VICEPRESIDENCIA DE LA REPÚBLICA DOMINICANA

ADESS

ADMINISTRADORA DE SUBSIDIOS SOCIALES

TÉRMINOS DE REFERENCIA

Renovación suite de seguridad tecnológica

Elaborado por:

Henry Amin Martinez,

Gerente sistemas, redes y soporte

Av. Gustavo Mejia Ricart #141, Ens. Julieta, Edif. ADESS

Santo Domingo, Rep. Dom., Código Postal: 10130

Indice

Objetivo General 3

Objetivos Específicos: 3

Alcance: 3

Metodología o forma en que se prestará el servicio 3

Actividades a realizar 4

Condiciones 4

Condiciones del lugar y duración del trabajo: 4

Condiciones de la solución: 5

Transferencia de conocimiento 8

Entregables: 9

Monto de la ejecución y modo de pago. 9

Confidencialidad de la información: 9

Conflicto de intereses – elegibilidad: 11

Requisitos legales: 11

Objetivo General

Renovar la suite de seguridad tècnológica EndPoint Protection Business, FortiMail y Web Security, Gateway edition a su última versión, bajo las mejores prácticas y recepción de capacitación oficial.

Objetivos Específicos:

- Contar con una solución de seguridad tecnológica de usuario final.
- Poder gestionar de manera efectiva la seguridad de la información mediante una herramienta que permita encriptar los datos y carpetas.
- Poder tener una herramienta de control de dispositivos móviles
- Recibir la capacitación oficial para la administración efectiva de la solución implementada.

Alcance:

La contratación incluye los servicios, bienes tangibles e intangibles necesarios para la implementación de la renovación de la solución de seguridad tecnológica hasta la puesta en producción de la solución requerida incluyendo la transferencia de conocimiento y capacitaciones para su administración.

Metodología o forma en que se prestará el servicio

El proveedor presentara la propuesta de la metodología usada para alcanzar los objetivos, atendiendo las condiciones presentadas en este TDR, este documento formara parte de los documentos requeridos para la evaluación.

Se realizara un levantamiento del diseño y de las informaciones requeridas por el proveedor o los interesados para estimar los recursos requeridos para la implementación llave en mano de la solución, esta visita se podrá realizar el próximo día laborable de la fecha de publicación de la oferta, para realizar el levantamiento de información requerido para la presentación de la oferta.

Los datos de los interesados deberán ser enviados a la cuenta compras@adess.gob.do indicando las siguientes informaciones mínimas de contacto:

- Nombre y apellido
- Cedula de identidad
- Nombre de la empresa que representa
- RNC
- NCF

Actividades a realizar

- Realizar el diseño de arquitectura para la implementación de la solución de monitoreo de dispositivos tecnológicos
- Registrar y entregar el o los licenciamiento relacionados a la solución.
- Configurar la solución según el diseño establecido, realizando las mejores prácticas.
- Realizar la transferencia de conocimiento del proceso de implementación a 2 técnicos del área de infraestructura.
- Configurar al menos 2 reglas por cada módulo de la suite.
- Realizar las pruebas de todas las políticas y establecidas.
- Entregar reporte final de implementación.

Condiciones

Condiciones del lugar y duración del trabajo:

- Todos los trabajos de implementación serán realizados en las instalaciones de la oficina principal de la Administradora de Subsidios Sociales dirección Av. Gustavo Mejia Ricart #141, Ens. Julieta, Edif. ADESS, Santo Domingo, Rep. Dom., Código Postal: 10130, en horarios a partir de las 8:00 AM- 10:00 PM en días laborables, a partir de las 8:00 AM- 5:00 PM para los fines de semana si fuera requerido.

- Todas las actividades de implementación serán realizadas in Situ, no se permitirán accesos remotos ni se suministraran equipos o suministros como PC, Laptops, Cables de red, etc. que sean requeridos para realizar los trabajos solicitados, el proveedor deberá de contar con todos los insumos requeridos para la entrega efectiva de la solución requerida.

