BOLETÍN DE ENMIENDAS Nro. 2

"ADQUISICIÓN DE FIREWALL NUEVA GENERACIÓN"

CÓDIGO: EC-L1253- P00016

El presente boletín de enmiendas se lo emite según lo estipulado en las Políticas para la Adquisición de Bienes y Obras financiadas por el Banco Interamericano de Desarrollo GN-2349-15, en la sección B. Documentos de Licitación - Claridad de los Documentos de Licitación, en el numeral 2.25 *"(…) Toda información, aclaración, corrección de errores o modificación adicional de los documentos de licitación se debe enviar, a cada uno de los posibles oferentes que adquirieron los documentos de licitación originales, con tiempo suficiente respecto a la fecha fijada como límite para la recepción de las ofertas, a fin de que los oferentes puedan tomar medidas apropiadas. De ser necesario, se debe prorrogar la fecha límite. El Banco debe recibir una copia (por escrito o en forma electrónica) y debe ser consultado con respecto a una notificación de "no objeción" cuando el contrato esté sujeto a revisión ex ante.";* y, en cumplimiento a lo determinado en la Solicitud de Ofertas en la Sección I. Instrucciones a los Oferentes (IAO) en el numeral 9. Enmienda al Documento de Licitación en los numerales:

"9.1 El Comprador podrá, en cualquier momento antes de que venza el plazo de presentación de Ofertas, modificar el documento de licitación mediante la publicación de enmiendas.

9.2 Todas las enmiendas publicadas formarán parte del documento de licitación y se comunicarán por escrito a todos los interesados que hayan obtenido el Documento de Licitación del Comprador de acuerdo con lo dispuesto en la IAO 7.3. Asimismo, el Comprador publicará sin demora la enmienda en su página web, con arreglo a la IAO 8.1.

Al respecto se informa las siguientes enmiendas, las mismas que se deberá tomar en cuenta al momento de elaborar la oferta a presentar:

ENMIENDA Nro. 1.-

Sección II. Datos de la Licitación (DDL), página 42, IAO 1.1:

Dice:

ÍTEM	TIPO DE RECURSO	DESCRIPCIÓN	CANTIDAD
1	Componente de Hardware	GATEWAYS DEL SISTEMA DE FIREWALL Debe incluir: • Garantía y soporte por 3 años, • Licenciamiento y/o suscripciones de seguridad por 3 años.	4
2	Componente de Hardware	SERVIDORES DE GESTIÓN Debe incluir: • Garantía y soporte de fábrica por 3 años, • Licenciamiento y/o suscripciones de LOM por 3 años.	2
3	Componente de Hardware	GESTORES DEL SISTEMA DE FIREWALL Debe incluir: • Soporte de fábrica por 3 años, • Licenciamiento y/o suscripciones de seguridad por 3 años.	2
4	Componente de Software	COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS Debe incluir: • Soporte de fábrica por 3 años, • Software base, • Licenciamiento y/o suscripciones por 3 años.	2
5	Componente de Software	SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO, POR AÑO Debe incluir: • Soporte de fábrica por 1 año, • Licenciamiento y/o suscripciones para 3384 buzones por 1 años.	3
6	Servicios conexos	MIGRACIÓN	1
7	Servicios conexos	SOPORTE LOCAL, POR 884 DÍAS Debe incluir: • Mantenimiento preventivo, • Mantenimiento correctivo, • Asistencia técnica.	1

Nota:

Los GESTORES DEL SISTEMA DE FIREWALL constituyen una función indispensable para la operación de los GATEWAYS DEL SISTEMA DE FIREWALL, siendo estos interdependientes. Por este motivo este ítem es considerado como componente de hardware

Dirá:

