Gobernación de Casanare
NIT: 892099216-6

ANEXO
ESPECIFICACIONES TÉCNICAS
ESTUDIO PREVIO 1810-2023

Es de gran importancia para la Gobernación de Casanare a través de la Dirección de Tecnologías de la Información y las Comunicaciones TIC, busca en el mercado productos de alta calidad, que cumplan con los requerimientos solicitados para el proceso con objeto: RENOVACION DE LICENCIAMIENTO SOFTWARE ANTIVIRUS PARA LA PROTECCION DE ESTACIONES DE TRABAJO Y SERVIDORES DE LA GOBERNACIÓN DE CASANARE, cumpliendo con las siguientes especificaciones técnicas:

Generalidades del licenciamiento de la solución de ciberseguridad para la Gobernación de Casanare

La renovación del licenciamiento debe soportar la solución ***Kaspersky Endpoint Security*** con enfoque en la nube en su ***versión Cloud*** bajo la modalidad de software como servicio (SaaS) requiriendo que cumpla con lo siguiente:

Se requieren licencias de una solución de ciberseguridad que ofrezcan protección a estaciones de trabajo, dispositivos móviles y servidores de archivos contra todo tipo de virus, troyanos y gusanos, entre otros, previniendo infecciones y manteniendo la información segura y completamente accesible a los usuarios de los recursos de la red.

Se requiere que la administración de esta solución este centralizada y con alojamiento en la nube, para lograr una gestión enfocada a la reducción de la indisponibilidad y a la extensión directa de los controles sobre las estaciones de trabajo que estén por fuera de la red interna, con el ánimo de extender las políticas de seguridad de la Gobernación de Casanare en los diferentes entornos en que se trabaje el equipo de cómputo.

El producto debe haber sido diseñado especialmente para responder a las crecientes demandas de optimización de recursos de los servidores.

Entre los aspectos más destacables el producto debe contemplar:

Características de Seguridad

- **Protección contra amenazas web, de archivos y de correo**
  Protección para estaciones de trabajo windows contra amenazas de programa maligno conocidas, desconocidas y avanzadas, motor antimalware.

- **Prevención contra ransomware y exploits**
  Motor de corrección que revierta las acciones llevadas a cabo por el malware en el sistema operativo, buen nivel de protección contra cryptolockers.

- **Firewall**
  Protección para computadoras contra amenazas de red cuando navegue por Internet o utilice una red local.

- **Bloqueador de ataques de red**
  Protección para computadoras contra amenazas de red cuando exista navegación por Internet o utilice una red local.

- **Análisis de vulnerabilidades**
  Consulta de parches disponibles para actualizar las aplicaciones a las versiones más recientes

- **Protección de dispositivos móviles**
  Protección para dispositivos Android y iOS.

- **Cloud Discovery**
  Supervisión del uso no controlado de servicios de nube, tiempo de uso en aplicaciones.

- **Control Adaptativo de anomalías**
  Determinar la incidencia de alguna amenaza a partir del comportamiento de las aplicaciones en conjunto con el usuario.

- **Prevención BadUSB**
  Prevención activa contra la vulnerabilidad existente en firmware de los dispositivos USB.

Características Administración y Gestión

- **Cloud Blocking**
  Bloqueo de acceso de usuarios a recursos de nube, redes sociales o aplicaciones de mensajería inapropiadas o no autorizadas.

- **Seguridad para Microsoft Office 365**
  Protección integral contra amenazas para los servicios de comunicación y colaboración de Microsoft Office 365. (Protección Proactiva en pro de mitigar los ataques de phishing a través de spam)

- **Control web**

Control de acceso de usuarios a recursos de Internet según el contenido o la ubicación del sitio.

- **Control de dispositivos**
  Administre el acceso de usuarios a dispositivos externos y extraíbles conectados a una computadora.

- **Administración del cifrado**
  Cifrado de dispositivos mediante BitLocker o FileVault para proteger los datos empresariales en caso de robo o pérdida de dispositivos

- **Administración de parches**
  Automatización del proceso de instalación de parches para que siempre tenga las versiones más recientes de las aplicaciones.

- **Control de Aplicaciones**
  Control de uso de aplicaciones aun sobre los servidores basado en el hallazgo de coincidencias en ruta, hash, nombre o extensión del archivo.

- **Borrado Remoto**
  La solución debe tener un módulo que permita el envío de comando para el borrado remoto de perfiles en caso de robo o pérdida del dispositivo.

Características de Investigación y Respuesta

- **Análisis de Causa Raíz**
  Facilitador de la analítica de incidencias y/o eventualidades sujetas al proceso de gestión de incidentes en sus diferentes etapas.

- **EDR (IoCScan)**
  Control de ciberseguridad que provee visibilidad de amenazas, investigación practica y respuesta automática frente a cualquier detección. Facilita la analítica de causas inmediatas con enfoque en el descubrimiento del análisis de causa raíz, detección de amenazas, respuesta ante amenazas, análisis con indicadores de compromiso, aislamiento de equipos, tarjeta de incidentes.

- **CITO Entrenamiento**
  Portal de entrenamiento como facilitador de entendimiento a los diversos temas que rodean las actividades de orden defensivo y la gestión de incidentes.

Gobernación de Casanare
NIT:892099216-6

ANEXO
ESPECIFICACIONES TÉCNICAS
ESTUDIO PREVIO 1810-2023

La administración departamental en la actualidad cuenta con una solución de seguridad perimetral (**UTM**) basada en políticas que enfocan una protección a nivel de red y es de suma importancia que articulen con la configuración de las directivas de la solución de seguridad de las estaciones de trabajo implementadas a través de los módulos de antivirus, control web, firewall de host, control de dispositivos, control de inicio y registro de aplicaciones & HIPS, entre otras, en aras de establecer una doble protección en tráfico de reglas de negocio (interVLAN), Navegación (Filtrado de Contenido).

Por lo anterior es obligatorio que las políticas del **UTM** articulen con la configuración de las directivas implementadas en la solución antivirus, haciendo necesario en el momento de la activación de las licencias, contar con el soporte de dos (2) profesionales en ingeniería de sistemas o carreras afines, con experiencia y certificados en configuración de soluciones de seguridad a nivel de redes y host en la marcas Fortinet y Kaspersky; uno de ellos debe contar con certificado en **NSE4**, superior o equivalente, además de contar con una certificación **KL302** de *Kaspersky Lab*.

El canal que distribuya el licenciamiento debe tener autorización para comercializar la solución ofertada y certificación de distribución.

KATHERINE LIESEL HEREDIA HERNANDEZ
DIRECCIÓN DE TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES TIC

Elaboró: Carlos Arturo Carmona, Profesional de Apoyo CTO N° 0767-2023