FICHA TÉCNICA / CONDICIONES TECNICAS MINIMAS

Las condiciones del servicio requerido para el presente proceso de selección están relacionadas con el cumplimiento del alcance descrito a continuación:

1. OBJETO.

"Adquisición de licenciamiento para una herramienta virtual que permita la capacitación en seguridad de la información de los colaboradores de la Federación Colombiana de Municipios, en cumplimiento de la función pública asignada."

2. CONDICIONES TÉCNICAS MÍNIMAS REQUERIDAS.

En marco del cumplimiento de la función pública, la Federación Colombiana de Municipios, en su calidad de administrador del Sistema Integrado de Multas y Sanciones por Infracciones a las Normas de Tránsito –Simit, requiere la: Adquisición de licenciamiento para una herramienta virtual que permita la capacitación en seguridad de la información de los colaboradores de la Federación Colombiana de Municipios, en cumplimiento de la función pública asignada.

Lo anterior, en virtud de que es necesario debido a que el factor humano es un pilar fundamental en la ciberseguridad, ya que el mayor porcentaje de brechas de seguridad se producen en los puestos finales de los funcionarios mediante campañas maliciosas de PHISHING O RANSOMWARE.

Los ciberdelincuentes prefieren destinar sus ataques a los usuarios, aprovechando el comportamiento humano inseguro, saltando así cualquier barrera de seguridad basada en software o hardware.

Teniendo en cuenta lo anterior la entidad busca mitigar este vector de ataque buscando un servicio de capacitación y concientización sobre seguridad de la información, el cual debe contar con al menos de 20 módulos de formación, estos deben ser desarrollados por un equipo de expertos en ciberseguridad.

La solución deberá contar con funcionalidades de concientización y capacitación en seguridad de la información, incluyendo campañas periódicas y programables mediante videos, cápsulas interactivas y evaluaciones, con segmentación por roles o perfiles. Asimismo, deberá permitir simulaciones y ejercicios de seguridad, incorporando phishing benigno y medición de clics, reportes y comportamiento de los usuarios.

La herramienta deberá ofrecer métricas y seguimiento mediante dashboards, reportes, exportación de resultados e historial de campañas y evaluaciones. A nivel técnico, se requiere una plataforma web con soporte RBAC, integración con directorios institucionales y capacidades de gestión de usuarios y roles.

En materia de seguridad y privacidad, deberá garantizar la protección de datos personales, autenticación y control de accesos, registro de eventos y cumplimiento de los principios de confidencialidad, integridad y disponibilidad.

La solución deberá alinearse con la norma ISO/IEC 27001, apoyando controles como A.6.3 Concientización y formación en seguridad de la información, A.5.16 Gestión de identidades, A.5.17 Información de autenticación y A.5.36 Cumplimiento de políticas de seguridad. Igualmente, deberá contribuir al cumplimiento del MIPG (Modelo Integrado de Planeación y Gestión), especialmente en Control Interno, Gestión del Conocimiento e Innovación, Seguridad Digital y fortalecimiento de la cultura organizacional orientada a la prevención del riesgo.

Finalmente, la herramienta deberá facilitar los procesos de Auditoría Interna mediante evidencia documental de capacitaciones, métricas e indicadores, trazabilidad de campañas y soporte a procesos de verificación y mejora continua.

Mediante el entrenamiento apropiado, los funcionarios serán conscientes de la seguridad y la importancia de esta, tanto en la organización como en su hogar. Podrán identificar y prevenir incidentes de seguridad de la información a través de buenas prácticas asimiladas de una manera natural e intuitiva.

La herramienta deberá permitir sensibilizar, capacitar, evaluar y medir el comportamiento de los colaboradores frente a riesgos de seguridad de la información, apoyando el cumplimiento normativo y los objetivos institucionales.

REQUERIMIENTOS FUNCIONALES

Concientización y capacitación
- Contenidos educativos en seguridad de la información.
- Campañas periódicas y programables.
- Formatos: videos, cápsulas interactivas, evaluaciones.
- Segmentación por roles o perfiles.

Simulaciones y ejercicios
- Simulaciones de drills de seguridad.
- Inclusión de phishing benigno.
- Medición de clics, reportes y comportamiento.

Métricas y seguimiento
- Dashboards y reportes.
- Exportación de resultados.
- Historial de campañas y evaluaciones.

REQUERIMIENTOS TÉCNICOS

- Plataforma web.
- Soporte RBAC.
- Integración con directorios institucionales.
- Gestión de usuarios y roles.

