BOLETÍN DE ACLARACIONES NRO. 1
DN Adquisición herramienta gestión de accesos privilegiados
CÓDIGO: EC-L1253-P00098

PREGUNTA 1.-
Pregunta sobre servidores virtuales: El TDR indica que la herramienta debe ser una solución basada en software implementada "ON-PREMISE" y compatible con servidores virtuales provistos por el SRI. ¿Cuáles son las especificaciones técnicas detalladas (CPU, RAM, almacenamiento, sistema operativo base) de la infraestructura virtual que pondrá a disposición el SRI para el despliegue tanto en producción como en contingencia?

RESPUESTA 1.-
Estimado oferente, la solución propuesta deberá instalarse como máquina(s) virtual(es) dentro de la infraestructura de virtualización VMware existente en el SRI. El contratista deberá proveer todo el licenciamiento necesario para la implementación de la Herramienta de Gestión de Accesos Privilegiados en producción y contingencia, así como cualquier licenciamiento adicional requerido para el funcionamiento de la herramienta, conforme lo establecido en la sección II. Licenciamiento/Suscripción y Mantenimiento/Soporte de Fábrica.

PREGUNTA 2.-
Pregunta sobre la Alta Disponibilidad: Se especifica que la solución debe configurarse en modo activo-pasivo y contar con redundancia en producción. ¿El balanceador de carga o los mecanismos de red para la conmutación (failover) entre el sitio de producción y contingencia serán provistos por el SRI, o deben ser incluidos y configurados en su totalidad por el proveedor?

RESPUESTA 2.-
Estimado oferente:

En el apartado VI. Implementación, sección 7. SERVICIOS CONEXOS REQUERIDOS se indica que: "*El contratista deberá realizar la implementación de la Herramienta de Gestión de Accesos Privilegiados en el ambiente de producción y contingencia en modo activo-pasivo, es decir que* ***la solución entrará a operar en contingencia una vez que se realice los procedimientos para trasladar la operación de la solución desde el ambiente de producción a contingencia***." [énfasis añadido]

Adicionalmente, refiérase a la Enmienda Nro. 4 del Boletín de Enmiendas Nro.1 donde se establece que: "*La herramienta deberá ser implementada en los ambientes de producción y contingencia en alta disponibilidad (24x7x365). La herramienta deberá tener al menos dos instancias (nodos) en el ambiente de producción. En el ambiente de contingencia deberá tener al menos una instancia (nodo). La instancia de producción debe replicarse al ambiente de contingencia, con toda la información necesaria para mantener la administración en un*

caso de falla del ambiente de producción. ***Si es requerido componentes y/o softwares adicionales, el proveedor deberá incluirlo como parte de la herramienta ofertada.***" [énfasis añadido]

PREGUNTA 3.-
Pregunta sobre Autoadministración de la Base de Datos: Las especificaciones indican que si la herramienta utiliza una base de datos como back-end, esta debe ser autoadministrable sin requerir un DBA para mantenimiento o *hardening*. Si la solución ofertada incluye una base de datos embebida licenciada por el propio fabricante que cumple con esto, ¿se requerirá algún tipo de homologación o permiso especial con las políticas internas de bases de datos corporativas del SRI?

RESPUESTA 3.-
Estimado oferente, no se requiere aplicar homologación alguna ni permiso especial en función de las políticas internas de bases de datos corporativas del SRI. Se requiere que la base de datos, embebida o instalada por separado, sea desplegada y configurada aplicando las mejores prácticas del fabricante de la base de datos y de la solución PAM para reducir al mínimo su exposición y la de la solución a explotaciones que intenten extraer, sustituir, modificar, eliminar o consultar sin autorización la información de autenticación, de accesos o de auditoría alojada en la solución PAM.

PREGUNTA 4.-
Pregunta sobre la Integración sin Agentes: Se solicita que la herramienta gestione las plataformas del SRI sin desplegar agentes en los servidores ni en las estaciones de trabajo de los administradores. ¿Existe alguna restricción de red (como protocolos bloqueados por firewalls internos, ej. SSH, RDP, HTTPS) que deba ser considerada previamente para garantizar la administración *agentless*?

RESPUESTA 4.-

Estimado oferente, el contratista deberá informar oportunamente todos los requerimientos de acceso, incluyendo permisos de firewall, para la implementación de la solución PAM de forma justificada. Estos serán evaluados y aplicados de acuerdo con los estándares de seguridad institucionales.

PREGUNTA 5.-
Pregunta sobre la Logística: Se establece que la transferencia de conocimientos debe ser para al menos 9 funcionarios, con una duración mínima de 20 horas basada en capacitación oficial, y que toda la logística correrá por cuenta del contratista. ¿La capacitación se requiere de forma presencial en las instalaciones del SRI en Quito, o se aceptarán modalidades virtuales?

RESPUESTA 5.-
Estimado oferente, "*Toda **logística** asociada con la transferencia de conocimiento correrá por cuenta del Contratista*" [énfasis añadido], de acuerdo con lo establecido en el apartado III. Implementación de la sección 5. METODOLOGÍA DE TRABAJO, y "*La transferencia de conocimientos deberá incluir los materiales, laboratorios con tecnología similar a la herramienta instalada, **equipos, acceso a internet, facilidades y talleres** necesarios para la correcta asimilación del contenido y la generación de destrezas necesarias en los asistentes. Esta actividad no representará costos adicionales para el SRI.*" [énfasis añadido], de acuerdo con lo establecido en el apartado VI. Implementación de la sección 7. SERVICIOS CONEXOS REQUERIDOS.

En consecuencia, la transferencia de conocimientos debe realizarse en un entorno provisto por el contratista que garantice el cumplimiento integral de lo definido en los pliegos. La participación debe ser presencial, salvo los casos específicos que el Administrador del Contrato defina.

PREGUNTA 6.-
Pregunta sobre la vigencia de certificaciones: Para el Líder de Proyecto y los Técnicos se exigen certificaciones específicas vigentes (ej. Gestión de Proyectos o del fabricante). En el caso de certificaciones de fabricantes que no tienen fecha de caducidad explícita (vitalicias o asociadas a una versión específica de software), ¿serán aceptadas como válidas para el cumplimiento del perfil mínimo?

RESPUESTA 6.-
Estimado oferente, se considerará como vigente un certificado que tenga una antigüedad de 5 años o menos a la fecha de presentación de la oferta.

PREGUNTA 7.-
Pregunta sobre el Mantenimiento Correctivo: El pliego menciona un servicio de soporte local 24x7 para la atención y solución de incidentes. ¿El SRI cuenta con una herramienta propia de mesa de ayuda (Ticketing) con la cual deba integrarse el flujo de reportes del proveedor, o las alertas e incidentes se gestionarán mediante los canales directos que proponga el contratista?

RESPUESTA 7.-
Estimado oferente, no se requiere que la solución PAM se integre con la herramienta de gestión de servicios (mesa de ayuda) de la institución.

PREGUNTA 8.-
Pregunta sobre Administración: El pliego dentro del punto 8 menciona." La herramienta deberá tener la capacidad para realizar el aprovisionamiento automática de cuentas a partir

de un Active Directory o LDAP, esto implica que la herramienta deberá ser capaz de integrarse con estos directorios de manera automática y transparente, de modo que pueda **crear, modificar o eliminar cuentas de manera automática** reflejando los cambios que ocurran en los directorios mencionados. ¿El SRI requiere que las tareas de creación, modificación se ejecuten sobre cuentas privilegiadas o se debe incluir la rotación para cuentas de usuario que se encuentran dentro del directorio activo?

RESPUESTA 8.-
Estimado oferente, la solución PAM debe ejecutar las tareas de creación, modificación y eliminación de las cuentas de altos privilegios, no de los usuarios privilegiados (administradores).

PREGUNTA 9.-
Pregunta sobre Administración: El pliego dentro del punto 10 menciona "Operaciones masivas sobre cuentas de altos privilegios propias de la herramienta: La herramienta debe permitir realizar acciones simultáneas o en grupo sobre múltiples cuentas de altos privilegios que están gestionadas directamente por la herramienta." ¿ Más allá de la carga de usuarios y el cambio masivo de contraseñas, ¿cuáles son las otras operaciones específicas que la entidad requiere ejecutar masivamente?

RESPUESTA 9.-
Estimado oferente, por favor, refiérase al numeral 10 del apartado Administración y al apartado Gestión de contraseñas y credenciales, de la sección 6. BIENES REQUERIDOS.

PREGUNTA 10.-
Pregunta sobre Garantía de Mantenimiento de la Oferta: se puede aclarar que se debe emitir una garantía con una aseguradora ó es un documento firmado por el Representante legal como proveedor para cumplir?

RESPUESTA 10.-
Estimado oferente, favor referirse a la Sección V. Formularios de la Oferta, páginas 70 y 72 de la SDO donde se especifica claramente que, tanto para la Garantía Bancaria como Fianza, no aplica para el presente proceso; por el contrario, se deberá observar lo dispuesto en la IAO 20.1 referente a la **Declaración de Mantenimiento de la Oferta**.

