I. RESPONSABLE DE LA EVALUACION:

ANALISTA DE SISTEMAS

II. FECHA

01 de Julio del 2019

III. JUSTIFICACION

En la actualidad los delitos informáticos se viene realizando, usando técnicas cada vez más sofisticadas para vulnerar las redes empresariales desplegando sus ataques haciendo uso de Software Maliciosos o Malware (virus, gusanos, troyanos, Spyware, Adware, ramsonware) y/o aplicaciones potencialmente peligrosas dentro de los mensajes de correo y sitios Web.

Así mismo con el creciente incremento de mensajes de correo no deseados y la necesidad de mejorar el control del uso de los recursos informáticos y de red, la ZONA ESPECIAL DE DESARROLLO ILO requiere adquirir un producto antivirus que permita brindar seguridad y control, para lo cual se *establecerá los atributos o características mínimas para la adquisición de dicha solución.*

IV. ALTERNATIVAS

Para la selección de los productos antivirus a analizar se ha tomado de manera muy referencia los productos más conocidos en el mercado, con la salvedad de haber encontrado diferencias sustanciales en las publicaciones, las que presumimos puede deberse a temas netamente comerciales.

ZED ILO ANALISTA DE SISTEMAS

Los productos analizados son:

- **Eset Endpoint Security Advanced**
- **Seqrite Endpoint Security Advanced**
- **Kaspersky Endpoint Security For Business Advanced**

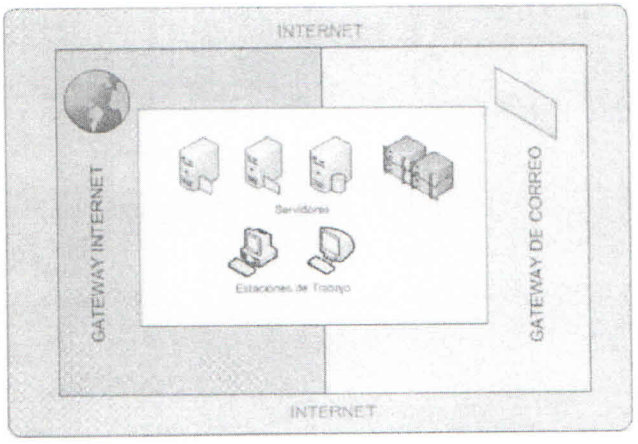
V. ANALISIS COMPARATIVO TECNICO

Se realizó aplicando la parte 3 de la Guía de evaluación de Software:

a. **Propósito de la Evaluación:**

Determinar los atributos o características mínimas para el Producto Final del Software Antivirus. El producto deberá proteger y controlar la seguridad en los siguientes niveles:

1) Estaciones de trabajo y servidores de red
2) En el perímetro de Internet
   a. Protocolo correo (SMTP)
   b. Protocolo de Internet. (HTTP / HTTPS / FTP)



b. Identificar el tipo del producto

ZED ILO ANALISTA DE SISTEMAS

Software de Seguridad Integrada para la protección multi-amenazas.

- Anti-virus.
- Anti-spyware.
- Anti-adware and PUAs(Aplicaciones potencialmente no deseadas adware, dialers, herramientas de Adm.remota y herramientas de hacking).
- Control de aplicaciones.
- Detección de intrusos de host - HIPS.
- Cliente firewall.
- Anti-spam
- Anti-phishing.
- Control del contenido de correo.
- Bloqueo de sitios Web maliciosos.
- Filtrado de productividad Web.

c. **Especificación del Modelo de Calidad.**

Se aplicará el Modelo de Calidad de Software descrito en la Parte I de la Guía de Evaluación de Software aprobado por Resolución Ministerial N° 139-2004-PCM.

d. **Identificación de Métricas.**

Las métricas fueron seleccionadas en base al análisis **de la información técnica de los** productos antivirus señalados en el punto "Alternativas", Como son las características del Producto y Requerimiento de instalación.

Del análisis realizado se ha determinado las siguientes características técnicas mínimas.

