

**Formato de Requerimientos técnicos de referencia para la contratación de bienes y servicios**

|  |  |
| --- | --- |
| **Instancia encargada del levantamiento de requerimientos** | **Subdirección de Estándares y Arquitectura - Grupo de Seguridad y Privacidad TI – CSIRT Gobierno**  |
| **Justificación de la necesidad** | Apoyando la implementación y consolidación de la Política de Gobierno Digital y coadyuvando al cumpliendo el objetivo de la misma el cual promueve el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para la consolidación del Estado y de ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital. El valor público se relaciona con el desarrollo social, la gobernanza, la garantía de derechos, la satisfacción de necesidades y la prestación de servicios de calidad. No sólo es hacer uso de las tecnologías, sino cómo las tecnologías ayudan a resolver problemas reales, igualmente es lograr que el Estado llegue a donde no llega el mercado, y posibilitar la creación de nuevos mercados.En la actualidad se encuentra vigente el Convenio Interadministrativo No 782 de 2018 entre el Ministerio de Tecnologías de la Información y las Comunicaciones y la Policía Nacional, el cual enmarca los esfuerzos técnicos y administrativos para el desarrollo de actividades de acompañamiento y fortalecimiento de la operación del CSIRT de Gobierno el cual empezó su operación en octubre de 2017, recibiendo del CSIRT PONAL el apoyo humano, técnico y de transferencia de conocimiento para el uso de las herramientas tecnológicas para realizar las actividades de análisis, seguimiento y gestión de la infraestructura Tl de las entidades del Estado de nivel nacional y territorial.  Con la puesta en funcionamiento del CSIRT Gobierno en las instalaciones del Centro de Capacidades para la Ciberseguridad de Colombia, C4 en agosto de 2018, ofreciendo servicios proactivos, reactivos y de Gestión de la Seguridad básicos, ya para el primer semestre de 2019, se amplia el portafolio de servicios básicos, teniendo en cuenta la consecución de nuevas herramientas de seguridad que permiten ampliar las capacidades del CSIRT Gobierno. Teniendo en cuenta lo anterior, se requiere adquirir solución tecnológica-software y Hardware que permitan gestionar los diferentes requerimientos de incidentes de las Entidades del Estado y establecer cuando un portal o un servicio ciudadano se encuentra indisponible.Para la gestión de requerimientos – Tickets, se requeriría un software de mesa de ayuda ON Premise que pueda ser configurable a las necesidades propias del CSIRT Gobierno para la gestión de incidentes, esta solución servirá como punto único de contacto entre las entidades del orden nacional y territorial y el CSIRT Gobierno, con el fin de responder de manera oportuna, eficiente y con calidad las solicitudes (Ticket) de acompañamiento y tratamiento de incidentes cibernéticos.  |
| **Objetivo general del requerimiento técnico** | Adquirir una aplicación ON Premise, para la gestión de requerimientos de incidentes cibernéticos que reportan las Entidades públicas al CSIRT Gobierno. |
| **Alcance del requerimiento**  | Adquirir una aplicación ON Premise, que permita al CSIRT Gobierno contar con un punto único de contacto a nivel Colombia para 10 agentes y un supervisor, para centralizar los requerimientos (Ticket) sobre incidentes cibernéticos de las entidades nacionales y territoriales, para ser instalada en ambiente virtual. |
| **Aspectos no incluidos en el requerimiento** | N/A  |
| **Productos, entregables y resultados esperados** | * Solución de gestión de ticket de incidentes de seguridad, instalada, configurada y operativa.
* Manuales de administración y usuarios.
* Capacitación y transferencia de conocimiento.
* Soporte y mantenimiento de fábrica por 14 meses.
* Configuración de reportes personalizados
* Configuración del sistema de backup de la herramienta.
 |