PREGUNTA 11.-
Basado en esta pregunta El administrador del contrato podrá realizar el cambio del lugar de entrega si así lo considera necesario, mediante notificación formal al contratista. Cuales serian las posibles lugares.

RESPUESTA 11.-
Estimado oferente, en caso de existir cambios de localidades se mantendrán en la misma ciudad de la instalación original previa coordinación con el Administrador de Contrato.

PREGUNTA 12.-

- **Confirmar si los formularios siguientes se deben llenar y enviar impresos?**

Formulario de Divulgación de la Propiedad Efectiva..... ¡Error! Marcador no definido.
Carta de Aceptación..... ¡Error! Marcador no definido.
Convenio Contractual..... ¡Error! Marcador no definido.
Garantía de Cumplimiento ..... ¡Error! Marcador no definido.
Garantía por Anticipo ..... ¡Error! Marcador no definido.
Fianza de Cumplimiento ..... ¡Error! Marcador no definido.

RESPUESTA 12.-
Estimado oferente, con relación a su consulta se aclara que los formularios enlistados corresponden a la Sección IX. Formularios del Contrato, página 135 de la SDO, en consecuencia, estos formularios deberán ser llenados y presentados por el oferente adjudicado en la etapa correspondiente.

PREGUNTA 13.-
Requerimiento: En el **capítulo 7. Servicios Conexos Requeridos**, en el ítem **VI Implementación**, como parte de los aspectos específicos se indica:

"La implementación deberá incluir:
Instalación y puesta en marcha de todo el software y demás componentes que formen parte de la herramienta de Gestión de Accesos Privilegiados en los ambientes de producción y contingencia; conforme a la arquitectura propuesta por el fabricante"

Pregunta: Para realizar el dimensionamiento de la arquitectura y la infraestructura necesaria para el funcionamiento de la solución ofertada, requerimos conocer: ¿cuántos usuarios se espera que accedan a la plataforma de manera concurrente, es decir al mismo tiempo?

RESPUESTA 13.-
Estimado oferente, para todo efecto práctico se debe dimensionar el licenciamiento, ya sea concurrente o no concurrente, de la solución para el total de 47 administradores, conforme la tabla 1 de la sección 4. INFRAESTRUCTURA ACTUAL.

PREGUNTA 14.-

Requerimiento: En el **capítulo 4. Infraestructura Actual**, de acuerdo con lo indicado en la **Tabla 2. "Dimensionamiento de administradores de la herramienta de Gestión de Accesos Privilegiados",** se especifica que existen 20 administradores que tendrán acceso a las bases de datos.

Pregunta: Para realizar el dimensionamiento de la arquitectura y la infraestructura necesaria para el funcionamiento de la solución ofertada, requerimos conocer: ¿cuántos administradores de base de datos se espera que accedan a de manera concurrente, es decir al mismo tiempo a las bases de datos a través de la plataforma?

RESPUESTA 14.-
Estimado oferente, para todo efecto práctico se debe dimensionar el licenciamiento, ya sea concurrente o no concurrente, de la solución para considerando un total de 20 administradores de bases de datos, conforme la Tabla 2. Dimensionamiento de administradores de la herramienta de Gestión de Accesos Privilegiados de la sección 4. Infraestructura Actual.

PREGUNTA 15.-
Requerimiento: En el capítulo 4. Infraestructura Actual, de acuerdo con lo indicado en la Tabla 2. Dimensionamiento de administradores de la herramienta de Gestión de Accesos Privilegiados se indica que existen varios dispositivos a los que se accede mediante una consola web.
Pregunta: ¿existen dispositivos diferentes a las bases de datos que se conectan mediante aplicaciones ejecutables (clientes instalables), favor indicar cuantos son y cuáles serían?

RESPUESTA 15.-
Estimado oferente, remitirse a las columnas "*Tipo de Conexión al sistema administrado lo detallado*" y "*Nombre de herramienta y versión (Sistema Administrado)*" de la Tabla 2. Dimensionamiento de administradores de la herramienta de Gestión de Accesos Privilegiados de la sección 4. Infraestructura Actual.

PREGUNTA 16.-
Requerimiento: En el **capítulo 4. Infraestructura Actual**, de acuerdo con lo indicado en la **Tabla 2. "Dimensionamiento de administradores de la herramienta de Gestión de Accesos Privilegiados"**, en el ítem **Gestión Interna de Centro de Cómputo (11)**, en la columna de **cantidad** se indica:
"12 licencias Toad for Oracle 17.1

Se debe **considerar la cantidad registrada para el motor de base de datos**
Finalmente, tener en cuenta que los **Administradores**, además de utilizar su cuenta privilegiada de administración, emplean **1081 usuarios privilegiados adicionales** para la gestión de las bases de datos"

Pregunta ¿Se solicita confirmar si estos 1081 usuarios privilegiados corresponden a usuarios que deberán ser licenciados, adicionalmente a los 47 administradores indicados,

RESPUESTA 16.-
Estimado oferente, refiérase a la Enmienda Nro. 1 del Boletín de Enmiendas Nro. 1.

PREGUNTA 17.-
Requerimiento: En el **capítulo 4. Infraestructura Actual**, de acuerdo con lo indicado en la **Tabla 2. "Dimensionamiento de administradores de la herramienta de Gestión de Accesos Privilegiados"**, en el ítem **Gestión Interna de Centro de Cómputo (11)**, en la columna de **Nombre de herramienta y versión (Sistema Administrado)** se indica:
"12 licencias Toad for Oracle 17.1

Se debe **considerar la cantidad registrada para el motor de base de datos.**
Finalmente, tener en cuenta que los **Administradores**, además de utilizar su cuenta privilegiada de administración, emplean **1081 usuarios privilegiados adicionales** para la gestión de las bases de datos"

Pregunta: ¿Se solicita indicar el número total de bases de datos a las que se conectarán los usuarios mediante estos 1081 clientes?

RESPUESTA 17.-
Estimado oferente, remítase a la información proporcionada en las filas 11 y 12, columna *"Cantidad"* de la Tabla 2. *Dimensionamiento de administradores de herramienta de Gestión de Accesos Privilegiados* en la Sección VI. Requisitos de los Bienes y Servicios Conexos.

PREGUNTA 18.-
Requerimiento: el capítulo 5. Metodología de trabajo, ítem V Acuerdo de nivel de servicio la columna PRIORIDAD 12, se solicita:
"El acceso al repositorio de cuentas de altos privilegios se deberá realizar mediante la autenticación de una contraseña maestra. Es la única contraseña que el usuario necesitará recordar y la herramienta deberá ser capaz de establecer la política para que la misma sea robusta y tenga diversidad de caracteres."
Aclaración: La solución de Segura no permite configuración manual de la contraseña maestra, proporciona un nivel de protección superior al requerido en este ítem, ya que utiliza automáticamente los siguientes mecanismos de protección

- Protección mediante cifrado AES-256 (Cumpliendo FIPS 140-2 Nivel 1
- Uso de diversidad de caracteres (alfanuméricos y caracteres especiales)
- Custodia compartida por múltiples personas, mínimo 2 usuarios administradores de la solución.

Pregunta: ¿Con la aclaración realizada, se aceptará este nivel de protección y gestión automática para la contraseña maestra?

RESPUESTA 18.-
Estimado oferente, por favor refiérase a la Sección 6. BIENES REQUERIDOS, apartado Seguridad de la solución, en lo referente a la seguridad de almacenamiento de credenciales de la solución PAM.

La contraseña maestra puede ser manual o automática, siempre y cuando sea capaz de establecer la política para que la misma sea robusta y tenga diversidad de caracteres.

PREGUNTA 19.-
Requerimiento: En el capítulo 5. Metodología de trabajo, item V Acuerdo de nivel de servicio la columna PRIORIDAD 38, se solicita:
"La herramienta propuesta deberá tener la capacidad de exportar los reportes a los siguientes formatos: XLS, CSV, PDF"

Aclaración: la solución propuesta permite la exportación de reportes en formatos CSV y PDF. Considerando que los archivos CSV pueden abrirse directamente con Microsoft Excel y convertirse de manera sencilla al formato .xlsx,
Pregunta: ¿Con la aclaración realizada, se puede considerar cumplido este requisito?

RESPUESTA 19.-
Estimado oferente, refiérase a la Enmienda Nro. 3 del Boletín de Enmiendas Nro. 1.

PREGUNTA 20.-
¿Se aplicará un protocolo de pruebas de aceptación (UAT) y criterios objetivos de aceptación antes de la suscripción del Acta de Entrega Recepción Parcial de Implementación?