ATRIBUTOS INTERNOS		
ITEM	**ATRIBUTO**	**DESCRIPCION**
1	**Sistemas Operativos Estaciones de Trabajo**	Windows XP/Vista / 7 / 10 de 32/64 bit **La solución deberá soportar las versiones de 32 y 64 bits.**
2	**Sistemas Operativos de Servidores**	Microsoft® Windows Server 2003 Microsoft® Windows Server 2003 R2 Microsoft® Windows Server 2012 Microsoft® Windows Server 2012 Essentials **La solución deberá soportar las versiones de 32 y 64 bits.**
3	**ACTUALIZACIONES**	• Deben ser manuales y automáticas (programadas) del repositorio de datos de los equipos designado y que estos se actualicen desde la red de internet para la distribución de políticas. • Los equipos deben de tomar las actualizaciones desde solo desde los equipos asignados como repositorio. • El tamaño de las actualizaciones debe ser pequeño.
4	**PROTECCIÓN PROACTIVA**	• La solución debe contar con una tecnología de detección proactiva de amenazas conocidas y desconocidas que detecte malware "antes de su ejecución (pre- execution)" y "en ejecución (on-execution)". • La solución debe incluir también una tecnología de detección de intrusos de host (HIPS) que brinde protección en acceso embebido en el producto. No debe requerir ejecutar agentes adicionales ni ejecutarse en forma programada.
5	**CONTROL Y PRODUCTIVIDAD EN LA RED**	• La solución debe contar con un sistema que permita el control de aplicaciones tanto instaladas y portables. • El sistema debe permitir controlar y bloquear el uso de aplicaciones que causan un impacto negativo a la productividad de los usuarios y el uso del ancho de banda en la red tales como: – Programas de mensajería (MSN, Yahoo Messenger, Google Talk, páginas sociales y otros.). – Programas de voz sobre ip (MSN, Skype, Google Talk) – Programas Peer-to-Peer (Kazaa, Imesh, Ares, etc). – Juegos en red y stand-alone, La solución debe permitir desinstalar remotamente las principales aplicaciones Peer-to-peer desde la Consola de Administración. • Herramientas de Control Remoto de Equipos (Logmein, Netcat, etc)

ZED ILO ANALISTA DE SISTEMAS

6	CONTROL DE DISPOSITIVOS	Puede bloquear el acceso a dispositivos con reglas predefinidas, a la vez el producto tiene que ser capaz de ser agregado a más dispositivos. • Dispositivos de almacenamiento masivo USB, Dispositivos inalámbricos, Unidades de DVD/CD-ROM, Dispositivos Windows CE ActiveSync. • Discos, Módems • Puertos COM y LPT (no controla el dispositivo, sino el puerto) • Impresoras • Lectores de tarjetas inteligentes • Dispositivos de generación de imágenes (cámaras y escáneres) • Controladores de host de bus IEEE 1394 • Dispositivos IrDA y Bluetooth
7	COMPATIBILIDAD	Carta del fabricante del software antivirus certificara la total compatibilidad con los sistemas operativos en las versiones anteriores mencionadas. La solución debe permitir instalarse remotamente desde la consola de administración remota a todos los equipos, mediante el envío de 1 solo agente que contenga todos los módulos de protección de la solución.
8	INSTALACIÓN	El instalador con todos los módulos incluidos debe de pesar por lo máximo 100 mb para las estaciones de trabajo la mejor performance al momento de realizar el despliegue dentro de la organización La instalación del Antivirus a las computadoras de los usuarios debe tener las siguientes facilidades: - Sincronización con el Directorio Activo de Microsoft - Desde la consola de administración - Instalación mediante CD o recurso UNC - Instalación desde la página Web, con seguridad de acceso (usuario y clave), para equipos fuera de la LAN.

ATRIBUTOS EXTERNOS

ITEM	ATRIBUTO	DESCRIPCION
9	CONSOLA DE ADMINISTRACIÓN	La herramienta debe contar con una Consola de Administración desde donde se pueda Administrar y controlar la solución antivirus y el cliente Firewall en forma remota. • La consola debe encontrarse en la nube para mejor desempeño de los servidores. • Permitir la administración simultánea de equipos y servidores. • La herramienta deberá ser escalable, administración de complejas redes, permitiendo la administración de más de 50 equipos desde una sola consola. • La consola debe sincronizarse con el Directorio Activo para la instalación automática de la solución de seguridad en los equipos. • La frecuencia de actualización de firmas de virus debe ser cada 05 minutos o menos. • La administración deberá estar basada en Políticas y debe contener al menos políticas para Actualización, Antivirus, Control de Aplicaciones, Control de Dispositivos, Control Web, Antispyware y Firewall por reglas y por servicios. • Debe contar con filtros de control que permitan detectar de

