

BOGOTÁ D. C., 22/4/2026

ASUNTO: SOLICITUD COTIZACIÓN.

RESPETADOS SEÑORES, RECIBAN UN CORDIAL SALUDO.

1. OBJETO.

“Adquirir una solución tecnológica de prevención de pérdida de datos (DLP) para la protección de la información institucional de la Federación Colombiana de Municipios en el marco de la función pública asignada.”

2. DESCRIPCIÓN Y JUSTIFICACIÓN DE LA NECESIDAD

La Federación Colombiana de Municipios requiere una solución de DLP Next Generation que permita asegurar la información que puede ser expuesta hacia a internet para aproximadamente 200 usuarios, garantizando el acceso seguro independientemente de la ubicación (red corporativa, conexión móvil, trabajo remoto, etc.), y priorizando su integración con servicios de correo, colaboración, almacenamiento e identidad corporativa en nube. La solución debe estar basada en arquitecturas que permitan poder aplicar políticas de DLP dentro y fuera de la red corporativa, preferiblemente mediante servicios cloud-native y capacidades integradas con el entorno de productividad e identidad de la Entidad. Los servicios en nube ofertados deberán contar con niveles de disponibilidad de hasta 99,999%, de acuerdo con los SLA publicados por el fabricante para los componentes incluidos en la propuesta. La exigencia de disponibilidad aplicará a los servicios cloud del fabricante y no a componentes on-premise. La tecnología ofertada debe permitir identificar si los usuarios se encuentran dentro o fuera del perímetro de la Entidad, usando dispositivos propios o de terceros y de acuerdo con este contexto aplicar políticas de seguridad independientes, privilegiando mecanismos de control basados en identidad, pertenencia a grupos, riesgo, ubicación, estado del dispositivo, cumplimiento del dispositivo y contexto de acceso. A continuación, se detallan los requerimientos de la solución:

Requerimientos Funcionales:

- Debe permitir implementar políticas para educar a los usuarios cuando consuman determinadas aplicaciones en base a los riesgos asociados al su uso o a la actividad que desarrollen dentro de las mismas, incluyendo advertencias contextuales, tips de política, banners o mecanismos de coaching al usuario en tiempo real.
-
- La solución debe conectar a los usuarios remotos directamente a las aplicaciones en entornos de nube pública sin la necesidad de pasar por la infraestructura corporativa.
- La solución deberá soportar controles efectivos sobre tráfico cifrado y sesiones

SOMOS REFERENTES DEL EMPODERAMIENTO Y DESARROLLO MUNICIPAL

☎ 57(1) 5934020 - Fax: 57 (1) 5934027

✉ fcmm@fcmm.org.co - contacto@fcmm.org.co • www.fcmm.org.co
📍 Cra7, N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica



Federación Colombiana de
Municipios



@Fedemunicipios



Federación Colombiana de
Municipios

protegidas, mediante capacidades nativas o integradas del fabricante, con preferencia por servicios cloud que no requieran infraestructura local dedicada como elemento principal de inspección.

- Debe proporcionar capacidad para integrarse con Active Directory en premisa o Azure AD.
- Debe permitir crear roles de administración RBAC y alinearlos con la identidad corporativa y grupos administrativos existentes.

Debe integrarse con sistemas de autenticación multifactor (MFA), compatibles con los estándares TOTP, FIDO2 o similares.

- Debe permitir excepcionar el tráfico en el descifrado SSL o del Steering hacia la plataforma.
- La plataforma no debe utilizar Proxy Reverso como único recurso para controlar la navegación en tiempo real y el acceso a aplicaciones SaaS.
- La plataforma debe contar con la capacidad de enviar el tráfico hacia la plataforma de nube a través de un agente ligero y compatible con Windows, macOS, iOS, Android, ChromeOS así como exploradores (browser), con prioridad funcional sobre estaciones corporativas administradas Windows y macOS, y con detalle expreso del alcance disponible en otras plataformas.
- Debe permitir detectar, analizar y bloquear las transmisiones de información si contienen información confidencial o sensible, así como alertar y educar al usuario sobre el riesgo del uso de aplicaciones cloud con capacidad prioritaria sobre correo, archivos, colaboración, dispositivos administrados y acceso a aplicaciones en nube.
- Debe permitir decodificar aplicaciones cloud y detectar el tránsito de los datos entre aplicaciones, para identificar posibles fugas de información.
- Debe contar con capacidades de analítica de comportamiento, riesgo de usuario, detección de anomalías o funcionalidades equivalentes que permitan identificar conductas inusuales relacionadas con fuga de información o uso indebido.
- Capacidad de diferenciar entre instancias de aplicaciones tales como gestionadas corporativas vs instancias de terceros corporativas vs instancias personales y usar la diferenciación a la hora de aplicar reglas de DLP.
- Debe permitir crear políticas en función de Usuario de AD, Grupo de AD, OU, IP de origen, calidad del dispositivo (administrado o no administrado), Sistema Operativo, Agente de Navegador de usuario, Geolocalización del usuario, Geolocalización de la aplicación, Categoría de la aplicación, Instancia de cliente de la aplicación, Nivel de Confianza en la

