ANEXO TÉCNICO

Renovar la suscripción del licenciamiento de las herramientas DLP, incluyendo soporte técnico, mantenimiento y actualización.

Septiembre 2026

OBJETO A CONTRATAR

Renovar la suscripción del licenciamiento de las herramientas DLP, incluyendo soporte técnico, mantenimiento y actualización.

ESPECIFICACIONES TÉCNICAS MÍNIMAS A CONTRATAR

Licenciamientos requeridos por un año: 500 licencias de una herramienta de Prevención en la pérdida de Datos (DLP) para usuarios por un (1) año, las cuales podrán ser usadas en los diferentes sistemas operativos como: Windows 10 y superior y Mac OS X.

- DESCRIPCIÓN: Adquisición de 500 licencias por un año de la solución DLP (Prevención en pérdida de datos) que incluye: Suscripción para 500 endpoints, incluyendo consola nativa cloud y soporte de fabricante.

Características Técnicas: La herramienta **DLP** debe contemplar los siguientes requerimientos como mínimo:

DLP (Data loss prevention)	
El Instituto Colombiano para la Evaluación de la Educación (ICFES) requiere del licenciamiento de la solución DLP para 500 dispositivos.	
Funciones básicas	**La solución de DLP debe tener mínimo las siguientes funcionalidades:**
	Especificar Marca:
	Especificar Modelo y/o referencia:
	Se requiere una solución DLP (Data Loss Prevention) que permita a la entidad a anticipar y prevenir la perdida de datos.
	La solución debe estar licenciada para 500 Endpoints por un periodo de 12 meses a partir de su activación en el portal del fabricante de la solución ofertada.
	La solución debe proporcionar amplios flujos de eventos de actividad de usuarios, datos y archivos
	La solución debe ser SaaS en su consola, no se aceptan soluciones en máquina virtual o físicas.
Requerimientos técnicos	La solución debe prevenir la exfiltración y pérdida accidental de datos.
	La solución debe proporcionar visibilidad inmediata sobre el movimiento y la actividad de los datos.
	La solución debe proporcionar visibilidad inmediata sin políticas sobre el movimiento de datos y los procesos empresariales.
	La solución debe aplicar políticas de riesgo interno con acciones de seguridad proactivas en tiempo real.
	La solución debe asegurar los datos en uso por aplicaciones SaaS y otras aplicaciones.
	La solución debe proporcionar visibilidad integral de las interacciones de los usuarios con los datos en la nube y mantener la protección a medida que los datos se mueven fuera de la nube, asegurando la protección continua de la información sensible, independientemente de su ubicación o método de acceso.
	La solución debe fortalecer las defensas contra posibles brechas de datos derivadas de la exposición de datos empresariales a través del uso no autorizado de aplicaciones, incentivando a los empleados a usar herramientas autorizadas.
	La solución debe identificar el uso de Shadow AI y detener la carga de datos sensibles.
	La solución debe monitorear el uso de aplicaciones SaaS, incluyendo herramientas de Shadow AI como Gen-AI, e incorporar educación de usuarios basada en riesgos en el punto de acceso a datos sensibles.
	La solución debe construir un inventario completo con puntuación de riesgo de las aplicaciones SaaS y herramientas GenAI utilizadas en toda la organización, con información sobre el ingreso, egreso y credenciales de datos.
	La solución debe estar disponible en la nube para facilitar su implementación y escalabilidad.
	La solución debe funcionar independientemente de la conexión de red y la ubicación.
	La solución debe utilizar tecnología de agente ligero compatible con sistemas operativos Windows, macOS y Linux para una implementación sin problemas y actualizaciones automáticas a escala empresarial.
	La solución debe permitir reducir los costos de ancho de banda, al no depender de un motor de escaneo de archivos basado en la nube.
	La solución debe proporcionar un agente unificado que consolide todas las funcionalidades de monitoreo y bloqueo.