- Los trabajos de implementación no pueden exceder las 2 semanas calendario a partir de la recepción de los equipos o recursos requeridos.

Condiciones de la solución:

1. Complete Endpoint Protection—Business

Antimalware (PC, Mac, Linux, máquinas virtuales)

Endpoint Security

- Se comunica con varias tecnologías de protección de endpoints en tiempo real para analizar y colaborar frente a las amenazas nuevas y avanzadas, bloqueándolas rápidamente antes de que afecten a sus sistemas y usuarios.

Contención dinámica de aplicaciones

- Examina los comportamientos de forma segura y contiene amenazas como greyware, ransomware, amenazas "paciente cero",etc., sin necesidad de conexión a la nube.

Real Protect

- Detecta y detiene amenazas avanzadas y de tipo zero-day con análisis de comportamientos en tiempo real y aprendizaje automático que combina la extracción de características antes de la ejecución con el análisis de comportamientos y memoria posterior a la ejecución, con el objetivo de capturar las amenazas.
- Protege frente a malware preparado para entornos aislados. Para ello, le permite ejecutar los comportamientos "maliciosos", lo analiza en tiempo real y, a continuación, con la función de contención dinámica de aplicaciones, suprime las acciones maliciosas antes de que el malware haya infectado ningún sistema.

Application Control

- Prevención de la instalación y ejecución de aplicaciones no deseadas y malware, con un mínimo impacto en el rendimiento del sistema, los usuarios o los administradores.

Prevención de intrusiones y firewall para equipos de sobremesa

- Protección contra amenazas desconocidas, de tipo zero-day y nuevas vulnerabilidades.
- Reducción de los parches de urgencia.

Global Threat Intelligence

- Protección contra las amenazas nuevas y emergentes en todos los vectores, gracias a la información sobre amenazas en tiempo real recopilada por millones de sensores ubicados en todo el mundo.
- Creación de controles personalizados para prevenir exploits, ataques a la memoria y amenazas que intentan ejecutarse con más privilegios.

2. Seguridad de la Web y de la mensajería

Control web de McAfee con filtrado de URL y búsquedas seguras

• Alerta a los usuarios sobre los sitios web maliciosos antes de que los visiten, con el fin de reducir el riesgo y garantizar el cumplimiento de las normativas.

• Implementa directivas de navegación en la Web que autorizan o bloquean el acceso a los sitios web.

Antimalware y antispam para el correo electrónico

- Protección de su servidor de correo electrónico e interceptación del malware antes de que llegue a la bandeja de entrada del usuario.
- Detección, limpieza y bloqueo del malware de los servidores Microsoft Exchange y Lotus Domino con McAfee Security for Email Servers.

Protección de datos

Control de dispositivos

- Prevención de la pérdida de datos confidenciales mediante la limitación del uso de soportes extraíbles.

Cifrado del disco completo, archivos, carpetas, soportes extraíbles y almacenamiento en la nube

- Protección de los datos confidenciales en PC, Mac, portátiles, servidores de red, soportes extraíbles y servicios de almacenamiento en la nube.

Administración

Software

- Administración de las directivas, el cumplimiento de normativas y la generación de informes desde una única consola centralizada.
- Administración simplificada en entornos de SO mixtos con directivas multiplataforma.

La solución presentada debe de ser presentada con modalidad de licenciamiento perpetuo para 100 nodos y contar con soporte del fabricante por 1 año.

3. Web Security (Web Protection, Web Gateway)

Seguridad avanzada

- Protección de la Web mediante la eficaz combinación de filtrado basado en la reputación y filtrado basado en categorías.
- El análisis preventivo que abre los contenidos en tiempo real para la prevención de amenazas zero-day
- La seguridad por capas ofrece una protección inmediata y eficaz contra el malware y otras amenazas ocultas.
- Protección del tráfico de entrada y de salida
- Detección del malware Zero-Day

La solución presentada debe de ser presentada con modalidad de licenciamiento perpetuo para 200 nodos y contar con soporte del fabricante por 1 año.