RESPUESTA 20.-
Estimado oferente, para la suscripción del Acta de Entrega Recepción Parcial de la Implementación y Transferencia de conocimientos el contratista debe presentar un informe de implementación, que incluye las pruebas de aceptación (ATP, por sus siglas en inglés) y que deberá ser aprobado por el Administrador de Contrato, conforme lo establecido en la CGC 16.1.

PREGUNTA 21.-
¿Las 1.081 cuentas privilegiadas adicionales de bases de datos deben incorporarse a la bóveda/gestión de la herramienta PAM dentro de las 47 licencias, o se gestionan fuera de la herramienta?

RESPUESTA 21.-
Estimado oferente, refiérase a la Enmienda Nro. 1 del Boletín de Enmiendas Nro. 1. En este sentido, las 1081 cuentas para la gestión de las bases de datos deben incorporarse a la bóveda/gestión de la solución PAM.

PREGUNTA 22.-
¿Se requiere Certificado de Fábrica / Formulario de Autorización del Fabricante para oferentes que no sean fabricantes de la solución PAM?

RESPUESTA 22.-
Estimado oferente, favor remitirse a la Sección II. Datos de la Licitación (DDL), página 42 y Sección V. Formularios de la Oferta, página 76 de la SDO, donde se establece que **no se requiere** el formulario de autorización del fabricante para oferentes que no sean fabricantes de la solución ofertada.

Sin embargo, el certificado de fábrica es requerido conforme se establece en la IAO 12.1 literal d de la Sección II. Datos de la Licitación (DDL), página 41 de la SDO.

PREGUNTA 23.-
¿El licenciamiento debe cubrir 47 usuarios nombrados administradores, o se acepta cualquier modelo del fabricante siempre que cubra los sistemas de la Tabla 2?

RESPUESTA 23.-
Estimado oferente, el modelo de operación y licenciamiento de la solución debe habilitar al SRI para que los administradores detallados en la tabla 1 de la sección 4. Infraestructura Actual tengan acceso a los sistemas institucionales detallados en la tabla 2 de la misma sección, considerando inclusive el escenario de que accedan a todos simultáneamente.

PREGUNTA 24.-
¿Cuál es el periodo mínimo de retención exigido para logs, grabaciones de sesión y reportes de auditoría?

RESPUESTA 24.-
Estimado oferente, la capacidad de retención real de la solución dependerá del tamaño de los archivos de registro y de la capacidad de almacenamiento de la infraestructura virtual disponible para el efecto. Sin embargo, si existieran requerimientos de licenciamiento para tal efecto, se debe considerar un periodo referencial de retención de hasta 9 meses, conforme la Política y necesidad institucional.

PREGUNTA 25.-

¿Cuál es el número estimado de sesiones privilegiadas concurrentes (RDP/SSH/Web) que debe soportar el ambiente de producción?

RESPUESTA 25.-
Estimado oferente, el modelo de operación y licenciamiento de la solución debe habilitar al SRI para que los administradores detallados en la tabla 1 de la sección 4. Infraestructura Actual tengan acceso a los sistemas institucionales detallados en la tabla 2 de la misma sección, considerando inclusive el escenario de que accedan a todos simultáneamente.

PREGUNTA 26.-
¿El SRI cuenta con un proveedor de identidad o solución de MFA corporativa existente con la cual deba integrarse la herramienta?

RESPUESTA 26.-
Estimado oferente, el SRI no cuenta actualmente con un proveedor de identidad o de MFA corporativa con la cual se integre la solución PAM.

El numeral 17 del apartado Seguridad de la solución de la sección 6. BIENES REQUERIDOS indica que la solución PAM "*además de la autenticación por contraseña* ***deberá contar con un doble factor****, al menos uno de los siguientes: Soft token OTP, códigos enviados al dispositivo móvil, entre otros.*" [énfasis añadido]

Adicionalmente, refiérase a la Enmienda Nro. 4 del Boletín de Enmiendas Nro.1 donde se establece que: "*La herramienta deberá ser implementada en los ambientes de producción y contingencia en alta disponibilidad (24x7x365). La herramienta deberá tener al menos dos instancias (nodos) en el ambiente de producción. En el ambiente de contingencia deberá tener al menos una instancia (nodo). La instancia de producción debe replicarse al ambiente de contingencia, con toda la información necesaria para mantener la administración en un caso de falla del ambiente de producción.* ***Si es requerido componentes y/o softwares adicionales, el proveedor deberá incluirlo como parte de la herramienta ofertada.***" [énfasis añadido]

PREGUNTA 27.-
¿Es obligatoria la integración con el SIEM institucional? De ser así, indicar producto, versión y protocolo requerido.

RESPUESTA 27.-
Estimado oferente, la solución PAM propuesta debe cumplir con lo establecido en el numeral 46 del apartado Monitoreo de actividad de usuarios de la sección 6. BIENES REQUERIDOS; es decir, "*deberá tener la capacidad de reportar comportamiento anormal de cuentas de altos privilegios basado en algoritmos de adopción y comportamiento orientado a soluciones SIEM.*"

PREGUNTA 28.-
¿Se requiere integración con algún sistema de gestión de tickets/ITSM del SRI? De ser así, indicar cuál.

RESPUESTA 28.-
Estimado oferente, no se requiere que la solución PAM propuesta se integre con la plataforma de gestión de servicios TI (ITSM) del SRI.

PREGUNTA 29.-
¿Se requiere que el fabricante emita una certificacion del personal tecnico del Partner a nivel Profesional o Experto?

RESPUESTA 29.-
Estimado oferente, el Técnico de Implementación y el Técnico de soporte local deben contar con una certificación vigente del fabricante de la Herramienta de Gestión de Accesos Privilegiados, conforme lo solicitado en la sección 4. Calificación del Oferente (IAO 37).

PREGUNTA 30.-
¿Cuál es el porcentaje máximo acumulado de multas antes de que el Comprador pueda declarar terminado el contrato por incumplimiento?

RESPUESTA 30.-

Estimado oferente, el numeral 9.1 de las Condiciones Generales del Contrato del pliego del proceso textualmente dice: "***Ley Aplicable 9.1 El Contrato se regirá y se interpretará según las leyes del país del Comprador, a menos que se indique otra cosa en las CEC";*** así mismo en las Condiciones Especiales del Contrato se establece que: "***La Ley que rige este contrato es la ley de la República del Ecuador***"; Por lo tanto, el porcentaje es el 5% del valor del contrato.

PREGUNTA 31.-
¿Existen tiempos máximos de solución/resolución por prioridad, adicionales a los tiempos de respuesta ya definidos?

RESPUESTA 31.-
Estimado oferente, no se han definido tiempos máximos de solución/resolución por prioridad, conforme lo definido en la sección V. Acuerdo de nivel de servicio.

PREGUNTA 32.-
¿Cómo se articula la Garantía de los Bienes (CGC 28) con el soporte de fábrica 24x7 de 3

años ya incluido en el alcance, al no traterse de BIENES se entiendo que esto no APLICA?

RESPUESTA 32.-
Estimado Oferente, su entendimiento es correcto, el objeto de contratación del proceso no detalla adquisición de bienes

PREGUNTA 33.-
¿Debe presentarse una matriz de cumplimiento punto por punto de las especificaciones de "BIENES REQUERIDOS"? De ser así, solicitar el formato oficial.

RESPUESTA 33.-
Estimado oferente, refiérase a la IAO 21.1.

PREGUNTA 34.-
¿El plazo de 90 días contempla la integración completa de las 1.081 cuentas privilegiadas adicionales de bases de datos, o se incorporan en una fase posterior no penalizada?

RESPUESTA 34.-
Estimado oferente, el plazo de 90 días contempla la puesta en producción integral de la solución de acuerdo con el alcance establecido en los pliegos.

PREGUNTA 35.-
¿El SRI cuenta actualmente con alguna herramienta de Gestión de Accesos Privilegiados en operación? De ser así, ¿se requiere migración o desmontaje de la solución anterior?

RESPUESTA 35.-
Estimado oferente, el SRI no cuenta actualmente con alguna herramienta de Gestión de Accesos Privilegiados en operación.

PREGUNTA 36.-
¿Confirmar si el licenciamiento de la base de datos backend (de requerirse) debe estar incluido en la oferta del contratista o es resposabilidad del SRI?

RESPUESTA 36.-
Estimado oferente, el contratista deberá proveer todo el licenciamiento necesario para la implementación de la Herramienta de Gestión de Accesos Privilegiados en producción y contingencia, así como cualquier licenciamiento adicional requerido para el funcionamiento de la herramienta, conforme lo establecido en la sección II. Licenciamiento/Suscripción y Mantenimiento/Soporte de Fábrica.

PREGUNTA 37.-
¿El SRI cuenta con una entidad certificadora interna para los certificados TLS de la solución, o el contratista debe proveerlos?

RESPUESTA 37.-
Estimado oferente, el SRI sí cuenta con una entidad certificadora interna, y puede firmar los certificados TLS internos, si la solución PAM así lo requiere.