	La solución debe utilizar agentes, extensiones de navegador y conectores en la nube para recopilar, enriquecer e indexar automáticamente la actividad a través de diferentes tipos de eventos (autenticación, web, email, aplicaciones, USB, creación de archivos, compartición y descarga de archivos).
	La solución debe integrarse fácilmente con los sistemas y plataformas existentes en la organización.
	La solución debe monitorear y bloquear datos sensibles transferidos a través de navegadores web a dominios públicos externos (por ejemplo, Gmail, Yahoo, Hotmail).
	La solución debe proporcionar visibilidad de datos, evaluación de riesgos y políticas de protección de datos listas para usar para proteger los activos de información críticos dentro y fuera de la red.
	La solución debe ayudar a cumplir con requisitos clave de cumplimiento, incluyendo PCI DSS, HIPAA, ISO 27001, NIST, entre otros.
	La solución debe abordar los controles de cumplimiento normativo relacionados con la prevención de pérdida de datos con un esfuerzo mínimo utilizando políticas predefinidas de PII/PHI/PCI.
	La solución debe priorizar la privacidad bajo regulaciones como GDPR y CCPA.
	La solución debe proporcionar un feed de actividad detallado y secuenciado en el tiempo que permita a los analistas ver la actividad de usuarios, datos y dispositivos antes, durante y después de un incidente.
	La solución debe proporcionar un dashboard para cumplimiento y auditoría.
	Los reportes deben poder exportarse fácilmente para compartir con otras áreas de la entidad.
	La solución debe monitorear y bloquear datos sensibles transferidos a dispositivos USB.
	La solución debe monitorear datos sensibles copiados a nivel de archivo/carpeta.
	La solución debe exportar un historial de todo el movimiento de datos dentro de la empresa, incluyendo datos provenientes de fuentes externas.
	La solución debe monitorear la descarga de datos sensibles por un usuario directamente desde una aplicación/servidor de aplicaciones.
	La solución debe bloquear el montaje de unidades de almacenamiento removibles (por ejemplo, USB, HDD externo).
	La solución debe integrarse de manera nativa con las herramientas perimetrales actuales de la entidad.
	La solución debe integrarse con Active Directory, Azure AD y soluciones LDAP de terceros.
Licenciamiento	Se debe incluir una asesoría y acompañamiento directo de fabrica por lo menos de 12 meses en los cuales se incluya asistencia directa en el diseño, planeación, afinamiento de la solución, seguimiento semanal durante la implementación. Estas etapas deben ser realizadas directamente por parte del fabricante. No se admite que lo realice un partner o canal.
	El periodo de licenciamiento y soporte es de 12 meses a partir de la activación de las licencias en el portal del fabricante ofertado.

La herramienta debe ser administrable a través de una consola Web Cloud nativa con asignación de roles por privilegios, con su correspondiente licencia en caso de que aplique.

NOTA: La solución se debe poder implementar en servidores físicos y/o virtuales, aclarando que el ICFES cuenta con una infraestructura para implementar la solución, la cual depende de los requerimientos de las herramientas cotizadas, se descartarán las soluciones que incluyan la adquisición de appliance o hardware para su funcionamiento.

Documentación:

- Entregar al ICFES dentro de los cinco (5) días hábiles siguientes a la firma del acta de inicio las 500 licencias (suscripciones) del DLP, con su correspondiente certificación de cantidades de usuarios o estaciones de trabajo, y la vigencia emitida por el fabricante.
- Entregar dentro de los 3 días hábiles posteriores a la firma del acta de inicio del contrato, el protocolo de soporte donde

relacione en detalle los canales de atención, el personal a cargo del contrato, los tiempos de respuesta, entre otros.

- Realizar los respectivos informes de cada una de las sesiones de soporte de la herramienta adquirida, que deben ser entregadas dentro de los tres (3) días hábiles siguientes a la realización del soporte.
- Entregar manuales técnicos, funcionales o cualquier documento asociado al uso y configuración de las herramientas una vez sea activadas las licencias y cuando exista una actualización sobre esta.
- Suscribir acuerdo de confidencialidad

Implementación y/o Afinamiento

Para la implementación se entiende como la instalación de agentes y despliegue de consola Cloud con la habilitación de nuevas funcionalidades y ajustes a la configuración del software para optimizar el rendimiento y la configuración de parámetros o políticas que conforman la solución.