ZED ILO ANALISTA DE SISTEMAS

		forma rápida los equipos no protegidos o los que no cumplen con las políticas de seguridad. • El administrador debe poder crear políticas desde la consola para evitar el uso de aplicaciones no deseadas así como eliminar, autorizar y limpiar las mismas en los clientes. • Debe incluir la capacidad para la desinfección y limpieza remota de Adware/aplicaciones potencialmente peligrosas, así como también de virus, troyanos, gusanos y Spyware. • La consola debe poder utilizar al menos 3 tipos diferentes de mecanismos para detectar equipos en la red (TCP/IP, Active Directory y otros). • Se debe poder crear políticas de actualización para equipos con conexión lenta pudiendo limitarse el ancho de banda utilizado durante las actualizaciones. • Desde la consola se debe administrar en cada uno de los clientes y/o grupos, la actualización de los clientes, en su versión de antivirus, actualización de los archivos, servicios de definición y/o firmas de virus, motor de búsqueda, parches de terceros y actualizaciones extraordinarias. • La consola de administración debe informar un estado actual de la solución por producto (Protección de estaciones, de servidores, de correo, etc. • La comunicación entre el agente y el servidor de la consola de administración debe ser bidireccional y por eventos; es decir, la comunicación se debe realizar sólo cuando la consola tenga una actualización para entregar, o cuando el equipo tenga una novedad que reportar (ataque, etc.), con el fin de evitar los broadcast no necesarios en la red. • La solución debe contar con mecanismos para la notificación en caso de presentarse un ataque de virus o código malicioso, estas notificaciones podrán ser enviadas al remitente, al receptor y al administrador. • Los reportes ofrecen información como virus presentes en la red, acciones tomadas, usuarios atacados, usuarios infectados, reporte de violaciones de seguridad, análisis de puntos de entrada, estadísticas de estado de actualización de los patrones, Top 10; etc. • La consola debe permitir crear usuarios administradores, por grupos de equipos y con privilegios totales de administración o de solo consulta • La consola de administración debe permitir realizar escaneos simultáneos, programados o manuales a todos los equipos de la red, por grupos, o de manera individual, cómo sea requerido por el administrador. • El producto debe permitir la instalación y desinstalación remota de los servidores y clientes antivirus. • El producto debe ser capaz de crear un paquete de instalación consolidado (archivo ejecutable) que pueda ser accedido por correo o por web, para la instalación de los antivirus o del agente. • La consola debe de tener una vista avanzada para lograr establecer políticas más personalizadas. • La consola debe ser capaz de determinar equipos que cumplen con las políticas remotas y/o que fueron modificadas localmente.

ZED ILO ANALISTA DE SISTEMAS

		• Eventualmente deberá poder "forzar" a los equipos a cumplir con las políticas remotas con tan solo un clic. • La consola deberá contar con un sistema de reportes y mecanismos de notificación de eventos vía correo electrónico y web. • Deberá almacenar un histórico de eventos de cada equipo administrado pudiéndose conocer también el Nombre del Equipo, Descripción, SO, Service Pack, IP, Grupo, Última Actualización, Eventos de error, etc. desde la consola.
10	**Defensa Integrada contra malware (Virus, Troyanos, Macro Virus, Virus Gusano, Spyware, Adware, Virus en Archivos comprimidos, PUAS (Aplica-ciones Potencial-mente Peligro-sas).**	• La solución de seguridad para estaciones y servidores debe ser de tipo Integrada; es decir debe incluir un único agente que brinde protección frente a virus, Spyware, Adware, comportamientos sospechosos, hackers (firewall por reglas y servicios) y aplicaciones potencialmente peligrosas en todos los protocolos de la red. • Debe contar con la capacidad de integración con las políticas de seguridad de Cisco NAC y deberá incluir un Firewall del mismo fabricante. • El firewall debe ser administrado remotamente por Reglas y por servicios. • Debe poder bloquear y autorizar aplicaciones y puertos específicos tanto local como remotamente. • El firewall debe poder trabajar en modo oculto. • La solución debe tener versiones para Linux el cual debe contar con un módulo de escaneo de archivos de máximo rendimiento, estabilidad y eficacia el cual debe permitir el escaneado en acceso, en demanda y programado de unidades locales, extraíbles y compartidas (como NFS y Samba), y otros sistemas de archivos. La versión para Linux debe poder ser configurado y administrado desde la consola remota. • La configuración del cliente para Linux debe poder realizarse desde la línea de comandos y mediante una interfaz Web en forma local y debe contar con al menos una certificación tipo RedHat Ready o Novel Suse Linux. • La solución debe contar con una Cuarentena de usuario final que permita controlar y/o autorizar el uso de ciertas aplicaciones no deseadas. • La solución tanto para Windows, Linux deberá notificar los eventos de virus, Spyware, Adware, aplicaciones no deseadas, intrusiones, cambios en la configuración del cliente antivirus y/o cliente firewall a la consola remota. • La solución debe poder actualizarse desde una consola remota y desde la Web del fabricante simultáneamente con el fin de asegurar una completa protección aun cuando la consola remotas no se encuentre activa.
11	**Defensa en el Perímetro de la Red (HIPS/IDS/IPS)**	• Se requiere una solución del mismo fabricante que brinde Seguridad y Control de la información entrante y saliente de la red vía los protocolos SMTP, HTTP y FTP. • La solución deberá rastrear, limpiar y eliminar Virus, Adware, y Spyware y aplicaciones potencialmente peligrosas en dichos protocolos. **Protocolo SMTP** • Deberá tener la capacidad de configurar como Replay del correo electrónico.