PREGUNTA 38.-
¿Existe segmentación de red (DMZ, VLANs) entre la plataforma PAM y los sistemas administrados que requiera reglas de firewall adicionales? ¿Quién las gestiona y en qué plazo?

RESPUESTA 38.-
Estimado oferente, el contratista deberá informar oportunamente todos los requerimientos de acceso, incluyendo permisos de firewall, para la implementación de la solución PAM de forma justificada. Estos serán evaluados y aplicados de acuerdo con los estándares de seguridad institucionales.

PREGUNTA 39.-
Confirmar si los materiales de transferencia de conocimiento y manuales pueden entregarse en el idioma original del fabricante (inglés) o deben traducirse.

RESPUESTA 39.-
Estimado oferente, favor referirse a lo establecido en la Sección II. Datos de la Licitación (DDL), página 40, IAO 11.1, y Sección VIII. Condiciones Especiales de Contrato (CEC), página 125, CGC 5.1 de la SDO donde se establece con claridad el idioma de presentación y entrega de la oferta y de todos sus anexos.

PREGUNTA 40.-
¿Existe un plazo máximo para que el Administrador de Contrato emita la notificación de inicio de ejecución tras la suscripción del contrato?

RESPUESTA 40.-
Estimado oferente, el plazo total de ejecución del contrato será de hasta 1.111 días calendario, contados a partir de la fecha que se indique en la notificación escrita enviada por el Administrador de contrato; en tal virtud no existe un plazo máximo para que el Administrador de contrato emita la notificación de inicio contractual.

PREGUNTA 41.-
¿Existe un desglose referencial (aunque sea indicativo) del presupuesto por infraestructura requerida.?

RESPUESTA 41.-
Estimado oferente, no existe un desglose referencial del presupuesto por infraestructura requerida.

PREGUNTA 42.-
¿Se aceptan certificados de experiencia en cualquier solución de ciberseguridad, o deben estar relacionados directamente con gestión de identidades/accesos privilegiados?

RESPUESTA 42.-
Estimado oferente, la experiencia será evaluada conforme a los criterios establecidos en la sección 4. Calificación del Oferente (IAO 37).

PREGUNTA 43.-
El fabricante de la solución de Gestión de Cuentas Privilegiadas PAM tiene presencia Global entre ella entidad fiscal Estados Unidos de Norte América ¿Favor si nos confirma si las cartas de representacion deben venir con la direccion de entidad fiscal de ese pais o en caso de tener una representacion regional por ejemplo Colombia debe venir con esa direccion los documentos?

RESPUESTA 43.-
Estimado oferente, la IAO 12.1 literal d) del proceso establece que el Certificado de Fábrica deberán ser certificados vigentes emitidos por los fabricantes que avalen que el oferente es un distribuidor autorizado de los componentes ofertados, con la dirección del país del emisor del certificado.

PREGUNTA 44.-
Favor nos confirma que la documentación técnica no será presentada en la oferta física original sino referenciada a un archivo o archivos de formato digital (formato pfd, no imágenes) como: fichas técnicas, hojas de especificación, catálogos, manuales o similares, de los productos y servicios ofertados. Esto puede ser compartido mediante una carpeta compartida o debe ser enviada mediante una USB o DVD?

RESPUESTA 44.-
Estimado oferente, favor hacer llegar su oferta y anexos, en formato físico conforme lo establece la SDO y además en formato digital almacenado en USB o DVD, siempre respetando los formatos establecidos.

PREGUNTA 45.-
¿Favor nos confirma que la documentación técnica citada en la pregunta 2 pueden estar en el idioma inglés?

RESPUESTA 45.-
Estimado oferente, favor referirse a lo establecido en la Sección II. Datos de la Licitación (DDL), página 40, IAO 11.1, y Sección VIII. Condiciones Especiales de Contrato (CEC), página 125, CGC 5.1 de la SDO donde se establece con claridad el idioma de presentación y entrega de la oferta y de todos sus anexos.

PREGUNTA 46.-
¿Favor si nos confirma que los documentos justificativos (copias simples) para la presentación de la oferta impresa provenientes del extranjero deben estar impresos en español o puede venir en ingles o debe ser traducidos?

RESPUESTA 46.-
Estimado oferente, favor referirse a lo establecido en la Sección II. Datos de la Licitación (DDL), página 40, IAO 11.1, y Sección VIII. Condiciones Especiales de Contrato (CEC), página 125, CGC 5.1 de la SDO donde se establece con claridad el idioma de presentación y entrega de la oferta y de todos sus anexos.

PREGUNTA 47.-
¿Favor si nos confirma que los documentos justificativos para la suscripción del contrato provenientes de un país elegible extranjero deben estar impresos en español o ingles, y para la firma del contrato deben ser apostillados?

RESPUESTA 47.-
Estimado oferente, la IAO 21.1 del proceso establece que: *"(...) La documentación de la oferta serán copias simples, sin embargo,* ***para la suscripción del contrato se requerirá los documentos que sean otorgados en territorio extranjero, debidamente legalizados ante agente diplomático o cónsul de Ecuador, acreditado en su territorio apostillados*** *(...)".* Adicionalmente si se encuentran en otro idioma, los mismos deberán contener la respectiva traducción.

PREGUNTA 48.-
¿El requerimiento de redundancia *activo-pasivo* debe considerarse como un requisito obligatorio, o también se aceptan arquitecturas *activo-activo* que proporcionen alta disponibilidad y recuperación ante desastres (Disaster Recovery). En caso de aceptarse ambas opciones, ¿existe alguna preferencia por parte de la entidad entre una arquitectura activo-pasivo y una activo-activo?

RESPUESTA 48.-
Estimado oferente, refiérase a la Enmienda Nro. 4, del Boletín de Enmiendas Nro. 1.

PREGUNTA 49.-
Requerimiento: En el capítulo 5. Metodología de trabajo, en el ítem III Implementación, en la sección de Aspectos generales se indica:
"El SRI proveerá la infraestructura de virtualización en sus data centers principal y alterno (basada en VMWARE vsphere 8.0 o superior) para la implementación de la herramienta, el contratista deberá entregar los requerimientos para el despliegue como: capacidad de procesamiento, memoria y almacenamiento."
Aclaración: Como parte de la arquitectura de la solución propuesta se necesitan servidores intermedios para las conexiones hacia las bases de datos y aplicativos ejecutable , estos servidores deben contar con licencias de Windows Server y deben contener licencias de RDS y CALs de usuarios para las conexiones.

Pregunta: ¿El SRI proveerá el software necesario con las licencias requeridas?

RESPUESTA 49.-
Estimado oferente, la solución propuesta deberá instalarse como máquina(s) virtual(es) dentro de la infraestructura de virtualización VMware existente en el SRI. El contratista deberá proveer todo el licenciamiento necesario para la implementación de la Herramienta de Gestión de Accesos Privilegiados en producción y contingencia, así como cualquier licenciamiento adicional requerido para el funcionamiento de la herramienta, conforme lo establecido en la sección II. Licenciamiento/Suscripción y Mantenimiento/Soporte de Fábrica.

PREGUNTA 50.-
Requerimiento: el capítulo 5. Metodología de trabajo, ítem V Acuerdo de nivel de servicio la columna PRIORIDAD número 22, se solicita:
"La herramienta deberá ser capaz de contar con un repositorio seguro, cifrado y a prueba de falsificaciones (tamper-proof) de credenciales de cuentas de altos privilegios, políticas, entitlements, registros de auditorías.
Aclaración: Si bien el requerimiento utiliza el término tamper-proof, la norma **ISO/IEC TS 30104:2015** establece que los sistemas completamente infalibles (tamper-proof) son, en la práctica, teóricos, debido a que no existe la invulnerabilidad absoluta frente a vectores de ataque futuros. La solución propuesta implementa mecanismos avanzados de tamper resistance (resistencia a la manipulación).
Adicionalmente, la plataforma garantiza una capa de seguridad completa, inalterable y de alta confianza sobre el repositorio mediante los siguientes controles: • **Cifrado de Estándar Internacional:** El núcleo criptográfico de la solución se rige bajo estándares globales de alta exigencia como **FIPS 140-2**, validando la seguridad de sus módulos de

datos.
• **Protección de Llave Maestra:** Toda la información confidencial, configuraciones y secretos de la bóveda electrónica se protegen mediante una llave maestra cifrada bajo el algoritmo militar **AES de 256 bits**.
• **Esquema de Custodia Múltiple:** Para evitar cualquier alteración unilateral, el acceso raíz y la recuperación de respaldos están distribuidos de forma obligatoria entre **múltiples usuarios custodios de confianza**, impidiendo fraudes o falsificaciones por parte de un único actor.
• **Control de Acceso Avanzado (RBAC):** El sistema restringe de manera estricta los permisos de visualización y modificación a nivel de roles, asegurando que solo el personal explícitamente autorizado interactúe con el repositorio.
Pregunta: ¿Con la aclaración realizada, se puede considerar cumplido este requisito?