SEGURIDAD Y PRIVACIDAD
- Protección de datos personales.
- Autenticación y control de accesos.
- Registro de eventos.
- Principios de confidencialidad, integridad y disponibilidad.

AUDITORÍA INTERNA
- Evidencia documental de capacitaciones.
- Métricas e indicadores.
- Trazabilidad de campañas.
- Soporte a procesos de verificación y mejora continua.

Implementación

El contratista debe garantizar la disponibilidad de personal idóneo y suficiente, así como el acompañamiento continuo de fabricante durante la fase de implementación y hasta la entrada en operación de la solución y durante el soporte de la herramienta por el tiempo contrado.

El contratista deberá garantizar la instalación, configuración, pruebas, puesta en producción y apoyo en la operación de las soluciones, asegurando su entrega completa y en condiciones de funcionamiento satisfactorias para la Entidad.

El contratista debe entregar a la Entidad la documentación técnica y administrativa derivada del proyecto, incluyendo diseños, configuraciones, procedimientos y manuales operativos, de manera estructurada y validada con el equipo designado por la Entidad.

Soporte

El fabricante deberá garantizar soporte 7x24 en español, incluyendo escalamiento técnico y de producto, con un portal disponible para apertura de tickets, chat, histórico y seguimiento de SLA. Además, deberá ofrecer canales de contacto como correo, teléfono y colaboración opcional mediante Slack o Teams si el cliente lo requiere.

El proveedor deberá establecer objetivos de resolución según severidad y realizar revisiones trimestrales de cumplimiento, manteniendo una matriz de escalamiento con contactos disponibles en todo momento, incluyendo gerencia de ingeniería y producto. Asimismo, deberá disponer de una base de conocimiento con artículos y guías actualizadas, junto con una página de estatus para notificar incidentes o mantenimientos con detalle de ETA y alcance. Los incidentes deberán cerrarse con un informe de causa raíz emitido dentro de 5 días hábiles, incluyendo acciones preventivas.

En cuanto a mantenimientos y cambios, el proveedor deberá anunciar con al menos 72 horas de anticipación las actividades programadas, indicando la ventana, el impacto y el plan de reversión. Todo cambio deberá gestionarse bajo un proceso documentado con pruebas previas en entornos no productivos. El soporte deberá incluir habilitación y onboarding con checklist para activar módulos en menos de una hora.

Tabla: Niveles De Servicio De Soporte Técnico

Matriz de prioridades

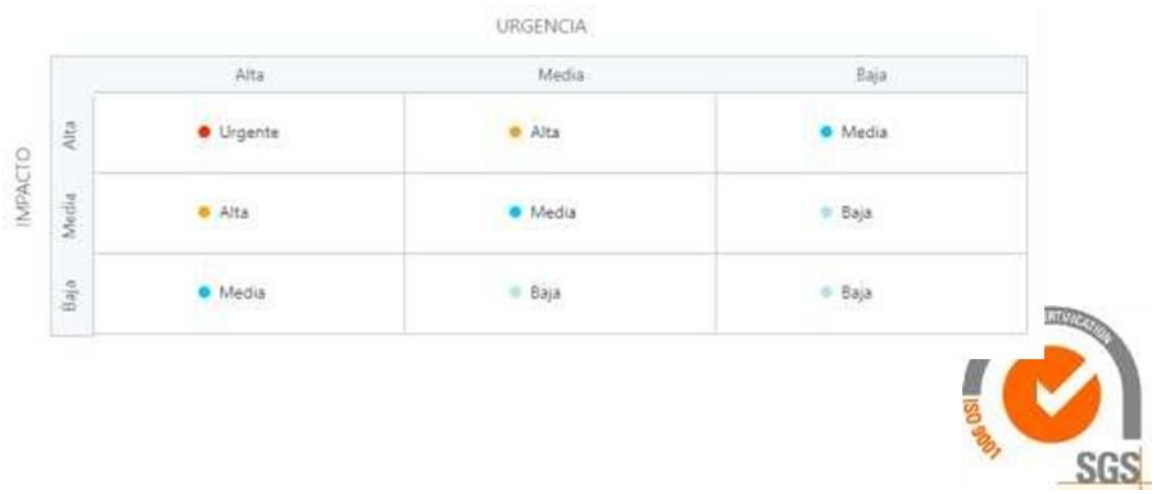
Prioridad		Descripción
1	Urgente o Crítica	La producción está parada o severamente impactada de manera que no se puede continuar trabajando. La operación es de misión crítica para la entidad y/o está en situación de emergencia. Este nivel de severidad tendrá más de una de las siguientes características: Total, pérdida o inestabilidad crítica de funciones. Impacto crítico de tráfico, pérdida total de conectividad o fallas vitales en la seguridad.
2	Alta	Experimenta pérdida de servicio, algunas características importantes no pueden ser utilizadas, sin embargo, la operación continúa de manera restringida
3	Media	Experimenta una pérdida de servicio menor, el impacto es un inconveniente.
4	Baja	No impacta en la operación del programa, no se experimenta perdida de servicio y no se impide la operación de los sistemas

Atención remota.