ÍTEM	TIPO DE RECURSO	DESCRIPCIÓN	CANTIDAD
1	Componente de Hardware	GATEWAYS DEL SISTEMA DE FIREWALL Debe incluir: • Garantía y soporte por 3 años, • Licenciamiento y/o suscripciones de seguridad por 3 años.	4
2	Componente de Hardware	SERVIDORES DE GESTIÓN Debe incluir: • Garantía y soporte de fábrica por 3 años, • Licenciamiento y/o suscripciones de LOM por 3 años.	2
3	Componente de Software	GESTORES DEL SISTEMA DE FIREWALL Debe incluir: • Soporte de fábrica por 3 años, • Licenciamiento y/o suscripciones de seguridad por 3 años.	2
4	Componente de Software	COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS Debe incluir: • Soporte de fábrica por 3 años, • Software base, • Licenciamiento y/o suscripciones por 3 años.	2
5	Componente de Software	SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO, POR AÑO Debe incluir: • Soporte de fábrica por 1 año, • Licenciamiento y/o suscripciones para 3384 buzones por 1 años.	3
6	Servicios conexos	MIGRACIÓN	1
7	Servicios conexos	SOPORTE LOCAL, POR 884 DÍAS Debe incluir: • Mantenimiento preventivo, • Mantenimiento correctivo, • Asistencia técnica.	1

ENMIENDA Nro. 2.-

Sección VIII. Condiciones Especiales de Contrato (CEC), página 173, CGC 16.1:

Dice:

ÍTEM	TIPO DE RECURSO	DESCRIPCIÓN	CANTIDAD
1	Componente de Hardware	GATEWAYS DEL SISTEMA DE FIREWALL Debe incluir: • Garantía y soporte por 3 años, • Licenciamiento y/o suscripciones de seguridad por 3 años.	4
2	Componente de Hardware	SERVIDORES DE GESTIÓN Debe incluir: • Garantía y soporte de fábrica por 3 años, • Licenciamiento y/o suscripciones de LOM por 3 años.	2
3	Componente de Hardware	GESTORES DEL SISTEMA DE FIREWALL Debe incluir: • Soporte de fábrica por 3 años, • Licenciamiento y/o suscripciones de seguridad por 3 años.	2
4	Componente de Software	COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS Debe incluir: • Soporte de fábrica por 3 años, • Software base, • Licenciamiento y/o suscripciones por 3 años.	2
5	Componente de Software	SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO, POR AÑO Debe incluir: • Soporte de fábrica por 1 año, • Licenciamiento y/o suscripciones para 3384 buzones por 1 años.	3
6	Servicios conexos	MIGRACIÓN	1
7	Servicios conexos	SOPORTE LOCAL, POR 884 DÍAS Debe incluir: • Mantenimiento preventivo, • Mantenimiento correctivo, • Asistencia técnica.	1

Nota:

Los GESTORES DEL SISTEMA DE FIREWALL constituyen una función indispensable para la operación de los GATEWAYS DEL SISTEMA DE FIREWALL, siendo estos interdependientes. Por este motivo este ítem es considerado como componente de hardware

Dirá:

ÍTEM	TIPO DE RECURSO	DESCRIPCIÓN	CANTIDAD
1	Componente de Hardware	GATEWAYS DEL SISTEMA DE FIREWALL Debe incluir: • Garantía y soporte por 3 años, • Licenciamiento y/o suscripciones de seguridad por 3 años.	4
2	Componente de Hardware	SERVIDORES DE GESTIÓN Debe incluir: • Garantía y soporte de fábrica por 3 años, • Licenciamiento y/o suscripciones de LOM por 3 años.	2
3	Componente de Software	GESTORES DEL SISTEMA DE FIREWALL Debe incluir: • Soporte de fábrica por 3 años, • Licenciamiento y/o suscripciones de seguridad por 3 años.	2
4	Componente de Software	COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS Debe incluir: • Soporte de fábrica por 3 años, • Software base, • Licenciamiento y/o suscripciones por 3 años.	2
5	Componente de Software	SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO, POR AÑO Debe incluir: • Soporte de fábrica por 1 año, • Licenciamiento y/o suscripciones para 3384 buzones por 1 años.	3
6	Servicios conexos	MIGRACIÓN	1

ÍTEM	TIPO DE RECURSO	DESCRIPCIÓN	CANTIDAD
7	Servicios conexos	SOPORTE LOCAL, POR 884 DÍAS Debe incluir: • Mantenimiento preventivo, • Mantenimiento correctivo, • Asistencia técnica.	1

ENMIENDA Nro. 3.-

Sección VI. Requisitos de los Bienes y Servicios Conexos, página 110, incluir numeral 16:

Es responsabilidad del contratista realizar el despliegue, instalación y configuración del software del nuevo agente de VPN. Los mecanismos de despliegue automático con los que cuenta el SRI (ejemplo: GPO, Gestor de paquetes de software) estarán disponibles para este fin; sin embargo, en el caso de que los mecanismos de distribución remota fallen, la instalación deberá ser realizada por el contratista de forma manual.