RESPUESTA 50.-
Estimado oferente, la solución PAM propuesta debe contar con mecanismos de protección que permitan reducir la probabilidad de que, si un atacante intenta explotar o utilizar métodos de trampa ("tamper"), este no logre obtener accesos privilegiados ni información confidencial; es decir que deberá cumplir con lo que se establece en la sección 6, Bienes Requeridos, apartado Seguridad de la Solución, numeral 22.

PREGUNTA 51.-
¿Es posible ampliar en 15 días el plazo para la entrega de la propuesta, es decir, hasta el martes 18 de agosto de 2026?

RESPUESTA 51.-
Estimado oferente, las Políticas para la Adquisición de Bienes y Obras Financiadas por el Banco Interamericano de Desarrollo GN-2349-15 en su numeral 2.51 **Plazo para la Preparación de las Ofertas** determina lo siguiente: "*(...) El plazo que se conceda para la preparación y presentación de las ofertas debe determinarse teniendo debidamente en cuenta las circunstancias especiales del proyecto y la magnitud y complejidad del contrato. En general, para las licitaciones internacionales dicho plazo no debe ser inferior a seis semanas a partir de la fecha del llamado a licitación (...)*", por otra parte, la IAO 8.1 del pliego de Licitación Pública Nacional establece: "*(...) Todo Oferente potencial que requiera alguna aclaración sobre el documento de licitación deberá comunicarse con el Comprador por escrito a la dirección del Comprador que se suministra* ***en los DDL****. El Comprador responderá por escrito a todas las solicitudes de aclaración, siempre que dichas solicitudes sean recibidas al menos veintiún (21) días antes de la fecha límite para la presentación de ofertas. (...)*". En consecuencia, toda vez que la Política del BID no establece un tiempo mínimo para presentación de ofertas en procedimiento de LPN, se resolvió dejar el tiempo mínimo requerido para una LPI esto es 42 días desde el llamado de Licitación; en tal virtud no procede la ampliación

para la entrega de ofertas y la misma se mantiene hasta las 10:00 am del 04 de agosto de 2026.

PREGUNTA 52.-
¿Desde qué momento empiezan a correr los 1.096 días de la suscripción: desde la entrega de la solución o desde su salida a producción?

RESPUESTA 52.-
Estimado oferente, conforme la CGC 16.1, sección PLAZO DE EJECUCIÓN:

- *"La activación del licenciamiento y soporte de fábrica será entregada hasta 15 días calendario contados a partir de la fecha que se indique en la notificación escrita enviada por el Administrador de contrato.*
- *"El licenciamiento y el soporte de fábrica de la solución de Accesos Privilegiados tendrá una vigencia de hasta 1.096 días calendario (3 años) contados a partir de la fecha de su activación".*

PREGUNTA 53.-
Dado que el SRI proveerá los requerimientos de hardware mediante máquinas virtuales, ¿el plazo del proyecto incluye el tiempo de gestión interna del SRI para entregar dichos recursos? Preguntamos esto para evitar posibles retrasos y garantizar los tiempos propuestos.

RESPUESTA 53.-
Estimado oferente, el plazo del proyecto incluye el tiempo de gestión interna del SRI para entregar los recursos virtuales.

PREGUNTA 54.-
¿Cuál es el método de evaluación de la oferta técnica y económica? ¿Se adjudica únicamente por el precio más bajo, o el SRI puede seleccionar una oferta que, sin ser la más económica, ofrezca mejores funcionalidades más allá de lo solicitado en el pliego?

RESPUESTA 54.-
Estimado oferente, conforme la Sección III. Criterios de Evaluación y Calificación página 48 de la SDO, se establece que:
El Comprador utilizará los criterios y las metodologías enumerados en las secciones 3 y 4 a continuación para determinar la Oferta Más Ventajosa. La Oferta Más Ventajosa es aquella que cumple con los criterios de calificación y que:
(a) se ajusta sustancialmente al documento de licitación, y
(b) tiene el costo evaluado más bajo.

PREGUNTA 55.-
Para la sección de experiencia, ¿se debe presentar la experiencia de la empresa oferente o únicamente la de los técnicos que participarán en el proyecto?

RESPUESTA 55.-
Estimado oferente, favor remitirse a la Sección III. Criterios de Evaluación y Calificación páginas 52 a la 54 de la SDO, donde se establecen los requisitos mínimos de experiencia tanto para el Oferente como para el personal técnico propuesto.

PREGUNTA 56.-
Los roles de implementación y de soporte técnico local normalmente son cubiertos por las mismas personas. ¿Puede un mismo ingeniero cumplir ambos roles dentro de este proyecto?

RESPUESTA 56.-
Estimado oferente, conforme lo establecido en el numeral 4. Calificación del Oferente (IAO 37), de la Sección III. Criterios de Evaluación y Calificación: "*Un técnico podrá prestar el servicio de Soporte local y el servicio de implementación de la solución al mismo tiempo siempre que cumplan con el perfil requerido.*"

PREGUNTA 57.-
En caso de que ciertos componentes requieran un sistema operativo, ¿el SRI proporcionará las licencias de los sistemas operativos necesarios para implementar la solución?

RESPUESTA 57.-
Estimado oferente, la solución propuesta deberá instalarse como máquina(s) virtual(es) dentro de la infraestructura de virtualización VMware existente en el SRI. El contratista deberá proveer todo el licenciamiento necesario para la implementación de la Herramienta de Gestión de Accesos Privilegiados en producción y contingencia, así como cualquier licenciamiento adicional requerido para el funcionamiento de la herramienta, conforme lo establecido en la sección II. Licenciamiento/Suscripción y Mantenimiento/Soporte de Fábrica.

PREGUNTA 58.-
¿La solución de gestión de cuentas privilegiadas debe integrarse con el Gestor de Identidades del SRI?

RESPUESTA 58.-
Estimado oferente, conforme lo establecido en el numeral 4 del apartado Plataformas, dispositivos, herramientas y sistemas operativos soportados de la sección 6. BIENES REQUERIDOS: La solución PAM debe tener la «*Capacidad para integrarse con las*

herramientas que utilizan los usuarios Administradores del SRI que constan en la sección "INFORMACIÓN QUE DISPONE LA ENTIDAD"».

En la columna "*Nombre de herramienta y versión (Sistema Administrado)*" de la Tabla 2. Dimensionamiento de administradores de la herramienta de Gestión de Accesos Privilegiados en la sección 4. Infraestructura Actual se detallan las herramientas que utilizan los usuarios Administradores del SRI.

Adicionalmente, refiérase a la Enmienda Nro. 2. del Boletín de Enmiendas Nro. 1.

PREGUNTA 59.-
¿El SRI mantendrá cuentas privilegiadas que no se almacenen en la bóveda del PAM?

RESPUESTA 59.-
Estimado oferente, por favor, remítase a la Tabla 2. Dimensionamiento de administradores de la herramienta de Gestión de Accesos Privilegiados en la sección 4. Infraestructura Actual donde constan los usuarios y cuentas de altos privilegios a integrarse en la solución PAM.

PREGUNTA 60.-
¿En qué momento debe impartirse la transferencia de conocimiento: antes o después de la implementación?

RESPUESTA 60.-
Estimado oferente, conforme lo indicado en el apartado III. Implementación de la sección 5. METODOLOGÍA DE TRABAJO, "*El calendario y horario de entrega de la transferencia de conocimiento se acordará con el administrador del contrato en función de la disponibilidad operativa del personal del SRI.*"

PREGUNTA 61.-
¿La transferencia de conocimiento puede realizarse sobre uno de los ambientes no productivos del SRI, o se requiere construir un ambiente nuevo exclusivo para esta actividad? Consultamos esto porque las integraciones estarán realizadas sobre los ambientes ya instalados en el SRI.

RESPUESTA 61.-
Estimado oferente, "*Toda **logística** asociada con la transferencia de conocimiento correrá por cuenta del Contratista*" [énfasis añadido], de acuerdo con lo establecido en el apartado III. Implementación de la sección 5. METODOLOGÍA DE TRABAJO, y "*La transferencia de conocimientos deberá incluir los materiales, laboratorios con tecnología similar a la herramienta instalada, **equipos, acceso a internet, facilidades y talleres** necesarios para*

la correcta asimilación del contenido y la generación de destrezas necesarias en los asistentes. Esta actividad no representará costos adicionales para el SRI." [énfasis añadido], de acuerdo con lo establecido en el apartado VI. Implementación de la sección 7. SERVICIOS CONEXOS REQUERIDOS.

En consecuencia, la transferencia de conocimientos debe realizarse en un entorno provisto por el contratista que garantice el cumplimiento integral de lo definido en los pliegos.

PREGUNTA 62.-
La Tabla 2 lista varias herramientas con sus versiones que deben estar soportadas por la solución. ¿El proveedor debe integrar todas las plataformas de la lista o un subconjunto de ellas?