El proponente deberá realizar Instalación y puesta en marcha y/o afinamiento para lo cual deberá entregar al supervisor del contrato el plan de trabajo a realizar para revisión y aprobación. El plan de trabajo deberá entregarse en un plazo no mayor a diez (10) días hábiles a partir de la suscripción del acta de inicio, de acuerdo con las actividades de afinamiento solicitadas por el ICFES y basado en un diagnóstico de la implementación actual de la solución de DLP que tiene la entidad, cual debe incluir recomendaciones de mejora si aplica, buenas prácticas para el uso de la herramienta, actividades, tiempos, objetivos a cumplir, evidencias que darán respuesta a cada actividad y plan de trabajo que se emplearán para su implementación.

El afinamiento debe contemplar actividades diferentes a la instalación y parametrización de la herramienta y debe contemplar actividades como las descritas a continuación:

- Desplegar y activar el licenciamiento adquirido por la entidad, evidenciando en el portal del fabricante las fechas de inicio y fin de la suscripción.
- Crear, validar y ajustar las reglas, políticas o reportes para determinar si son efectivas y cumplen con las necesidades del ICFES.
- Parametrización de Reportes y Módulos, siempre y cuando se encuentren dentro de la licencia de DLP.
- Pruebas de funcionamiento de las reglas.
- Revisar que los backups configurados se están generando de forma correcta.
- Verificar que no exista pérdida de información.
- Revisar el uso de las herramientas de detección, diagnóstico y resolución de novedades que ayuden a conservar la estabilidad y óptimo rendimiento de la solución; revisar el uso y configuración de las herramientas de reportes y almacenamiento de logs.
- Configuraciones de alertas y eventos masivos**.**
- Responder las inquietudes del Instituto relacionadas con afinamientos y cambios en la configuración de la solución.
- Actualización de versiones de la herramienta
- Activación de nuevas funcionalidades
- Entre otros

La puesta en marcha y/o afinamientos se podrán realizar de manera presencial o remoto según requerimientos o necesidad. En caso de que se requiera acceder de forma remota a los equipos de la solución, esto debe ser autorizado con el supervisor del contrato por parte del ICFES, con previa presentación y aprobación del plan a realizar.

A los tres (3) días hábiles de efectuada alguna actividad el afinamiento, el contratista deberá entregar el informe técnico al personal designado por el ICFES, con el resultado de las actividades realizadas, hallazgos y recomendaciones sobre la solución, con la relación de las horas ejecutadas.

Transferencias de Conocimiento:
El contratista se compromete a realizar transferencia de conocimiento en las acciones realizadas para el mantenimiento preventivo y afinamiento de las herramientas, esta transferencia de conocimiento está dirigida a máximo cinco (5) colaboradores de la entidad e impartida directamente por el personal certificado por el fabricante, en idioma español con una duración mínima de ocho (8) horas laborales, en las instalaciones del instituto previa coordinación con el supervisor del contrato.

Las condiciones mínimas del personal que prestará el soporte técnico mínimo requerido para la adquisición y el soporte, a nivel de formación y experiencia, se relaciona a continuación, el cual no podrá modificarse sin la previa aprobación del ICFES.