ENMIENDA Nro. 4.-

Sección VI. Requisitos de los Bienes y Servicios Conexos, página 140, A. COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS, SUPERVISIÓN, numeral 31:

Dice:

La función de supervisión debe emitir alertas al menos por correo electrónico y por mensajería instantánea Telegram

Dirá:

La función de supervisión debe emitir alertas al menos por correo electrónico y por un canal gratuito de mensajería instantánea, de preferencia Telegram.

ENMIENDA Nro. 5.-

Sección III. Criterios de Evaluación y Calificación, PERSONAL TÉCNICO MÍNIMO, página 60, rol “Técnico especialista de soporte técnico”, perfil “Estudios o certificados requerido”:

Dice:

Técnico especialista de soporte técnico (*Personal a presentarse en la ejecución contractual*)	3	**Nivel de Estudio:** Título Universitario **Titulación Académica:** Ingeniero en Sistemas, o Ingeniero en Telecomunicaciones, o Ingeniero en Electrónica, o equivalente. **Tipo de experiencia:** Proyectos de mantenimiento o soporte de la solución ofertada. Para el efecto se deberá presentar certificados que respalden la experiencia. **Tiempo mínimo de experiencia:** 2 años **Número de proyectos:** Mínimo 1 proyecto **Estudios o certificado requerido:** Certificación Técnica vigente nivel profesional, avanzado o equivalente emitida por el fabricante del sistema de Firewalls y/o el servicio SaaS de protección de correo electrónico ofertados.	• Gestionar los casos de mantenimiento correctivo, mantenimiento preventivo, asistencia técnica y garantía técnica. • Diligenciar todos los insumos necesarios para la atención de los casos de soporte local. • Gestionar y coordinar las actividades con el fabricante necesarias para la atención de los casos de soporte local. • Elaborar la documentación de respaldo de la gestión del soporte local.

Dirá:

Técnico especialista de soporte técnico (*Personal a presentarse en la ejecución contractual*)	3	**Nivel de Estudio:** Título Universitario **Titulación Académica:** Ingeniero en Sistemas, o Ingeniero en Telecomunicaciones, o Ingeniero en Electrónica, o equivalente. **Tipo de experiencia:** Proyectos de mantenimiento o soporte de la solución ofertada. Para el efecto se deberá presentar certificados que respalden la experiencia. **Tiempo mínimo de experiencia:** 2 años **Número de proyectos:** Mínimo 1 proyecto **Estudios o certificado requerido:** Certificación Técnica vigente nivel profesional, avanzado o equivalente emitida por el fabricante del sistema de Firewalls **y** el servicio SaaS de protección de correo electrónico ofertados.	• Gestionar los casos de mantenimiento correctivo, mantenimiento preventivo, asistencia técnica y garantía técnica. • Diligenciar todos los insumos necesarios para la atención de los casos de soporte local. • Gestionar y coordinar las actividades con el fabricante necesarias para la atención de los casos de soporte local. • Elaborar la documentación de respaldo de la gestión del soporte local.

ENMIENDA Nro. 6.-

Sección VI. Requisitos de los Bienes y Servicios Conexos, PROTECCIÓN DE CORREO ELECTRÓNICO, página 142, numeral 24:

Dice:

La solución debe permitir la adición de etiquetas en el correo electrónico entrante que permitan, al menos, informar al destinatario:

- Cuando un correo electrónico es enviado desde un dominio externo,
- Si se trata de un remitente desconocido,
- Si es un dominio recientemente registrado.

Dirá:

La solución debe contar con los siguientes mecanismos de protección para el correo entrante:

- Informar al destinatario cuando un correo electrónico es enviado desde un dominio externo,
- Informar al destinatario cuando se trata de un remitente desconocido,
- Poner en cuarentena el correo cuando se trata de un dominio recientemente registrado.