RESPUESTA 62.-
Estimado oferente, conforme lo establecido en el numeral 4 del apartado Plataformas, dispositivos, herramientas y sistemas operativos soportados de la sección 6. BIENES REQUERIDOS: La solución PAM debe tener la «*Capacidad para integrarse con las herramientas que utilizan los usuarios Administradores del SRI que constan en la sección "INFORMACIÓN QUE DISPONE LA ENTIDAD"*».

En la columna "*Nombre de herramienta y versión (Sistema Administrado)*" de la Tabla 2. Dimensionamiento de administradores de la herramienta de Gestión de Accesos Privilegiados en la sección 4. Infraestructura Actual se detallan las herramientas que utilizan los usuarios Administradores del SRI.

Adicionalmente, refiérase a la Enmienda Nro. 2. del Boletín de Enmiendas Nro. 1.

PREGUNTA 63.-
¿Las plataformas listadas en la Tabla 2 cuentan con soporte vigente del fabricante? ¿El SRI dispone de especialistas que apoyen en la ejecución del proyecto PAM y, de ser necesario, en las integraciones?

RESPUESTA 63.-
Estimado oferente, el SRI mantiene contratos de soporte de fábrica de las versiones vigentes de las herramientas detallas en la columna "*Nombre de herramienta y versión (Sistema Administrado)*" de la Tabla 2. Dimensionamiento de administradores de la herramienta de Gestión de Accesos Privilegiados en la sección 4. Infraestructura Actual.

PREGUNTA 64.-
La Tabla 2 incluye Oracle 11g (fuera de soporte del fabricante desde 2020). ¿El SRI requiere gestión de credenciales a nivel del motor de base de datos para esas instancias, o

es suficiente la gestión a nivel de sistema operativo (SSH)?

RESPUESTA 64.-
Estimado oferente, en la columna "*Tipo de conexión al sistema administrado*" de la Tabla 2. Dimensionamiento de administradores de la herramienta de Gestión de Accesos Privilegiados en la sección 4. Infraestructura Actual se indica la conexión solicitada.

PREGUNTA 65.-
En la Tabla 2 se indica, para la aplicación Developer versión 23.1.0 y superiores: "Se debe considerar que, además de acceder con su cuenta privilegiada de administración, los administradores utilizan otro usuario privilegiado para la gestión de las bases de datos." ¿Cuántas personas administradoras estarán registradas en el PAM? ¿Ese "otro usuario privilegiado" se registrará en el PAM como una persona adicional, distinta de las 47 personas? De esta respuesta depende la cantidad de licencias requeridas.

RESPUESTA 65.-
Estimado oferente, refiérase a la Enmienda Nro. 1 del Boletín de Enmiendas Nro. 1.

PREGUNTA 66.-
En la Tabla 2 se indica, para la aplicación Toad for Oracle 17.1 y superiores: "Finalmente, tener en cuenta que los administradores, además de utilizar su cuenta privilegiada de administración, emplean 1.081 usuarios privilegiados adicionales para la gestión de las bases de datos." ¿Esos 1.081 usuarios requieren cuenta individual en la herramienta PAM (lo que excedería las 47 licencias), o son únicamente cuentas de base de datos a resguardar en el PAM, operadas por los 47 administradores licenciados?

RESPUESTA 66.-
Estimado oferente, los "*1.081 usuarios privilegiados adicionales*" son únicamente cuentas de base de datos a resguardar en el PAM, operadas por los 47 administradores licenciados.

Adicionalmente, refiérase a la Enmienda Nro. 1 del Boletín de Enmiendas Nro. 1.

PREGUNTA 67.-
¿Las cuentas privilegiadas que gestionará la solución PAM operan bajo un modelo de cuentas genéricas/compartidas por plataforma (p. ej., root, Administrator), o corresponden a cuentas administrativas nominales asignadas individualmente a cada operador?

RESPUESTA 67.-
Estimado oferente, las cuentas de altos privilegios que gestionará la solución PAM corresponden a cuentas genéricas/compartidas por plataforma (p. ej., root, Administrator).

PREGUNTA 68.-

Las plataformas Consola Web IBM Storage Insights, Consola Web OME, vSphere Client, Enterprise Manager Cloud Control, IBM Security Identity Manager y Symantec Encryption Management Server, ¿cuentan con autenticación mediante AD o LDAP?

RESPUESTA 68.-
Estimado oferente, el mecanismo de autenticación de las herramientas detalladas en la columna "*Nombre de herramienta y versión (Sistema Administrado)*" de la Tabla 2. Dimensionamiento de administradores de la herramienta de Gestión de Accesos Privilegiados en la sección 4. Infraestructura Actual es mixto.

PREGUNTA 69.-
Para esas mismas plataformas (IBM Storage Insights, OME, vSphere Client, Enterprise Manager Cloud Control, IBM Security Identity Manager y Symantec Encryption Management Server), ¿el cambio de contraseña se realiza mediante SSH o únicamente a través de la consola web?

RESPUESTA 69.-
Estimado oferente, el mecanismo de cambio de contraseña de las herramientas detalladas en la columna "*Nombre de herramienta y versión (Sistema Administrado)*" de la Tabla 2. Dimensionamiento de administradores de la herramienta de Gestión de Accesos Privilegiados en la sección 4. Infraestructura Actual es mixto.

PREGUNTA 70.-
¿Contaríamos con un especialista del SRI que nos asista en la instalación de los clientes y configuración de los archivos TNS de las bases de datos y sus respectivos clientes de conexión?

RESPUESTA 70.-
Estimado oferente, el personal de contratista trabajará en conjunto con el personal del SRI, de acuerdo con sus competencias, en la implementación de la solución, siendo responsabilidad del contratista, la correcta y oportuna ejecución de cada actividad.

PREGUNTA 71.-
Para las conexiones SSH, ¿qué cliente SSH utilizan en su operación diaria? ¿Ese cliente está instalado en las máquinas de los colaboradores del SRI o es portable?

RESPUESTA 71.-
Estimado oferente, en la columna "*Tipo de conexión al sistema administrado*" de la Tabla 2. Dimensionamiento de administradores de la herramienta de Gestión de Accesos Privilegiados en la sección 4. Infraestructura Actual se detallan las formas de conexión a los sistemas.

PREGUNTA 72.-
Las bases no definen la técnica ni las herramientas que utilizarán los administradores para gestionar las plataformas (por ejemplo, Escritorio Remoto para Windows, PuTTY para Linux, etc.). ¿El SRI puede precisar la forma en que se gestionarán las sesiones?

RESPUESTA 72.-
Estimado oferente, en la columna "*Tipo de conexión al sistema administrado*" de la Tabla 2. Dimensionamiento de administradores de la herramienta de Gestión de Accesos Privilegiados en la sección 4. Infraestructura Actual se detallan las formas de conexión para la gestión de las sesiones.

PREGUNTA 73.-
Entendemos que las aplicaciones de la Tabla 2 son las que utilizan los administradores para gestionar las plataformas. ¿Existe preferencia por acceder a estas herramientas mediante un Terminal Server, o se prefiere que los administradores las ejecuten localmente en sus propias máquinas para mejorar la experiencia de usuario? ¿Se desea también que esta gestión pueda realizarse desde una consola web? Consultamos esto porque la experiencia de usuario no está definida y el trabajo mediante Terminal Server no resulta cómodo. En consecuencia, ¿el SRI evaluará de manera distinta una oferta que permita únicamente conexiones por Terminal Server frente a una que permita conexiones con las herramientas instaladas en la máquina del administrador o mediante navegador?

RESPUESTA 73.-
Estimado oferente, la evaluación de las ofertas se realizará conforme a lo establecido en la Sección VI. Requisitos de los Bienes y Servicios Conexos.

PREGUNTA 74.-
Sección 6, Bienes requeridos, punto 3: se solicita que las credenciales se almacenen en un repositorio cifrado y protegido. ¿Existe algún requerimiento técnico específico o estándar de cifrado obligatorio (p. ej., AES-256, ¿FIPS 140-2) que deba cumplir la solución?

RESPUESTA 74.-
Estimado oferente, cúmplase con lo requerido en el numeral 3, del apartado Plataformas, dispositivos, herramientas y sistemas operativos soportados de la sección 6. BIENES REQUERIDOS: "*Capacidad para almacenar cuentas de altos privilegios a modo de repositorio, en la que las credenciales de las cuentas de altos privilegios se encuentren cifradas y protegidas contra accesos no autorizados.*"

PREGUNTA 75.-
Sección 6, Bienes requeridos, punto 9: ¿Es posible la creación de nuevos grupos de AD o LDAP para mantener y optimizar la granularidad de los permisos de acceso a las cuentas privilegiadas, según los requerimientos del SRI?