La atención de los requerimientos es categorizada de acuerdo con su prioridad y niveles de servicios contratados.

Prioridad		Descripción
1	Urgente o Crítica	De manera remota (1 horas).
2	Alta	De manera remota (1.5 horas).
3	Media	De manera remota (3 a 5 horas).

4	Baja	De manera remota (48 horas).



Transferencia De Conocimiento

El contratista debe realizar la transferencia de conocimiento hasta un máximo de 3 horas, dirigida a un grupo de 3 funcionarios designados por la Entidad, asegurando que el contenido de las sesiones cubra las competencias necesarias para la operación y mantenimiento de las soluciones implementadas.

El proveedor deberá ofrecer un plan de capacitación con objetivos claros y resultados medibles, incluyendo un onboarding práctico que permita activar cada módulo en menos de una hora con guía y checklist. Además, entregará materiales actualizados en español como manuales, guías rápidas, runbooks y presentaciones.

La capacitación deberá contar con laboratorios prácticos en un entorno seguro con datos simulados, evaluaciones pre y post-test para medir avances, y un reporte de brechas por participante. Finalmente, el proveedor deberá emitir constancias o certificados de aprovechamiento por rol y módulo al cumplir los criterios de aprobación.

El contratista debe garantizar que las sesiones incluyan aspectos teóricos y prácticos, abarcando administración, monitoreo, resolución de incidentes y buenas prácticas de uso de las soluciones implementadas.

3. PLAZO

El plazo de ejecución del contrato será de DOS (2) MESES de ejecución, contado a partir del cumplimiento de los requisitos de ejecución, sin que sobrepase el 27 de diciembre de 2026.

El acceso al licenciamiento debe ser de DOCE (12) MESES, contados a partir del recibo a satisfacción por parte del supervisor del contrato, una vez implementada la herramienta y

realizadas las mejoras.

4. 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.

5. Clasificador de bienes y servicios – UNSPC

De igual manera este objeto se encuentra enmarcado dentro del plan anual de adquisiciones publicado en el Secop II y en la página web de la entidad en la fila N° 84 del archivo PAA 2026:

COD. SEGMENTO	COD. FAMILIA	COD. CLASE	COD. PRODUCTO	DESCRIPCIÓN	OBJETO A CONTRATAR
43	23	25	00	Software educativo o de referencia	Adquisición de licenciamiento para una herramienta virtual que permita la capacitación en seguridad de la información de los colaboradores de la Federación Colombiana de Municipios, en cumplimiento de la función pública asignada.

6. GARANTÍAS.

- Cumplimiento del contrato: Equivalente al diez por ciento (10%) del valor total del contrato, por un término igual al plazo del contrato y seis (6) meses más.
- Calidad del servicio: Equivalente al diez por ciento (10%) del valor total del contrato, por un término igual al plazo del contrato y doce (12) meses más.
- Pago de salarios, prestaciones sociales e indemnizaciones laborales: Equivalente al cinco por ciento (5%) del valor total del contrato, por un término igual al plazo del mismo y tres (3) años más.