SOMOS REFERENTES DEL EMPODERAMIENTO Y DESARROLLO MUNICIPAL

☎ 57(1) 5934020 - Fax: 57 (1) 5934027

✉ fcm@fcm.org.co - contacto@fcm.org.co • www.fcm.org.co
📍 Cra7, N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica



Federación Colombiana de
Municipios



@Fedemunicipios



Federación Colombiana de
Municipios

nube, Clasificación de los datos en movimiento (PCI, PII, etc), file type, Actividad del usuario (tales como compartir, subir, publicar, seguir, descargar, cargar, etc), Credenciales usadas del origen o destino (si se comparte con internos o externos).

- La solución deberá proporcionar capacidades integrales de protección de datos (DLP) y visibilidad unificada sobre la información, permitiendo el monitoreo, control y prevención de fuga de datos en múltiples vectores, incluyendo tráfico de red (con inspección de contenido y cifrado), entornos cloud (IaaS/PaaS), aplicaciones SaaS tanto en datos en movimiento como en reposo, correo electrónico, navegación web, uso de aplicaciones de inteligencia artificial generativa, así como el control de transferencias a través de dispositivos y canales locales como USB y Bluetooth, y la gestión y auditoría de impresiones, todo ello mediante políticas centralizadas y consistentes.

La solución avanzada de Protección de Datos (DLP) debe estar integrada dentro de la plataforma de seguridad en la nube, que permita identificar, analizar y controlar la transmisión de información confidencial hacia aplicaciones web y durante la navegación general en internet.

Debe permitir parametrizar políticas de detección con base en:

- Lógica booleana o Proximidad entre datos o Número de coincidencias.
- Ajuste de nivel de sensibilidad en los hallazgos.
- La solución debe permitir la configuración de políticas basadas en diccionarios personalizados.
- La solución debe estar en capacidad de analizar como mínimo 1500 tipos de archivo.
- La solución debe incluir gestión, investigación y remediación de incidentes de DLP dentro de la misma plataforma unificada, sin depender de consolas externas, hardware onpremise o integraciones obligatorias con terceros.

La solución debe permitir la aplicación de políticas mediante técnicas de:

- Exact Data Match (EDM) o File Fingerprinting.

La solución debe integrar detectores avanzados alimentados con técnicas de Machine Learning que permitan reconocer información sensible en:

- Archivos de imagen o Capturas de pantalla o Documentos no estructurados (clasificadores de ML preentrenados).

SOMOS REFERENTES DEL EMPODERAMIENTO Y DESARROLLO MUNICIPAL

☎ 57(1) 5934020 - Fax: 57 (1) 5934027

✉ fcm@fcm.org.co - contacto@fcm.org.co • www.fcm.org.co
📍 Cra7, N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica



Federación Colombiana de
Municipios



@Fedemunicipios



Federación Colombiana de
Municipios

DLP PARA CORREO ELECTRÓNICO (SMTP)

La solución de Data Loss Prevention (DLP) para correo electrónico saliente debe permitir inspeccionar y controlar los mensajes enviados por usuarios hacia dominios externos, garantizando el cumplimiento de políticas de protección de datos antes de que el correo abandone la Entidad.

La solución debe integrarse dentro del flujo SMTP corporativo sin afectar la continuidad del servicio de correo.

A continuación, se detallan los requerimientos funcionales:

- La solución debe permitir la inspección de correos electrónicos salientes iniciados por usuarios, antes de su entrega a servidores externos.
- La solución debe integrarse en el flujo SMTP entre el servicio de correo en la nube (por ejemplo, Exchange Online o Gmail) y el MTA ascendente.
- La solución debe inspeccionar el contenido del cuerpo del mensaje y los archivos adjuntos en tiempo real, aplicando políticas de protección de datos configuradas previamente.

La solución debe permitir la aplicación de políticas de protección en tiempo real incluyendo:

- El Bloqueo del mensaje o Permitir con registro o Modificación de encabezados o Aplicación de etiquetas o marcas de auditoría.
- La solución debe permitir el procesamiento de múltiples mensajes dentro de una misma sesión SMTP, con el fin de reducir latencia y carga sobre los servidores de correo.
- La solución debe validar que el remitente especificado en el sobre SMTP (SMTP envelope) sea válido y autorizado, evitando que el servicio pueda ser utilizado como proxy abierto.
- La solución debe permitir la inserción de encabezados personalizados en el correo cuando se detecten coincidencias con políticas DLP.
- La solución debe añadir un encabezado que permita evidenciar que el correo fue inspeccionado por el motor DLP.
- La solución debe soportar como mínimo TLS 1.2 y TLS 1.3.

- La solución debe permitir el reenvío del tráfico nuevamente hacia el servicio de correo original en caso de no existir un MTA intermedio.