ENMIENDA Nro. 7.-

Sección VI. Requisitos de los Bienes y Servicios Conexos, página 144, PROTECCIÓN DE PROTOCOLO SMTP, numeral 38:

Dice:

La solución debe permitir al administrador configurar las reglas de protección de correo electrónico en base de al menos los siguientes parámetros:

- Tamaño de archivo adjunto,
- Cantidad de archivo adjunto,
- Cantidad de archivos contenidos en un solo archivo comprimido,
- Metadatos de archivo adjuntos,
- Campo MFROM del remitente y receptor,
- Campo desde el subtítulo y el receptor,
- Extensión de archivo adjunta,

- Nombre de archivo adjunto,
- Tamaño de archivo comprimido,
- Contenido HTML contenido en el cuerpo del correo electrónico,
- Cualquier etiqueta HTML contenida en el cuerpo del correo electrónico,
- Número de restantes,
- Lenguaje utilizado en el cuerpo del correo electrónico,
- Código de país Origen enviando correo electrónico,
- Tiempo de registro de dominio utilizado en los campos de o MFROM,
- Detectar si el correo electrónico está encriptado,
- Campo Helo,
- Número de conexiones SMTP de una sola IP,
- Antigüedad del dominio utilizado en el campo desde y/o MFROM.

Dirá:

La solución debe permitir al administrador configurar las reglas de protección de correo electrónico en base de al menos los siguientes parámetros:

- *Tamaño de archivo adjunto,*
- *Cantidad de archivo adjunto,*
- *Cantidad de archivos contenidos en un solo archivo comprimido,*
- *Metadatos de archivo adjuntos,*
- *Campo MFROM del remitente y receptor,*
- *Campo desde el subtítulo y el receptor,*
- *Extensión de archivo adjunta,*
- *Nombre de archivo adjunto,*
- *Tamaño de archivo comprimido,*
- *Contenido HTML contenido en el cuerpo del correo electrónico,*
- *Cualquier etiqueta HTML contenida en el cuerpo del correo electrónico,*
- *Número de destinatarios,*

- *Lenguaje utilizado en el cuerpo del correo electrónico,*
- *Código de país Origen desde el que se envía el correo electrónico,*
- *Tiempo de registro de dominio utilizado en los campos de o MFROM,*
- *Detectar si el correo electrónico está encriptado,*
- *Campo Helo,*
- *Número de conexiones SMTP de una sola IP."*

ENMIENDA Nro. 8.-

Sección VI. Requisitos de los Bienes y Servicios Conexos, página 144, CONTROL ANTISPAM, numeral 41:

Dice:

La función de control antispam debe ser al menos de tercera generación, incluyendo análisis por medio de aprendizaje automático ("machine learning").

Dirá:

La función de control antispam debe contar con al menos las siguientes funcionalidades avanzadas de protección:

- Uso de inteligencia artificial (IA) o algoritmos de machine learning para la detección de amenazas.
- Análisis contextual y semántico del contenido.
- Mecanismos de autenticación avanzados: SPF, DKIM, DMARC.
- Análisis de comportamiento de usuarios y remitentes.
- Actualizaciones automáticas basadas en bases de datos globales de amenazas.

ENMIENDA Nro. 9.-

Sección VI. Requisitos de los Bienes y Servicios Conexos, FIREWALL (FW), página 123, numeral 20:

Dice:

El Firewall debe soportar el uso de etiquetas en los objetos para su referenciación o agrupación.

Dirá:

El Firewall debe soportar el uso de etiquetas, categorías u otros mecanismos en los objetos o políticas para su referenciación o agrupación.

ENMIENDA Nro. 10.-

Sección VI. Requisitos de los Bienes y Servicios Conexos, CONTROL ANTISPAM, página 145, numeral 49:

Dice:

La cuarentena debe almacenar los mensajes en carpetas diferenciadas de acuerdo con el tipo motor de detección.

Dirá:

La cuarentena debe contar con un mecanismo para identificar el tipo de motor de detección con el cual fueron puestos en cuarentena los correos, de manera que permita configurar acciones diferenciadas en función de esta clasificación.

ENMIENDA Nro. 11.-

Sección VI. Requisitos de los Bienes y Servicios Conexos, CONTROL ANTIMALWARE, página 145, numeral 53:

Dice:

La solución debe tener la capacidad de detectar y bloquear:

- Virus,
- Riskware,
- Spyware,
- Archivos cifrados,
- Archivos con contraseña.