4. Protección del correo electrónico en la nube

Posibles despliegues:

- Modo Relay o Gateway
- Modo Transparente enrutado o Bridge

Métodos de detección de spam

Inspección durante la conexión

- Reputación IP
- Base de datos Botnet
- Reputación dinámica de remitentes en local
- Límite de conexiones por IP remota

Inspección de cabeceras

- Verificación de remitentes
- Cumplimiento RFC
- Control de ratio de errores SMTP
- Listas de remitentes blancas y negras
- Protección DHA
- SPF/DomainKey Identified Mail (DKIM)
- Greylisting

Inspección del contenido

- FortiGuard Spam DB
- Detección Heurística
- Filtros Bayesianos
- Detección de Newsletter
- Detección Anti-Malware
- Filtro de contenidos Web

Cifrado Basado en políticas

- TLS
- S/MIME
- Identity Based Encryption (IBE)

Soporte LDAP

La solución presentada debe de ser presentada con modalidad de licenciamiento perpetuo para 150 nodos y contar con soporte del fabricante por 1 año.

Transferencia de conocimiento

- El proveedor realizara la trasferencia de conocimiento del proceso de implementación al personal técnico (2 técnicos) de la institución que le acompañaran.

Capacitación

El proveedor presentara una capacitación oficial ya sea por el fabricante o por una academia certificada, no menos de 32 horas de entrenamiento con laboratorio, que incluya los siguientes tópicos:

- ePolicy Orchestrator (ePO) Overview
- Overview of McAfee Security Risk Management (SRM)
- Policy Tuning ePO Repositories Global Updating
- Deploying Common Management Agent
- Setting up Dashboards within ePO
- Deploying VirusScan +Anti-Spyware
- Artemis+ Site Advisor.
- Local installation
- Deploying with ePO
- Working with VirusScan Policies
- McAfee default policies Configuring Alerting policies
- Deploying Host Intrusion prevention (HIPs)

- Checking packages into the ePO repository
- Setting and pushing deployment tasks
- Working with HIPs Policies Firewall configuration
- Configuring Host Intrusion Prevention
- Policies Trusted applications and
- application blocking Adaptive learning mode
- Reporting Overview
- Custom Configuration
- Queries Displaying queries on the dashboard
- Device Control
- Basic Configuration

Entregables:

1. Cronograma de trabajo y recepción activos
2. Entrega de los activos (físicos, licencia).
3. Entrega de toda la documentación relativa a la garantía ofrecida, garantía local, diseños requeridos y matriz de escalamiento de soporte, etc.
4. Entrega de todos las licencias implementadas y adquiridas.

Recursos y facilidades a ser provistos por la entidad

- Acompañamiento de personal técnico de Sistemas tecnológicos, sujeto a las condiciones de horarios establecidas.
- Servicios de energía interrumpida
- Servicios de comunicación telefónica local
- Servicios de Internet (Wifi)
- Datos e informaciones técnicas requeridas

Monto de la ejecución y modo de pago.

El monto contratado incluirá equipos, periféricos, partes, materiales, mano de obra y supervisión en adición a valores aplicables a este contrato, estipulados por ley, tales como: Seguros, Pólizas y Fianzas.

Los pagos serán realizados de acuerdo los productos entregables, a razón de:

- Pago único con crédito a 45 días a partir de la implementación llave en mano, incluyendo todas las actividades presentadas en los entregables.

Perfil del proveedor:

Perfil mínimo requerido para la implementación de la solución:

Formación Académica del Consultor:

- ✓ Bachiller Industrial, Perito, Auditor, Ingeniero, especialista certificado en soluciones de seguridad tecnológica.

Habilidades y otros conocimientos:

- ✓ Amplios conocimientos sobre en soluciones de seguridad tecnológica, seguridad de red, WAn y LAN, VPN, etc.

Experiencia previa en la prestación de estos servicios:

- ✓ Experiencia mínima de 3 años en implementaciones y prestaciones de servicios orientados a en soluciones de seguridad perimetral.