ZED ILO ANALISTA DE SISTEMAS

		• Deberá integrarse con el protocolo LDAP y Directorio Activo para la autenticación de usuarios y creación de políticas. • Deberá incluir un filtro Anti Spam del mismo fabricante que soporte descargas automáticas de políticas Anti spam. • Deberá incluir varias técnicas de detección, como reputación de IP, heurística avanzada, huellas de mensajes y adjuntos, análisis de palabras clave, detección de direcciones Web, etc. • El producto debe tener una efectividad de detección de SPAM fuera de caja de un mínimo del 95%. • Deberá entregarse información del fabricante para certificar esta funcionalidad. • Deberá ofrecer una tecnología que permita el acceso en tiempo real a una amplia gama de información reciente contra spam. • Deberá detectar ataques de robo de información (phishing), ataques de denegación de servicio (DoS) y cosecha de información (Harvest). • Deberá contar con un módulo específico para el Filtrado por Reputación que permite el bloqueo por IP's de servidores dudosos y permitir elaborar excepciones tanto a nivel MTA como a nivel de políticas de correo. Esta lista deberá residir en el servidor y deberá ser actualizado en promedio cada 10 minutos y en forma incremental. • Deberá de poder detectar, eliminar y limpiar virus y Spyware en los archivos adjuntos al correo electrónico y en el cuerpo del mensaje y deberá ser del mismo fabricante. • Deberá de realizar el bloqueo de archivos adjuntos según el tipo de archivo y no de la extensión. • Deberá de realizar el bloqueo de correos por asuntos, destinatario o texto en el cuerpo del mensaje. • Deberá contar con un Editor de Políticas para filtrar el contenido del tráfico entrante y saliente. • Deberá de poder hacer reglas de filtrado por usuario. • Deberá de poder hacer creaciones de lista de aceptación y negación (blanca y negra) de dominios y usuarios (cuentas de correo) confiables. • Deberá de enviar notificaciones configurables al emisor, receptor y al administrador sobre mensajes electrónicos infectados y/o bloqueados. • Deberá contar con un sistema de Administración vía Web Seguro (HTTPS). • Debe permitir crear usuarios para la administración basada en roles para delegar ciertas funcionalidades de administración. El acceso a la interfaz de administración basada en roles debe ser vía Web seguro y debe funcionar en un puerto distinto al del Administrador principal. • Deberá contar con un administrador de cuarentena remota a nivel de consola. • Deberá contar con un administrador de la cuarentena por usuario que permita a su vez administrar la lista blanca y negra de cada usuario. • Debe poder desactivarse ciertas opciones a las cuales no se desea que los usuarios tengan acceso. • Deberá contar con un sistema automático que permita realizar el backup de la cuarentena. Esta opción es configurable desde la