RESPUESTA 75.-
Estimado oferente, sí es factible que, para la correcta operación de la solución PAM, se generen nuevos grupos de AD o LDAP para mantener y optimizar la granularidad de los permisos de acceso a las cuentas de altos privilegios, según los requerimientos del SRI.

PREGUNTA 76.-
Sección de arquitectura, numeral 16: se indica que "en el ambiente de producción, además de alta disponibilidad, la herramienta deberá contar con redundancia." Entendemos que se trata de un despliegue Activo–Pasivo, y que esa es la alta disponibilidad y redundancia que requiere el SRI. Por favor confirmarlo.

RESPUESTA 76.-
Estimado oferente, refiérase a la Enmienda Nro. 4, del Boletín de Enmiendas Nro. 1.

PREGUNTA 77.-
Sección 7, Servicios Conexos requeridos, punto 4: ¿La solución PAM debe desplegarse en un esquema de Alta Disponibilidad (HA) Activo/Pasivo, con el nodo Pasivo en un sitio alterno? De ser así, ¿qué latencia existe entre ambos sitios?

RESPUESTA 77.-
Estimado oferente, refiérase a la Enmienda Nro. 4, del Boletín de Enmiendas Nro. 1.

PREGUNTA 78.-
¿El SRI proveerá los recursos de cómputo (vCPU, RAM) necesarios según las recomendaciones del fabricante?

RESPUESTA 78.-
Estimado oferente, la solución propuesta deberá instalarse como máquina(s) virtual(es) dentro de la infraestructura de virtualización VMware existente en el SRI. El contratista deberá proveer todo el licenciamiento necesario para la implementación de la Herramienta de Gestión de Accesos Privilegiados en producción y contingencia, así como cualquier licenciamiento adicional requerido para el funcionamiento de la herramienta, conforme lo establecido en la sección II. Licenciamiento/Suscripción y Mantenimiento/Soporte de Fábrica.

PREGUNTA 79.-

¿El SRI cuenta con una Autoridad Certificadora (CA) interna para firmar los certificados SSL/TLS requeridos por los appliances del PAM, o se espera el uso de certificados autofirmados?

RESPUESTA 79.-
Estimado oferente, el SRI sí cuenta con una entidad certificadora interna, y puede firmar los certificados TLS internos si la solución PAM así lo requiere.

PREGUNTA 80.-
Sección "Gestión de contraseñas y credenciales", numeral 29: se solicita que "la herramienta deberá tener la capacidad de fortalecer la política de contraseña cuando las cuentas se cambian manualmente, así como cuando los sistemas cambian la contraseña aleatoriamente." ¿Pueden ampliar cómo se cambian las cuentas manualmente y qué sistemas, distintos del PAM, realizarán cambios de contraseña en las aplicaciones? Consultamos esto porque, para esta funcionalidad, utilizamos una cuenta funcional y una cuenta gestionada: la gestionada sí soporta el cambio de contraseña por otros sistemas, pero no debemos perder la contraseña de la cuenta funcional, ya que sin ella no es posible gestionar ninguna cuenta del sistema.

RESPUESTA 80.-
Estimado oferente, el requerimiento citado consiste en que, cuando la solución PAM asuma el rol de centralizar la gestión de contraseñas aplique los criterios de fortaleza de claves, ya sea en claves que se ingresen manualmente o en claves generadas automáticamente por la misma solución.

PREGUNTA 81.-
Complementando lo anterior: para todas las aplicaciones de la Tabla 2, ¿podemos crear estas dos cuentas (funcional y gestionada) en todas las plataformas? Nos interesa especialmente poder crear la cuenta funcional.

RESPUESTA 81.-
Estimado oferente, el requerimiento citado consiste en que, cuando la solución PAM asuma el rol de centralizar la gestión de contraseñas aplique los criterios de fortaleza de claves, ya sea en claves que se ingresen manualmente o en claves generadas automáticamente por la misma solución.

PREGUNTA 82.-
Para las aplicaciones web entendemos que no es posible mantener una cuenta funcional, sino únicamente cuentas gestionadas, por lo que en esos casos no se podría rotar la contraseña. ¿Es esto aceptable?

RESPUESTA 82.-
Estimado oferente, el requerimiento citado consiste en que, cuando la solución PAM asuma el rol de centralizar la gestión de contraseñas aplique los criterios de fortaleza de claves, ya sea en claves que se ingresen manualmente o en claves generadas automáticamente por la misma solución.

PREGUNTA 83.-
Sección 6, Bienes requeridos, punto 17 (MFA): ¿El SRI ya cuenta con un proveedor de MFA a integrar (RADIUS, Azure MFA, etc.) o es aceptable el MFA nativo de la herramienta ofertada?

RESPUESTA 83.-
Estimado oferente, el SRI no cuenta actualmente con un proveedor de identidad o de MFA corporativa con la cual se integre la solución PAM.

El numeral 17 del apartado Seguridad de la solución de la sección 6. BIENES REQUERIDOS indica que la solución PAM "*además de la autenticación por contraseña* ***deberá contar con un doble factor****, al menos uno de los siguientes: Soft token OTP, códigos enviados al dispositivo móvil, entre otros.*" [énfasis añadido]

Adicionalmente, refiérase a la Enmienda Nro. 4 del Boletín de Enmiendas Nro.1 donde se establece que: "*La herramienta deberá ser implementada en los ambientes de producción y contingencia en alta disponibilidad (24x7x365). La herramienta deberá tener al menos dos instancias (nodos) en el ambiente de producción. En el ambiente de contingencia deberá tener al menos una instancia (nodo). La instancia de producción debe replicarse al ambiente de contingencia, con toda la información necesaria para mantener la administración en un caso de falla del ambiente de producción.* ***Si es requerido componentes y/o softwares adicionales, el proveedor deberá incluirlo como parte de la herramienta ofertada.***" [énfasis añadido]

PREGUNTA 84.-
Sección 6, Bienes requeridos, punto 17 (MFA mediante Soft Token): ¿La organización tiene estandarizado el uso de alguna aplicación de autenticación (Microsoft Authenticator, Google Authenticator u otra), o la herramienta ofertada debe incluir su propia aplicación móvil de gestión de tokens?

RESPUESTA 84.-
Estimado oferente, el SRI no cuenta actualmente con un proveedor de identidad o de MFA corporativa con la cual se integre la solución PAM.

El numeral 17 del apartado Seguridad de la solución de la sección 6. BIENES REQUERIDOS indica que la solución PAM "*además de la autenticación por contraseña*

***deberá contar con un doble factor**, al menos uno de los siguientes: Soft token OTP, códigos enviados al dispositivo móvil, entre otros.*" [énfasis añadido]

Adicionalmente, refiérase a la Enmienda Nro. 4 del Boletín de Enmiendas Nro.1 donde se establece que: "*La herramienta deberá ser implementada en los ambientes de producción y contingencia en alta disponibilidad (24x7x365). La herramienta deberá tener al menos dos instancias (nodos) en el ambiente de producción. En el ambiente de contingencia deberá tener al menos una instancia (nodo). La instancia de producción debe replicarse al ambiente de contingencia, con toda la información necesaria para mantener la administración en un caso de falla del ambiente de producción.* ***Si es requerido componentes y/o softwares adicionales, el proveedor deberá incluirlo como parte de la herramienta ofertada.***" [énfasis añadido]

PREGUNTA 85.-
Sección 6, Bienes requeridos, punto 23: entendemos que las plataformas y sistemas del SRI deben gestionarse sin agentes en los servidores. Sin embargo, ¿los operadores del SRI pueden contar con software instalado localmente para la apertura de los accesos privilegiados?

RESPUESTA 85.-
Estimado oferente, el software instalado localmente que utilizan los administradores (usuarios privilegiados) se detalla en la *Tabla 2. Dimensionamiento de administradores de herramienta de Gestión de Accesos Privilegiados*

PREGUNTA 86.-
Sección 6, Bienes requeridos, punto 23: las cuentas encargadas de la rotación y gestión de contraseñas del PAM (cuentas funcionales) en Windows, ya sean locales o de dominio, ¿podrían tener deshabilitada la directiva de seguridad UAC, o existe alguna política interna de seguridad que lo impida?

RESPUESTA 86.-
Estimado oferente, no existe una política interna que impida desactivar la directiva de seguridad UAC en servidores Windows.

PREGUNTA 87.-
Sección 6, Bienes requeridos, punto 45: ¿Qué tipos de amenazas o actividades sospechosas esperan que el PAM detecte y alerte?

RESPUESTA 87.-
Estimado oferente, el numeral 45 no restringe el alcance a tipos específicos de amenazas; exige que la herramienta cuente con capacidad de análisis inteligente para detectar y alertar

sobre cualquier amenaza o actividad sospechosa asociada al uso de cuentas de altos privilegios, incluyendo, sin limitarse a, los escenarios de comportamiento anómalo (numeral 46) y uso excesivo o fuera de horario laboral (numeral 47). Se espera que el oferente describa el alcance y las capacidades de detección de su solución conforme a las mejores prácticas de la industria para herramientas PAM.