El oferente debe garantizar la Implementación de las funcionalidades DLP para navegación WEB, CASB, EMAIL y DLP en el dispositivo, para los 200 usuarios. Dentro de las tareas a ejecutar se encuentran las siguientes:

- Levantamiento de Información y Seguimiento en la liberación de prerequisites.
- Despliegue del 100% de los agentes o licencias licenciados a través de herramientas que permitan despliegue automatizado o por medio de cualquier método.
- Sincronización de los grupos y usuarios de Active Directory con el Tenant de la solución
- Apoyo para habilitar MFA en los clientes.
- Apoyo para la configuración y pruebas de funcionamiento de las aplicaciones requeridas
- Configuración y pruebas de DLP.
- Transferencia de conocimiento para tres colaboradores de la entidad quienes operan la herramienta.

SOPORTE:

Servicios de Soporte 7x24, en idioma en español por un año desde el inicio hasta la finalización del licenciamiento adquirido, para atender cualquier tipo de incidente que se presente con la plataforma, así como aportar documentación en caso de ser necesario.

Severidad 1 (Crítico – servicio inoperante): respuesta en máximo 1 hora, resolución en máximo 4 horas.

Severidad 2 (Alto – degradación grave): respuesta en máximo 4 horas, resolución en 24 horas.

Severidad 3 (Medio/Bajo): respuesta en 8 horas hábiles, resolución en 72 horas hábiles.

El proponente deberá indicar el canal oficial de apertura de tickets (portal web, correo, teléfono).

3. LA FORMA DE PAGO:

La Federación Colombiana de Municipios cancelará el valor total del contrato, así:

El valor del contrato será pagado por la Federación Colombiana de Municipios al Contratista en un solo pago, una vez el supervisor del contrato reciba la certificación del licenciamiento y soporte contratado de la plataforma tecnológica por un año, adquirida por la Federación Colombiana de Municipios en cumplimiento de la función pública asignada.

4. PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será de 2 meses, contado a partir del cumplimiento de los requisitos de ejecución.

5. CLASIFICADOR DE BIENES Y SERVICIOS – UNSPSC

El bien o servicio objeto del presente proceso de selección está codificado en el clasificador de Bienes y Servicios UNSPSC, como se indica a continuación:

SEGMENTO	FAMILIA	CLASE	NOMBRE
43	4323	432327	Software de seguridad y protección
43	4323	432332	Software de Aplicación de red
43	4323	432337	Software de administración de sistemas

6. GARANTÍAS.

Cumplimiento del contrato, por un valor de mínimo el 10% del valor total del contrato y por el plazo del contrato y seis meses más.

Calidad del servicio, por un valor de mínimo el 10% del valor total del contrato y por el plazo del contrato y seis meses más

Pago de salarios, prestaciones sociales legales e indemnizaciones laborales. Por un valor de mínimo el 5% del valor total del contrato

7. DATOS MÍNIMOS EN LA COTIZACIÓN DEL PROPONENTE DEBEN TENER:

- Nombre del proponente.
- NIT O N° de C.C.
- Representante legal.
- C.C. del representante legal.
- Teléfono de contacto.
- Correo de contacto.

SOMOS REFERENTES DEL EMPODERAMIENTO Y DESARROLLO MUNICIPAL

☎ 57(1) 5934020 - Fax: 57 (1) 5934027

✉ fcm@fcm.org.co - contacto@fcm.org.co 🌐 www.fcm.org.co
📍 Cra7, N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica



Federación Colombiana de
Municipios



@Fedemunicipios



Federación Colombiana de
Municipios

En la cotización se debe especificar:

- Identificación de valor por ITEM detallado.
- El valor de la propuesta económica deberá estar ajustado al peso más próximo por cada concepto (Valor antes de IVA, IVA y Valor Total).

Nota 1: Esta solicitud de cotización, no genera compromiso para la Federación Colombiana de Municipios, toda vez que su fin es el de soportar el análisis del mercado y estudios del sector.

Con la cotización de precios por favor informar a partir de cuándo y por cuanto tiempo es el soporte de las licencias a adquirir.

Favor enviar la cotización incluyendo el Registro Único Tributario – RUT y RUP actualizado o estados financieros de su organización con corte a diciembre de 2025 a más tardar dentro de los dos (5) días siguientes a la publicación del evento de cotización en la plataforma SECOP II.

De tener dudas frente a la cotización, podrá comunicarse a través de mensaje por la plataforma SECOP II.

Gracias por la atención prestada y esperamos poder contar con su participación.

Proyecto: Ing Juan Carlos Gamarra Anaya – Profesional Oficial De Seguridad De La Información.

SOMOS REFERENTES DEL EMPODERAMIENTO Y DESARROLLO MUNICIPAL

☎ 57 (1) 5934020 - Fax: 57 (1) 5934027

✉ fcmm@fcmm.org.co - contacto@fcmm.org.co • www.fcmm.org.co
📍 Cra7, N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica



Federación Colombiana de
Municipios



@Fedemunicipios



Federación Colombiana de
Municipios