I) OBLIGACIONES DEL CONTRATISTA

a) Obligaciones Generales

1. Cumplir con el objeto contratado de acuerdo con los requerimientos definidos por la Entidad.
2. Cumplir oportunamente con todas las exigencias y procedimientos establecidos para la firma electrónica de los contratos y sus modificaciones en la plataforma de SECOP II.
3. Publicar para cada pago en la plataforma del Sistema Electrónico de Contratación Pública SECOP II los informes y/o productos de ejecución contractual, con los soportes, si hubiere lugar a ellos, de acuerdo con lo estipulado en la Ley 1712 de 2014, o en la plataforma que corresponda.
4. Asistir a las reuniones programadas, relacionadas con la ejecución del objeto contractual.
5. Presentar los informes que el supervisor del contrato solicite en desarrollo del objeto contractual.
6. Acatar las directrices establecidas por la Federación Colombiana de Municipios la Función Pública en cuanto a los trámites para el cobro de los valores pactados en el presente contrato, cumpliendo los requisitos y fechas definidas por la entidad.
7. Mantener al día sus pagos en el Sistema General de Seguridad Social Integral y entregar antes de cada pago, copia de la planilla correspondiente al supervisor del contrato, si se trata de personas naturales, o entregar para cada pago, la certificación suscrita por el representante legal o revisor fiscal, que acredite el cumplimiento del pago de aportes al Sistema de Seguridad Social Integral, parafiscales, ICBF, SENA y cajas de compensación familiar de los últimos seis (6) meses.
8. Aplicar durante la ejecución del contrato, los lineamientos establecidos en el Sistema de de Calidad de la Entidad.
9. Reportar al supervisor del contrato, novedades o anomalías relacionadas con la ejecución contractual.
10. Responder por las actuaciones u omisiones derivadas de la celebración del contrato y de la ejecución del mismo, de conformidad con lo establecido en la Ley 80 de 1993.
11. No acceder a peticiones o amenazas de quienes actúen por fuera de la Ley con el fin de obligarlos a hacer u omitir cualquier acto o hecho.
12. Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones y entrabamientos que puedan presentarse y, en general, cumplir con lo establecido en la Ley 80 de 1993, la Ley 1150 de 2007, Ley 1474 de 2011, sus reformas y decretos reglamentarios.
13. EL CONTRATISTA autoriza a LA FEDERACIÓN l tratamiento de datos personales para dar cumplimiento con lo establecido en la Ley 1581 de 2012, reglamentada parcialmente por los Decretos 1377 de 2013 y 1081 de 2015, y el Decreto 255 de 2022 y demás normas que los modifiquen, complementen o sustituyan; en total conocimiento, entendimiento y aceptación de la política de datos, disponible en https://www.fcm.org.co/politica-de-datos/
14. En consecuencia, autoriza de manera libre, expresa, voluntaria y debidamente informada a LA FEDERACIÓN para dar tratamiento a los datos que han sido suministrados y que se han incorporado en las distintas bases de datos con el ánimo de garantizar la seguridad de su información y el ejercicio de sus derechos y el desarrollo de su actividad.
15. Las demás que se deriven del artículo 5° de la Ley 80 de 1993, así como todas aquellas que señalen la Constitución y la Ley y que tengan relación directa con el objeto del contrato.
16. El contratista se obliga a cumplir las disposiciones normativas de la política de Tratamiento de datos personales, Políticas de Operación Institucionales, Política de seguridad de la información y Políticas técnicas de seguridad de la información adoptadas por la Entidad.

17. Deberá guardar absoluta reserva sobre la información PÚBLICA RESERVADA, PÚBLICA CLASIFICADA, DATOS SENSIBLES, DATOS PRIVADOS, DATOS SEMIPRIVADOS, SECRETO EMPRESARIAL COMERCIAL, durante toda la vigencia del contrato y hasta 2 años después de la liquidación (si aplica) del mismo, so pena de las sanciones y consecuencias tanto contractuales como penales, que fueren del caso

a) Obligaciones Especificas

1. El contratista se obliga al cumplimiento de la ficha técnica durante la ejecución del contrato.
2. El contratista deberá suministrar y habilitar la herramienta dentro de los cinco (5) días hábiles siguientes al cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato cumpliendo las especificaciones técnicas descritas en la ficha técnica. El plazo restante del contrato debe emplearse para la puesta en funcionamiento y mejoras necesarias de acuerdo con los requerimientos de la supervisión.
3. El contratista se obliga al cumplimiento del soporte en los términos de la ficha técnica.
4. La plataforma de capacitación y concientización sobre seguridad entregado a la entidad debe contar con mínimo 20 módulos de formación. Los cuales deben ser desarrollados por un equipo de expertos en ciberseguridad y deberá cubrir un mínimo de doscientos (200) usuarios con acceso a todos los módulos y a la plataforma de simulación.
5. La plataforma de capacitación y concientización sobre seguridad debe contar con un portal de administración que ofrezca un panel de control actualizado de la actividad del usuario.
6. La plataforma de capacitación y concientización sobre seguridad debe integrarse e incluir un servicio de simulación de suplantación (phishing) para la misma cantidad de usuarios 200 para comprobar la concientización de los funcionarios, este servicio debe ser del mismo fabricante de la solución de capacitación, o que este avalado por el fabricante.
    a. La plataforma de phishing debe incluir
    b. Informes detallados
    c. Generar phishing personalizado
    d. Nivel de riesgo
7. La plataforma de capacitación y concientización sobre seguridad debe permitir a los administradores crear reglas dinámicas con acciones de capacitación basadas en los resultados de la simulación de suplantación de identidad.
8. La plataforma deberá garantizar una disponibilidad mínima del noventa y nueve por ciento (99%) mensual, excluyendo mantenimientos programados comunicados con 72 horas de anticipación.
9. La plataforma de capacitación y concientización sobre seguridad debe incluir exámenes (o evaluaciones) y verificaciones de conocimientos a lo largo de la capacitación para comprobar la comprensión y retención de los funcionarios.
10. La plataforma de capacitación y concientización sobre seguridad debe tener la posibilidad de personalizar la marca.
11. La plataforma de capacitación y concientización sobre seguridad entregado por el oferente a la entidad debe contar con módulos de formación orientados al equipo