Dirá:

La solución debe tener la capacidad de detectar y aplicar acciones de control sobre:

- Virus,
- Riskware,
- Spyware,
- Archivos cifrados,
- Archivos con contraseña.

ENMIENDA Nro. 12.-

Eliminar el numeral 54 de la Sección VI. Requisitos de los Bienes y Servicios Conexos, CONTROL ANTIMALWARE, página 145 que dice:

La solución debe soportar el análisis y la aplicación de acciones específicas para archivos cifrados o protegidos por contraseña o con compresión múltiple.

ENMIENDA Nro. 13.-

Sección VI. Requisitos de los Bienes y Servicios Conexos, CONTROL ANTIMALWARE, página 145, numeral 55:

Dice:

La solución debe contar con inteligencia que permita intentar acceder a un archivo protegido con contraseña utilizando información contextual del mensaje utilizado para su envío.

Dirá:

La solución debe contar con inteligencia que permita acceder y analizar un archivo protegido con contraseña.

ENMIENDA Nro. 14.-

Sección VI. Requisitos de los Bienes y Servicios Conexos, CONTROL ANTIMALWARE, página 146, numeral 60:

Dice:

Si al momento de realizar análisis de sandboxing de un hipervínculo el recurso web asociado no se encuentra disponible, la solución debe contar con la opción de que el mensaje sea entregado no sin antes reescribir la dirección URL del hipervínculo de manera que, si el usuario hace clic, este se despliegue en un entorno controlado y aislado

Dirá:

La solución debe tener la capacidad de reescribir la dirección URL del hipervínculo de manera que, si el usuario hace clic, este se despliegue en un entorno controlado y aislado.

ENMIENDA Nro. 15.-

Sección VI. Requisitos de los Bienes y Servicios Conexos, CONTROL ANTIMALWARE, página 146, numeral 63:

Dice:

La solución debe ser capaz de analizar al menos los siguientes tipos de archivos comprimidos: ZIP, TGZ, 7Z, CAB, LZH, RAR, TNEF.

Dirá:

La solución debe ser capaz de analizar al menos los siguientes tipos de archivos comprimidos: ZIP, TGZ, 7Z, CAB, RAR

ENMIENDA Nro. 17.-

Eliminar el numeral 54 de la Sección VI. Requisitos de los Bienes y Servicios Conexos, CONTROL DE PHISHING, página 146 que dice:

"La solución debe tener la capacidad de reescribir la dirección URL del hipervínculo de manera que, si el usuario hace clic, este se despliegue en un entorno controlado y aislado."

ENMIENDA Nro. 18.-

Sección VI. Requisitos de los Bienes y Servicios Conexos, GESTIÓN DE EVENTOS, REPORTES Y AUDITORÍA, página 147, numeral 88:

Dice:

La solución debe contar con paneles ("dashboards") o reportes que provean al administrador información sobre estadísticas y tendencias de las amenazas de seguridad detectadas, incluyendo:

- Cuentas comprometidas,
- Archivos confidenciales potencialmente expuestos,
- Correos electrónicos filtrados,
- Credenciales de usuarios expuestas,
- Accesos OAuth no seguros,
- Usuarios o cuentas que han sido más atacados,
- Usuarios con comportamientos de alto riesgo,
- Acciones del análisis de caja de arena ("sandbox"),
- Accesos (clics) a direcciones URL,
- Malware detectado,
- Mensajes spam,
- Cómo se atacan esas cuentas,
- Compartición riesgosa de archivos en las aplicaciones de Microsoft Office 365,

- Demás amenazas detectadas por la solución.

Dirá:

La solución debe contar con paneles (“dashboards”) o reportes que provean al administrador información sobre estadísticas y tendencias de las amenazas de seguridad detectadas, incluyendo:

- Cuentas comprometidas,
- Archivos confidenciales potencialmente expuestos,
- Correos electrónicos filtrados,
- Credenciales de usuarios expuestas,
- Accesos no seguros,
- Usuarios o cuentas que han sido más atacados,
- Usuarios con comportamientos de alto riesgo,
- Acciones del análisis de caja de arena (“sandbox”),
- Accesos (clics) a direcciones URL,
- Malware detectado,
- Mensajes spam,
- Cómo se atacan esas cuentas,
- Compartición riesgosa de archivos en las aplicaciones de Microsoft Office 365,
- Demás amenazas detectadas por la solución.