EQUIPO MINIMO DE TRABAJO REQUERIDO

Equipo	Titulo / Certificaciones / Cursos	Experiencia Profesional Especifica
Un (01) Ingeniero Gerente de Proyecto	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones, industrial o carreras afines. Tarjeta Profesional con expedición mínimo de cinco (5) años Posgrado en Gerencia de Proyectos y/o Certificación PMP. Certificación ITIL Foundation v3 o superior Certificación ITIL Managing Professional Certificacion Auditor Interno ISO 27001	Experiencia mínima 10 proyectos gerenciando y/o coordinando proyectos de TI y/o Seguridad Informática.
Un (01) Ingeniero Líder Técnico	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. Especialización o maestría en Seguridad de la Información o ciberseguridad o informática. Certificación vigente en SCRUM Foundations Professional (SFPC) Certificación en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018 Certificación en AUDITOR LÍDER en la norma ISO/IEC 27001:2022. Certificación vigente como Arquitecto o Experto o su equivalente en seguridad en redes emitida por el fabricante con el cual se está presentando el proponente.	Experiencia general de cinco (5) años en proyectos de TI, de los cuales mínimo de tres (3) años como líder o coordinador o gerente de servicio de TI. Certificaciones de Experiencia especifica de mínimo años (4) años en implementación o administración en plataformas de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.
Un (01) Ingeniero Implementador	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. Especialización o maestría en Seguridad de la Información o ciberseguridad o informática. Certificación en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018 Certificación en AUDITOR INTERNO en la norma ISO/IEC 27001:2022 Certificación vigente como Arquitecto o Experto o su equivalente en seguridad en redes emitida por el fabricante con el cual se está presentando el proponente. Certificación vigente como Arquitecto o Experto o su equivalente en seguridad en Nube emitida por el fabricante con el cual se está presentando el proponente.	Experiencia general de tres (5) años en proyectos de TI, de los cuales mínimo de tres (3) años en implementación, soporte y/o monitoreo de soluciones de seguridad La experiencia se cuenta a partir de la expedición de la tarjeta profesional.

	Un (01) Ingeniero de Soporte	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. Especialización o maestría en Seguridad de la Información o ciberseguridad o informática. Certificación en AUDITOR INTERNO en la norma ISO/IEC 27001:2022 Certificación vigente como Arquitecto o Experto o su equivalente en seguridad en redes emitida por el fabricante con el cual se está presentando el proponente. Certificación vigente como Arquitecto o Experto o su equivalente en seguridad de Operaciones emitida por el fabricante con el cual se está presentando el proponente.	Experiencia general de tres (5) años en proyectos de TI, de los cuales mínimo de tres (3) años en implementación, soporte y/o monitoreo de soluciones de seguridad La experiencia se cuenta a partir de la expedición de la tarjeta profesional.	
Nota: El personal de técnico requerido debe ser propio del oferente, no se aceptan figuras de tercerización de servicios o prestación de servicios, para ello se deberán enviar las hojas de vida y/o contrato de vinculación laboral en conjunto con la propuesta, una vez se suscriba el acta de inicio				

El proveedor deberá notificar la designación de estos profesional mediante la presentación de la hoja de vida y los soportes laborales y de estudio de cada perfil, en comunicación dirigida a la persona que la entidad designe para ejercer la supervisión del contrato que se suscribe y radicada en la Oficina de la Unidad de Atención al ciudadano del Icfes: Calle 26 N. 69- 76, Edificio Elemento, Torre Fuego, piso 16 en la ciudad de Bogotá, dentro de los dos (2) días hábiles siguientes a la firma del acta de inicio del contrato.

En el evento de un cambio del profesional este debe ser informado con mínimo quince (15) días calendario a la Entidad, presentado la documentación (hoja de vida y los soportes laborales y de estudio) respectiva del nuevo profesional, el cual debe cumplir el perfil requerido. Si bien es cierto solo se está requiriendo de un profesional, el proveedor debe disponer del recurso humano requerido para atender el soporte técnico en los tiempos requeridos.

El oferente debe presentar certificación de distribuidor autorizado del fabricante donde se evidencie que tiene el nivel de membresía más alto del fabricante: Gold, Premium, Expert o Platinum (según aplique al fabricante). Lo anterior con el fin de garantizar la experiencia en la implementación de las soluciones que requiere la entidad. esta certificación debe estar dirigida a la entidad y no debe superar los 30 días de expedición y se debe mencionar el objeto y numero del proceso.