| **Criterios de aceptación de los productos** | Que la solución de ticket cumpla con los requerimientos técnicos solicitados por el CSIRT Gobierno. |
| **Otros requerimientos técnicos** | La solución debe ser instalada en un servidor virtual.  |
| **Obligaciones técnicas específicas que deberá cumplir el contratista** | Especificaciones – Gestión de Tickets – Mesa de Ayuda* Gestión de ticket para 10 agentes y un supervisor.
* Configurable los formularios de entrada de datos, según requerimientos del CSIRT
* Implementación de solución en un servidor virtual de la infraestructura tecnológica de CSIRT Gobierno.
* Solución sobre plataforma Linux
* Incluir el licenciamiento del motor de base de datos.
* Aplicación escalable.
* Integración con la plataforma de intercambio de amenazas MISP, software gratuito y de código abierto que ayuda a compartir información de inteligencia de amenazas, incluidos los indicadores de seguridad cibernética. <https://www.misp-project.org/.>
* Integración con la herramienta de análisis de datos Tableau.
* Reportes ejecutivos configurables y personalizados
* Subida masiva de datos – migración de la data
* Capacitación para Administradores y usuarios
* Establecimiento de ANS de servicios para el soporte
* Entrega de manuales de usuario
* Creación de perfiles de lectura, escritura y modificación para usuarios
* Envió de notificaciones por correo electrónicos configurables
* Generación de Logs de auditorias
* Almacenamiento de soportes (documentos) del incidente en formato PDF.
* Soporte técnico deber ser ingeniero 5x8 telefónico con un tiempo de respuesta de máximo 30 minutos, en caso de no poder resolver el problema presentado, se debe hacer la atención en la Oficina de Telemática de la Policía Nacional Cra 59 No 26-21 Bogotá.
* La garantía debe ser para la totalidad de la solución.
* Realizar todas las actualizaciones liberadas de la solución contratada, durante el tiempo que dure el servicio.
* La herramienta debe permitir construir una base de conocimiento, con la información de los incidentes registrados.
* La herramienta debe permitir enviar notificaciones, cuando se realicen actualizaciones en el estado de los incidentes.
* La herramienta debe permitir extraer la información de los correos configurados en un buzón específico, con el fin de que permita crear los tiquetes de manera automática, a partir de las alertas enviadas por herramientas de seguridad, al buzón mencionado
* La herramienta debe permitir configurar listas desplegables de acuerdo a la clasificación del incidente.
* La herramienta debe permitir configurar plantillas diligenciadas previamente con la información de la respuesta del incidente, dependiendo del tipo.
 |
| **Obligaciones técnicas específicas que deberá cumplir ACAC para la ejecución del contrato** | 1. Pagar el valor de la contratación, en la forma, fechas y bajo las condiciones señaladas más adelante.
2. Verificar la afiliación y pago de aportes que EL CONTRATISTA debe efectuar al Sistema de Seguridad Social y ARL como independiente.
3. Vigilar la debida y oportuna ejecución del contrato y el cumplimiento de todas las obligaciones contractuales a cargo de EL CONTRATISTA.
 |
| **Duración del Contrato:** | 14 meses   |
| **Valor estimado del contrato:** | $167,790,000 IVA INCLUIDO |
| **Documentos Anexos requeridos:** | * Acuerdos de Niveles de Servicios
* Protocolo de escalabilidad soporte técnico a problemas con el servicio.
* Acuerdos de confidencialidad
* Documentos requeridos por ACAC para realizar la contratación.
	+ Certificador de representación legal de cámara y comercio vigente
	+ Estados financieros con corte 31 de diciembre 208
	+ Carta de intención para la creación de unión temporal en caso que se requiera
	+ Carta de propuesta firmada por el representante legal
* Cronograma de plan de implementación.
* Documentación técnica
 |
| **Observaciones:** | N/A  |
|