ZED ILO
ANALISTA DE SISTEMAS

		herramienta de gestión del producto. • Deberá generar un mensaje donde les informe a los usuarios finales los mensajes de correo puestos en cuarentena y que estos puedan recuperar todos o individualmente tan sólo con un solo clic. • La herramienta debe contar con un sistema de actualización de cada parte de los componentes del producto incorporado en la herramienta de administración web.
12	GATEWAY WEB	**Protocolo HTTP/FTP** • El producto debe permitir bloquear programas espía (Spyware), virus, pesca de información (Phishing), programas maliciosos y aplicaciones no deseadas (Adware, PUAS) en la puerta de enlace, y permitir un control completo del acceso a Internet para una navegación segura y productiva. • Deberá ofrecer la inspección de tráfico de doble dirección (entrante y saliente) de códigos maliciosos, programas no deseados y el cumplimiento de políticas de uso de Internet. • Deberá proveer un filtro de contenido (URL Filtering) del mismo fabricante y deberá estar basado en categorías. • Deberá contar con al menos con cincuenta (50) tipos de categorías organizados de acuerdo al contenido de cada sitio Web. • Deberá contar con una interfaz de administración Web Segura (HTTPS). • Deberá garantizar una adecuada detección con bajo impacto en la red y mínima latencia. El postor debe presentar una copia de la información pública y oficial del producto que permita certificar esta característica (Brochures y/o Impresión de Página Web oficial). • Deberá contar con un sistema de administración basado en grupos con indicadores visuales y reportes en línea. • Deberá incluir un Proxy interno que permita ocultar la dirección IP del equipo donde esté implementado la solución. • Deberá recibir actualizaciones automáticas de las firmas de virus, filtrado de contenido (URL) como mínimo cada 15 minutos. • Deberá permitir crear políticas de uso de Internet por grupos de usuarios, por hora o por días. • Deberá permitir controlar la descarga de aplicaciones potencialmente peligrosas incluyendo dialers, herramientas de administración remota y aplicaciones de monitoreo de Pc's y archivos de Streaming (música, videos). • Deberá permitir la integración con el Directorio Activo de Microsoft para la generación de políticas de seguridad y control del producto. • Deberá contar con un sistema de reportes que contenga 10 o más reportes y que permita conocer: - Usuarios que intentaron descargar virus. - Usuarios que intentaron visitar sitios de alto riesgo. - Usuario que intentaron descargar aplicaciones potencialmente peligrosas. - Los principales usuarios que intentaron violar las políticas de seguridad y control de la entidad.

ZED ILO
ANALISTA
DE SISTEMAS

13	**ESCANEO**	• Permitir configurar la detección sobre todos los archivos, o tipos de archivos, comprimidos (cualquier formato de comprensión, rar, zip, cab, arj, arz), ocultos y archivos en ejecución. • Deberá realizar los siguientes tipos de rastreo; en tiempo real, bajo demanda, programado y remoto a través de la consola de administración. • Para el escaneado en el Gateway de correo y Web el producto cuenta con un escáner de una vía que permita detectar malware y realizar el filtrado URL en una sola pasada. • Protección de correo Webmail y mensajería instantánea • Información en detalle del Virus o elemento no deseado encontrado
14	**PRODUCTIVIDAD**	No deberá consumir muchos recursos de memoria y procesador en los equipos de los usuarios.
15	**ALERTAS Y REPORTES**	• La consola de administración deberá de ser capaz de notificar los eventos de virus a través de diferentes medios (correo electrónico, alertas de registros, etc.). • Además generar reportes gráficos de tipo barra, pastel, imprimibles y exportables de la cobertura de versiones, actualizaciones e infecciones. • Deberá contar con un Panel de Control donde se visualice en línea y en forma automática el estado de la seguridad de la red. • Deberá contar con un Panel de Control donde se visualice en línea y en forma automática el número de equipos sin protección, protegidos, con errores, que no cumplen con las políticas corporativas.
16	**FACILIDAD DE USO**	Toda la solución deberá incluir capacitación a usuarios para el uso más fácil y rápido.
17	**SOPORTE AL USUARIO**	• Debe contar con soporte técnico 24/7 escalable hacia la casa matriz incluido en la licencia y en español. El postor deberá presentar un documento del fabricante donde certifique que cuenta con este tipo de soporte. • Si para el escalamiento se requiere de un código especial para el soporte desde la casa matriz el postor deberá especificarlo mediante una declaración jurada comprometiéndose a brindar dicho código el cual deberá ser emitido a nombre de ZED ILO al momento de la firma del contrato.
18	**EFICACIA**	Deberá ser capaz de permitir a la Oficina de Informatica de ZED ILO, lograr las metas específicas con exactitud e integridad, de acuerdo a las especificaciones técnicas y requerimiento.