El oferente debe presentar al menos CINCO (5) especialidades técnicas del mismo fabricante con el cual se está presentando, dentro de la cuales son obligatorias Secure Networking Firewall, Secure Networking LAN Y Cloud Security o sus equivalentes. Esta certificación debe estar dirigida a la entidad y no debe superar los 30 días de expedición y se debe mencionar el objeto y numero del proceso

En el evento de presentación de la oferta en forma conjunta (consorcios o uniones temporales), cada uno de los integrantes deberá aportar las mencionadas certificaciones para el cumplimiento del requerimiento.

El oferente debe entregar los documentos técnicos y/o datasheet del fabricante de las soluciones ofertadas, donde se evidencie el cumplimiento de cada uno de los ítems solicitados en los requerimientos técnicos de las soluciones.

Alcance y Descripción del Soporte
Debe incluir el soporte técnico, en la modalidad Estándar 7*24*365 por el periodo en el cual estén activos los licenciamientos, es decir un (1) año a partir de su activación, teniendo en cuenta los siguientes ítems:

- Soporte, mantenimiento y actualización de las soluciones por un (1) año a partir de la activación de los productos.
- Se debe confirmar la recepción del incidente, entregando un número de caso, en un tiempo máximo de 30 minutos contados a partir de la recepción del incidente.
- El Contratista debe dar respuesta a los incidentes reportados por el ICFES en un tiempo máximo de 4 horas, los cuales pueden ser reportados las 24 horas del día, 7 días de la semana.
- Número de casos ilimitados

- Definir por lo menos dos (2) canales para el reporte de incidentes o casos de soporte, los cuales eran notificados al ICFES en el Protocolo de Soporte.
- Analizar el incidente y, según corresponda, verificar la existencia del problema, identificar la causa raíz y dar solución y/o reportar los avances según los tiempos de gestión definidos.
- Brindar orientación y asistencia al Instituto para resolver la incidente vía remoto en primera instancia y en caso de no dar solución al incidente, la asistencia debe ser presencial.
- Se deben incluir en la oferta dos (02) actividades de mantenimiento preventivo y afinamiento con el fin de minimizar problemas y mantener los sistemas actualizados, estas actividades deberán ser con previa aprobación del responsable TI de la entidad.

NOTA: El contacto con el canal de soporte se debe realizar única y exclusivamente a través de los profesionales designados por el ICFES, quienes centralizaran, priorizaran y filtraran las solicitudes de soporte de los usuarios de acuerdo con los criterios generales del alcance del soporte. Estos profesionales deberán haber recibido capacitación y ser conocedores del sistema de información a soportar y de su implementación y operación

CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACIÓN

- Dada la naturaleza de las actividades a realizar en desarrollo del objeto contractual, el contratista debe garantizar la integridad y confidencialidad de la información institucional a la cual llegue a tener acceso directamente o por intermedio de terceros, para lo cual el contratista suscribe el respectivo compromiso de confidencialidad que hará parte integral del contrato. El contratista deberá asegurar el cuidado, la confidencialidad y la correcta utilización de la información entregada y generada durante la duración de la garantía, soporte y mantenimiento del contrato, así como de los elementos que para su ejecución el Instituto ponga a su disposición.

- De igual manera, de los afinamientos, las políticas y los procesos en la actualización de la solución serán considerados por el contratista como información confidencial propiedad del Instituto Colombiano para la Evaluación de la Educación – ICFES, en tal virtud, adoptará todas las medidas necesarias para impedir su duplicación, sustracción, divulgación, alteración, ocultamiento o utilización indebida.

- Durante los afinamientos, actualización y soporte de las herramientas, el contratista se compromete a no hacer uso indebido de las herramientas utilizadas en desarrollo del objeto contractual, ni duplicar, sustraer, divulgar o alterar información a la cual pueda tener acceso a través de ellas.

Robinson Rivera Cardona
Director de Tecnóloga e Información (E)

Elaboró: Diego Mauricio Salas/ Subdirector de Información