**Características del servidor para instalación aplicación de gestión de Tiqckets**

|  |  |
| --- | --- |
| **CARACTERÍSTICA**  | **DESCRIPCIÓN**  |
| Chasis  | Con base o de montaje en Rack, cable de alimentación, guía de instalación, kits de montaje  |
| Trusted Platform Module (TPM)  | Trusted Platform Module 2.0  |
| Procesador que cuente como mínimo con las siquientes características  | Intel® Xeon® Gold 6154 3.0G, 18Cores / 36T, 10.4GT / s, 25M Cache, Turbo, HT (200W) DDR4-2666  |
| Procesador adicional que cuente como mínimo con las siquientes características  | Intel® Xeon® Gold 6154 3.0G, 18Cores / 36T, 10.4GT / s, 25M Cache, Turbo, HT (200W) DDR4-2666  |
| Configuración térmica del procesador  | 2 Standard Heatsinks for 125W or less CPUs  |
| Tipo de configuración de memoria  | Fault Resilient Memory-Vmware  |
| Tipo y velocidad de los DIMM de memoria  | 2666MT/s RDIMMs  |
| Memoria  | 256GB instalados en 8 RDIMM Dual Rank de 32 GB cada uno, 2666MT/s,  |
| Sistema Operativo  | VMware ESXi 6.5 U2 Embedded Image  |
| Virtualization software and Support  | VMware vCenter Foundation, per instance limit 4 hosts 3 year  |
| Discos duros y configuración RAID 5  | 480GB SSD SATA 12Gbps 2.5 in Hot-plug AG Drive, 1 DWPD, 876 TBW, Cantidad: 6 (seis) El RAID debe estar instalado y configurado  |
| Controladora de discos:  | Interfaces requeridas: SAS Velocidad de transferencia de datos requerida: 12 Gbit/s Número de canales: 8 (ocho) Capacidad mínima de cantidad unidades de almacenamiento: 16  |
| Controladora y configuración de RAID  | Controladora dedicada (Hardware) configurada para RAID 5 que cumpla con: Chipsets Intel compatibles Una unidad de disco duro ATA serie (SATA)  Controlador RAID habilitado en el BIOS  BIOS de la motherboard que incluye la primera ROM de la opción Intel Software de Intel RST  |
| Boot Optimized Storage Cards  | BOSS controller card + with 2 M.2 Sticks 240G (RAID 1),FH  |
| Fuente de alimentación  | Dual, Hot-plug, Redundant Power Supply (1+1), 1100W  |
| Cable de poder  | Incluido para cada fuente  |
| Embedded Systems Management  | Especificar el requerido por el sistema propuesto y ofrecido por el fabricante  |
| Adaptador de Red  | Broadcom 57416 2 Port 10Gb Base-T + 5720 2 Port 1Gb Base-T, rNDC  |
| Adaptador de red adicional  | Broadcom 57416 Dual Port 10Gb, Base-T, PCIe Adapter, Full Height, Cantidad (6)  |
| Quick Sync  | Quick Sync 2 (At-the-box mgmt)  |
| Guías para rack  | Rieles deslizantes con brazo o soporte para administración de cableado  |
| Garantía básica  | 3Yr Basic Warranty - Next Business Day - Minimum Warranty  |
| Servicios ampliados  | 3Yr ProSupport Plus and Next Business Day Onsite Service  |

**Campos Requeridos Formulario de entrada - Planilla de Registro**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | No. DE TICKET | MEDIO DEL REPORTE | ORDEN DE LA ENTIDAD | SECTOR/DEPARTAMENTO |
|  |  |  |  |  |
| NOMBRE DE LA ENTIDAD | FECHA DE SOLICITUD | CATEGORÍA DEL SERVICIO | NOMBRE DEL SERVICIO | CLASE DE INCIDENTE |
|  |  |  |  |  |
| TIPO DE INCIDENTE | IMPORTANCIA | CAUSA RAIZ | DESCRIPCIÓN | SOLICITUD |
|  |  |  |  |  |
| NOMBRE RESPONSABLE ENTIDAD | CORREO RESPONSABLE ENTIDAD | TELEFONO RESPONSABLE ENTIDAD | FECHA DE RESPUESTA | EXPERTO ACOMPAÑAMIENTO |
|  |  |  |  |  |
| ACCIONES | RESPUESTA | ESTADO | NOMBRE DEL DOCUMENTO SOPORTE | RUTA EN SHAREPOINT DEL SOPORTE |