PREGUNTA 88.-
Sección 6, Bienes requeridos, punto 47: respecto a la capacidad de generar notificaciones por uso excesivo del PAM, ¿es aceptable reportar el uso al SIEM y que sus correlaciones detecten y notifiquen el acceso excesivo, cumpliendo así el objetivo?

RESPUESTA 88.-
Estimado oferente, el numeral 47 exige que la herramienta de Gestión de Accesos Privilegiados propuesta cuente, de forma nativa, con la capacidad de generar notificaciones de uso excesivo y de uso fuera de horario laboral de las cuentas de altos privilegios. El requisito recae sobre la herramienta PAM y no se satisface mediante el envío de logs a un SIEM externo para que sea este quien efectúe la correlación y notificación. Una integración con SIEM puede complementar el monitoreo, pero no sustituye la capacidad exigida en el numeral 47, la cual debe residir en la solución PAM ofertada.

PREGUNTA 89.-
Sección 6, Bienes requeridos, punto 47: en lugar de únicamente notificar el uso fuera del horario laboral, ¿podemos limitar dicho uso o condicionarlo a una aprobación previa, como medida preventiva para cumplir este requisito?

RESPUESTA 89.-
Estimado oferente, se aclara que la solución PAM debe permitir a los gestores de Seguridad aplicar políticas de seguridad sobre el uso excesivo y uso fuera de horario laboral de las cuentas de altos privilegios. La notificación es solicitada para que los gestores de Seguridad tengan conocimiento oportuno de estas novedades.

PREGUNTA 90.-
¿El PAM se integraría a un SIEM del SRI? De ser así, ¿cuál es?

RESPUESTA 90.-
Estimado oferente, la solución PAM propuesta debe cumplir con lo establecido en el numeral 46 del apartado Monitoreo de actividad de usuarios de la sección 6. BIENES REQUERIDOS; es decir, "*deberá tener la capacidad de reportar comportamiento anormal de cuentas de altos privilegios basado en algoritmos de adopción y comportamiento orientado a soluciones SIEM.*"

PREGUNTA 91.-
¿Cuentan con almacenamiento NFS o un recurso compartido de Windows (Windows File Sharing) de 1 TB disponible para enviar los respaldos de configuración y archivar las grabaciones de sesiones antiguas del PAM?

RESPUESTA 91.-
Estimado oferente, la provisión del almacenamiento designado para alojar los componentes de la solución PAM se hará en función de la necesidad y disponibilidad institucional y de la retención (en tiempo o capacidad de disco) definida por el Administrador de Contrato, según la arquitectura y las mejores prácticas del fabricante, y conforme lo indicado en el apartado III. Implementación, sección 5. METODOLOGÍA DE TRABAJO.

PREGUNTA 92.-
¿Cuál es el tiempo de retención mínimo aceptable para las grabaciones del PAM (por ejemplo, 1 año, 5 años)?

RESPUESTA 92.-
Estimado oferente, la provisión del almacenamiento designado para alojar los componentes de la solución PAM se hará en función de la necesidad y disponibilidad institucional; y de la retención (en tiempo o capacidad de disco) definida por el Administrador de Contrato, según la arquitectura y las mejores prácticas del fabricante, y conforme lo indicado en el apartado III. Implementación, sección 5. METODOLOGÍA DE TRABAJO.

PREGUNTA 93.-
¿Cuál es la duración promedio de una sesión privilegiada de un operador en el PAM?

RESPUESTA 93.-
Estimado oferente, cada administrador, dependiendo de sus funciones y de la tarea asignada, mantiene diferentes periodos de conexión hacia los sistemas que tiene a su cargo. No es factible establecer una duración promedio referencial.

PREGUNTA 94.-
¿El SRI tiene definido algún lineamiento o política para escenarios de acceso de emergencia ("Break-Glass") en caso de indisponibilidad de los sistemas de autenticación primaria (p. ej., Active Directory, ¿MFA)?

RESPUESTA 94.-
Estimado oferente, el mecanismo de acceso de emergencia ("Break-Glass") se definirá y operativizará como parte de la implementación de la solución PAM, en función de la arquitectura y mejores prácticas del fabricante y de la infraestructura del SRI.

PREGUNTA 95.-
¿Los usuarios registrados en el Active Directory del SRI son los mismos que están en el LDAP?

RESPUESTA 95.-
Estimado oferente, de acuerdo con los numerales 8 y 9 del apartado Administración de la sección 6. BIENES REQUERIDOS:

"*8. La herramienta deberá tener la capacidad para realizar el aprovisionamiento automática de cuentas a partir de un Active Directory o LDAP, esto implica que la herramienta deberá ser capaz de integrarse con estos directorios de manera automática y transparente, de modo que pueda crear, modificar o eliminar cuentas de manera automática reflejando los cambios que ocurran en los directorios mencionados.*

"*9. La herramienta deberá tener la capacidad de manejar los controles de acceso basado en roles mediante la administración de grupos de usuarios de Active Directory o LDAP.*"

PREGUNTA 96.-

Requerimiento: En la sección VI. Requisitos de los Bienes y Servicios Conexos, 3. Especificaciones Técnicas en el capítulo 4. Infraestructura Actual, de acuerdo con lo indicado en la Tabla 2. "Dimensionamiento de administradores de la herramienta de Gestión de Accesos Privilegiados", en el ítem Gestión Interna de Centro de Cómputo, en la columna de Cantidad se indica:

"12 licencias Toad for Oracle 17.1

Se debe **considerar la cantidad registrada para el motor de base de datos**

Finalmente, tener en cuenta que los **Administradores**, además de utilizar su cuenta privilegiada de administración, emplean **1081 usuarios privilegiados adicionales** para la gestión de las bases de datos"

Pregunta: ¿Con el fin de dimensionar correctamente la implementación, solicitamos confirmar si la referencia a "1081 usuarios privilegiados adicionales" corresponde a 1081 credenciales de bases de datos que serán gestionadas por el PAM como objetos de la bóveda de credenciales, o si se trata de 1081 usuarios administradores distintos que accederán a la solución PAM?

RESPUESTA 96.-

Estimado oferente, refiérase a la Enmienda Nro. 1 del Boletín de Enmiendas Nro. 1.

PREGUNTA 97.-

Requerimiento: En la sección **VI. Requisitos de los Bienes y Servicios Conexos, 3. Especificaciones Técnicas en el capítulo 4. Infraestructura Actual,** de acuerdo con lo indicado en la **Tabla 2. "Dimensionamiento de administradores de la herramienta de Gestión de Accesos Privilegiados",** en el ítem **Gestion Interna de Seguridad Gestión Interna de Centro de Cómputo,** en la columna **de Cantidad** se indica**:**

"3 bases de datos Se debe considerar que, además de acceder con su cuenta privilegiada de administración, los administradores utilizan otro **usuario privilegiado** para la gestión de las bases de datos.

12 licencias Toad for Oracle 17.1

Se debe considerar la cantidad registrada para el motor de base de datos

Finalmente, tener en cuenta que los Administradores, además de utilizar su **cuenta privilegiada** de administración, emplean 1081 **usuarios privilegiados** adicionales para la gestión de las bases de datos"

Pregunta: Solicitamos aclarar el alcance de los términos **"cuentas privilegiadas"** y **"usuarios privilegiados"** utilizados en el presente proceso.

RESPUESTA 97.-

Estimado oferente, los "*1.081 usuarios privilegiados adicionales*" son únicamente cuentas de base de datos a resguardar en el PAM, operadas por los 47 administradores licenciados.

Adicionalmente, refiérase a la Enmienda Nro. 1 del Boletín de Enmiendas Nro. 1.

PREGUNTA 98.-

Requerimiento: En la sección **VI. Requisitos de los Bienes y Servicios Conexos, 3. Especificaciones Técnicas en el capítulo 4. Infraestructura Actual,** de acuerdo con lo indicado en la **Tabla 2. "Dimensionamiento de administradores de la herramienta de Gestión de Accesos Privilegiados",** en el ítem **Gestion Interna de Seguridad Gestión Interna de Centro de Cómputo,** en la columna de **Cantidad** se indica**:**

“3 bases de datos Se debe considerar que, además de acceder con su cuenta privilegiada de administración, los administradores utilizan otro **usuario privilegiado** para la gestión de las bases de datos.”

Pregunta: Solicitamos confirmar si el ¿otro usuario privilegiado para la gestión de las bases de datos" corresponde a una credencial de la base de datos (por ejemplo, usuarios Oracle como SYSTEM, SYS u otras cuentas DBA) que será administrada por la bóveda de PAM, o si se refiere a un segundo usuario privilegiado para acceder a la plataforma y que debe ser tomado en cuenta en la licencia?

RESPUESTA 98.-

Estimado oferente, refiérase a la Enmienda Nro. 1 del Boletín de Enmiendas Nro. 1.