J	Protección para servidores ambiente Linux.
K	Detecta amenazas complejas Aislamiento del host Iniciar un escaneo del host Eliminación de archivos (Eliminación de procesos Impedir que el proceso se ejecute)
L	Evaluación y Gestión de Vulnerabilidades Inventario y Control de Licencias Distribución Software Implementación Sistema Operativo Integración con SEM Cifrado de Datos Seguridad Móvil Gestión de Dispositivos Móviles (MDM) Gestión de Aplicaciones Móviles (MAM) Seguridad para servidoras Control de aplicaciones Control de dispositivos Control WEB Anti-Malware + Firewall
M	**Servicios de actualización:** Actualización del servidor de administración Kaspersky Security Center a la nueva versión. Instalación y configuración Servidor de Administración Kaspersky Security Center Cloud Instalación en las estaciones de trabajo físicas del módulo de protección EDR Optimum. Instalación componente de seguridad EDR Optimum en los servidores y estaciones virtuales. Creación en el servidor de administración Kaspersky Security Center de directivas de seguridad integradas con el módulo EDR Optimum. Configuración de respuestas automáticas de amenazas detectadas. Creación de directivas de seguridad integradas con el módulo EDR Optimum en el servidor de administración Kaspersky Security Center. Configuración de respuestas automáticas ante amenazas detectadas. Configuración de tareas de Análisis de indicadores de compromiso (IoC). Con base en amenazas descubiertas Configuración de consola, herramienta de inventario, herramienta de cifrado, tareas de escaneo de acuerdo a lo solicitado y capacitación sobre estas herramientas al personal de soporte de la oficina de informática. Configuración de protección automática de exploits e inteligencia de seguridad en la nube mediante la activación y configuración del KSN. Creación de los paquetes de instalación para los servidores y estaciones virtuales. Instalación de las licencias de los servidores y estaciones de trabajo .Configuración Servidor de administración de servidores y estaciones Creación de directivas, tareas de actualización y análisis en los servidores y estaciones virtuales. Configurar sistema de prevención e intrusiones HIPS, junto con el system watcher y el firewall para asegurar y proteger las actividades de las aplicaciones en la red. Creación de plantilla de control de aplicaciones con listas blancas y dinámicas que permitan permitir y bloquear la ejecución de las aplicaciones en ambientes controlados. Configuración de reglas de control de acceso de dispositivos de forma granular de conexión de los dispositivos de almacenamiento extraíbles al igual que los periféricos, definiendo derechos de usuario para las operaciones de lectura y escritura. Configuración de aplicación de parches de seguridad y actualización de vulnerabilidades desde la consola de administración. Creación de paquetes de distribución y actualización del sistema operativo.