Documentación legal previa al contrato del proveedor del servicio:

- ✓ El proveedor deberá presentar certificado de fábrica en original, sellada, timbrada y firmada por el fabricante indicando que este cuenta con su aprobación para realizar implementaciones de productos y soluciones de seguridad perimetral
- ✓ Contar con buena reputación moral y social.

Referencias de trabajos similares proporcionados

- ✓ Experiencia en al menos 3 proyectos similares en los últimos 3 años.

Criterios de selección/evaluación:

Documentos sujetos a criterios de evaluación	Escala de puntos (min-máx.)	Puntuación
Formación Académica del Consultor y Habilidades y otros conocimientos.	0-10	
Experiencia previa en la prestación de estos servicios.	0-10	
Referencias de trabajos similares proporcionados.	0-10	
Documentación legal del proveedor del servicio.	0-10	
Cronograma de ejecución y recepción activos	0-5	
Cumplimiento al RFT y condiciones de la solución.	0-40	
Capacitaciones y entrenamiento y Transferencia del conocimiento.	0-15	
Total	0-100	
Total según evaluación:		

Confidencialidad de la información:

Todo el ejecutivo, operativo y personal técnico que interactúe con los datos e informaciones de configuraciones, datos guardados, etc. deberá de aceptar el documento Acuerdo de Confidencialidad y Privacidad con terceros que serán entregados con la adjudicación del contrato.

Conflicto de intereses – elegibilidad:

Para efectos de la decisión de participar en el proceso de selección y/o aceptación de la contratación, los candidatos deberán tener en cuenta las causales de conflicto de interés y elegibilidad establecidas en la ley 340-06 sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones, los cuales podrán ser consultados en la página Web:

http://www.comprasdominicana.gov.do/web/guest/leyes-y-decretos

Requisitos legales:

Para proveedor:

- Facturas a clientes comerciales, al menos 3 del último año de operaciones.
- Mínimo dos (2) referencias de trabajos ejecutados, en los últimos cinco años, de naturaleza similar al licitado; se aceptan referencias de trabajos ejecutados por un monto inferior al monto de la Oferta.
- Certificación original emitida por la Dirección General de Impuestos Internos (DGII), donde se manifieste que se encuentra al día en el pago de sus obligaciones fiscales. (Válido para la evaluación legal).
- Dos (2) Estados Financieros auditados de los últimos 2 periodos fiscales, certificados por una firma o un CPA; cuando la empresa tenga dos (2) años o más de constituida. Dichos estados financieros deben incluir los estados de resultados, mediante los cuales se verifique la facturación anual.
- Registro de Proveedor del Estado (RPE).
- Certificación emitida por la Tesorería de la Seguridad Social, donde se manifieste que se encuentra al día en el pago de sus obligaciones de la Seguridad Social.
- Copia del certificado de Registro Mercantil actualizado.
- Copia cedula del representante legal de la empresa.
- Copia de los Estatutos Sociales y Acta Constitutiva debidamente registrada y certificada por la Cámara de Comercio y Producción correspondiente al domicilio de la empresa; certificada y firmada de conformidad a su original por la gerencia

o por quienes ostenten poder de representación otorgado por dicha gerencia y debidamente sellada con el sello social de la empresa.

- Poder especial de representación en el cual la empresa autoriza a la persona a contratar en su nombre, debidamente legalizado por un notario y sellado con el sello de la empresa. El documento debe estar legalizado en la Procuraduría General de la Republica (PGR).

En caso de Consorcios, en adición se requieren los siguientes documentos:

- Convenio de Consorcio. Debidamente notariado y legalizado ante la Procuraduría General de la Republica (PGR).
- Acta de Asamblea de cada empresa que sea socia, en la que se refiera la decisión de participar en el Consorcio y la designación de un representante dentro del mismo. Acta debidamente registrada y certificada por la Cámara de Comercio y Producción correspondiente al domicilio de la empresa y debidamente sellada con el sello social de la empresa.

NOTA: Todas las certificaciones deben estar vigentes, la falta de cualquiera de estos documentos legales anula la oferta sin que pueda ser evaluada.