ZED ILO
ANALISTA DE SISTEMAS

e. **Niveles, escalas para métricas:**

ITEM	ATRIBUTO INTERNOS	Puntaje
1	Sistemas Operativos / Estaciones de Trabajo	10
2	Sistemas Operativos / Servidores de Red	10
3	Actualizaciones	10
4	Protección Proactiva	10
5	Control y Productividad en la Red	10
6	Compatibilidad	10
7	Instalación	10
8	Certificaciones	10
ITEM	**ATRIBUTOS EXTERNOS**	
9	Consola de Administración	10
10	Defensa Integrada contra malware	10
11	Defensa en el Perímetro de la Red	40
12	Escaneo	10
ITEM	**ATRIBUTOS DE USO**	
13	Productividad	10
14	Alertas y Reportes	10
15	Facilidad de Uso	10
16	Soporte al Usuario	10
17	Eficacia	10
	TOTAL	**200**

ZED ILO
ANALISTA DE SISTEMAS

No se ha comparado los productos de software antivirus, porque el objetivo es establecer características técnicas mínimas de software antivirus, que sirvan para una posterior comparación y evaluación.

VI. ANALISIS COMPARATIVO TECNICO.

En el siguiente cuadro comparativo se puede apreciar las ventajas de los productos software que fueron analizados técnicamente.

ITEM	ATRIBUTO INTERNOS	Puntaje	Seqrite	Kaspers.	Nod Eset
1	Sistemas Operativos / Estaciones de Trabajo	10	10	10	10
2	Sistemas Operativos / Servidores de Red	10	10	10	10
3	Actualizaciones	10	10	10	10
4	Protección Proactiva	10	10	8	8
5	Control y Productividad en la Red	10	10	8	9
6	Compatibilidad	10	10	10	10
7	Instalación	10	10	10	10
8	Certificaciones	10	10	8	10
ITEM	ATRIBUTOS EXTERNOS				
9	Consola de Administración	10	10	10	10
10	Defensa Integrada contra malware	10	10	10	10
11	Defensa en el Perímetro de la Red	40	40	39	36
12	Escaneo	10	9	8	10
ITEM	ATRIBUTOS EN USO				
13	Productividad	10	10	10	10
14	Alertas y Reportes	10	10	10	10
15	Facilidad de Uso	10	9	10	9
16	Soporte al Usuario	10	10	10	9
17	Eficacia	10	10	10	9
	TOTAL	**200**	**198**	**191**	**190**

ZED ILO
ANALISTA DE SISTEMAS

Con la finalidad de comprobar lo que las publicaciones especializadas indicaban sobre el grado de cumplimiento de las funcionalidades y atributos de los productos, se procedió a analizar los productos.

Factores Evaluados (Pruebas Plito)	Seqrite	Kaspers.	Nod Eset
Instalación y Configuración en Servidor	10	10	9
Políticas y Gestión de Control	10	9	9
Protección de Datos	10	9	9
Performance en los equipos instalados	9	9	9
Soporte Técnico	10	9	9
Verificación de Control de Dispositivos	10	9	9
Verificación de Control de Aplicaciones (Web)	9	9	9
Procesos de Interiorización y Conocimiento	9	10	9
Totales	**77**	**74**	**72**

VII. ANALISIS COMPARTIVO – COSTO BENEFICIO

El Análisis Costo - Beneficio tiene como referencia la cantidad de licencias de software antivirus posibles de adquirir, tal como se puede apreciar en el siguiente cuadro:

ITEM	PROGRAMA	TIEMPO	PRECIO
1	RENOVACION ESET	36 MESES	S/ 2,444.00
2	SEQRITE SECURITY TOTAL EDITION	36 MESES	S/ 2,435.28
3	KASPERSKY	36 MESES	S/ 2,700.00

VIII. CONCLUSIONES.

1. Se determinó los atributos o características técnicas mínimas que deben ser considerados para una evaluación de software, asimismo se estableció la valoración cuantitativa de cada característica y los resultados obtenidos en dicho análisis determinan que el mayor puntaje es para el software SEQRITE.
2. De acuerdo al análisis costo beneficio la solución SEQRITE es de menor costo.
3. Por lo anteriormente expuesto propongo la adquisición de 22 licencias del software SEQRITE.

ZED ILO ANALISTA DE SISTEMAS

Ing. Aura Olaya Cruz
Analista de Sistemas

Ilo, 01 de Julio del 2019