gerencial y ejecutivo. Los cuales deben ser desarrollados por parte de un equipo de expertos en ciberseguridad.

12. La plataforma de capacitación y concientización sobre seguridad debe incluir recursos de refuerzo del aprendizaje adicionales, tales como: carteles, protectores de 20 nano videos de comunicación, posters, hojas de consejos.
13. La plataforma de capacitación y concientización sobre seguridad debe permitir la creación de campañas personalizadas con módulos de capacitación seleccionados para satisfacer las necesidades de la entidad.
14. La plataforma de capacitación y concientización sobre seguridad debe incluir el envío a los funcionarios de correos electrónicos de “inicio”, del recordatorio y de finalización del curso.
15. La plataforma de capacitación y concientización sobre seguridad debe incluir informes integrados en formato PDF para administradores y ejecutivos.
16. La plataforma de capacitación y concientización sobre seguridad debe incluir informes integrados con la siguiente información:
    a. Informe individual de campaña
    b. Informe semanal, mensual o al finalizar la campaña
    c. Informe ejecutivo de la campaña
    d. Tasa de culminación total
    e. Progreso de todas las campañas
17. La plataforma de capacitación y concientización sobre seguridad deben tener disponible el contenido para los empleados en diferentes idiomas y debe permitir esta configuración de forma simultánea
18. La plataforma de capacitación y concientización sobre seguridad debe permitir la creación de los funcionarios a través de creación manual, archivo CSV o sincronización desde un directorio LDAP.
19. La plataforma de capacitación y concientización sobre seguridad debe permitir la integración con los dominios de la entidad.
20. La plataforma de capacitación y concientización sobre seguridad debe contar con un dashboard en el portal de administración que permita visualizar las campañas de capacitación en curso, los módulos incluidos en cada campaña y la cantidad de funcionarios asociados a estas.
21. La plataforma de capacitación y concientización sobre seguridad debe contar con un menú en el portal de administración que permita los administradores establecer el contenido de aprendizaje que luego se asignará a los alumnos. Los administradores pueden elegir algunos o todos los módulos disponibles.
    a. La plataforma de capacitación y concientización sobre seguridad debe contar con reglas de remediación que les permitan a los administradores tomar acciones como enviar una notificación a un estudiante cuando se le asigna una Campaña, emitir un certificado, o una competencia al finalizar el programa, o enviar un recordatorio cuando el programa está atrasado.

b) OBLIGACIONES DE LA FEDERACIÓN:

1) Pagar a EL CONTRATISTA el valor convenido posterior a la presentación de cada entregable y cumplimiento de actividades, previa verificación y certificación por parte del supervisor.
2) Entregar oportunamente o poner a disposición de EL CONTRATISTA los elementos, documentos, datos e informes necesarios para el eficiente y eficaz cumplimiento del objeto contractual.
3) Exigir a EL CONTRATISTA la calidad en los servicios prestados objeto del contrato.
4) Exigir a EL CONTRATISTA la ejecución idónea y oportuna del objeto del contrato.
5) Adelantar las gestiones necesarias para el reconocimiento y pago de las sanciones pecuniarias y garantías a que hubiere lugar.

Nota: Cuando haya lugar a la modificación del plazo o valor consignado en el contrato LA CONTRATISTA deberá constituir los correspondientes certificados o anexos de modificación de las garantías, sin perjuicio de la obligación que le asiste al tomador de mantener informada a la aseguradora de cualquier modificación del estado de riesgo amparado. Así mismo, será de cargo de LA CONTRATISTA el pago de todas las primas y demás erogaciones de constitución, mantenimiento y restablecimiento inmediato de su monto, cada vez que se disminuya o agote por razón de las sanciones que se impongan, por sus prórrogas o suspensiones.