: _____

Cédula física o jurídica del oferente: _____

Tel: _____ Fax: _____ Dirección Postal: _____

Correo electrónico para notificaciones: _____

Provincia: _____ Cantón: _____ Distrito: _____

Dirección (domicilio exacto): _____

Nombre del apoderado: _____

Cédula de identidad del apoderado: _____

Cargo que ocupa en la empresa: _____

Firma del participante o _____
Representante legal:
(La autenticación no será requerida cuando el documento se suscriba mediante firma digital)

Autenticación de firmas: Doy fe de que la firma que consta en este documento fue estampada en mi presencia. Lugar**:** _____ Fecha: __/__/____

Licenciado(a): _____ Carné: _____