FORMATO 2 – FICHA TÉCNICA / ACEPTACIÓN DE LAS CONDICIONES TÉCNICAS

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 una plataforma tecnológica bajo modelo SaaS para la gestión de riesgos y el fortalecimiento de la postura de seguridad, detección temprana de exposiciones de información en entornos digitales incluida Deep y Dark Web, y la prevención de suplantación de marca y phishing para de la Federación Colombiana de Municipios en cumplimiento de la función pública asignada."

2. CONDICIONES TÉCNICAS MÍNIMAS REQUERIDAS.

Se requiere una solución en nube tipo SaaS, la cual debe garantizar una cobertura 360° de exposición externa durante doce (12) meses, incluyendo monitoreo de (2) dominios, subdominios, IP públicas, buckets, repositorios de código y menciones en comunidades clandestinas. La plataforma debe incorporar inteligencia de amenazas con acceso comunidades en deep y dark web, con evidencia pública de las fuentes monitoreadas. Además, contar con un motor de scoring para medir severidad y riesgo, considerando criticidad, explotabilidad, impacto y contexto de negocio. La interfaz, reportes y soporte estarán disponibles en inglés y español, con selección configurable.

El soporte técnico de la solución deberá operar en modalidad 7x24 en español, con canales formales de atención y escalamiento, asegurando niveles de servicio con disponibilidad mínima de 99%. Los datos sensibles deben estar protegidos mediante cifrado AES 256 en reposo y TLS 1.2, 1.3 en tránsito. El portal de soporte incluirá chat y gestión de tickets con respuesta a incidentes críticos en menos de una hora. La solución actualizará diariamente fuentes OSINT, deep y dark web, y permitirá etiquetar activos críticos.

La plataforma deberá generar evidencias seguras con hash criptográfico y sello de tiempo para garantizar cadena de custodia. También mantendrá repositorios con historial de versiones y acciones de usuarios. Ofreciendo indicadores de desempeño como "time to shield", fijando objetivos y umbrales. Incluyendo tableros ejecutivos y técnicos con filtros de severidad, estado y fuente, además de exportación de reportes en formatos CSV, Excel o PDF. El flujo de gestión de hallazgos seguirá estados estandarizados con trazabilidad completa.

En cuanto a seguridad, la solución deberá permitir autenticación multifactor (OTP o 2FA) administrable, gestión de usuarios y roles, y asignación de ownership de vulnerabilidades. Permitirá definir SLA por prioridad con alertas de vencimiento e integración con ITSM para creación de casos. Unificará hallazgos de múltiples escáneres en un modelo único, deduplicando y agrupando por activo, CVE, servicio y puerto. Además, administrará escalas de severidad propias y estándares internacionales, con vistas de inteligencia, tendencias y rankings.

La plataforma incluirá un módulo de gestión de vulnerabilidades con trazabilidad por evento, registro

ofensivo alineado a MITRE ATT&CK y cálculo de edad por vulnerabilidad. Planes de mitigación con hitos y responsables, y monitoreo de cuentas VIP con atributos de riesgo, privilegios e IAM. Integrando capacidades de inspección y derribo de phishing (pagina que suplanten los dominios o la actividad de la organización), generación automática de evidencias, monitoreo continuo de dominios y tablero de cumplimiento con referencia a marcos normativos.

Integraciones

La solución debe integrarse con sistemas SIEM como Chronicle, QRadar, Splunk y otros, además de plataformas PAM como CyberArk, BeyondTrust o HashiCorp, garantizando una gestión centralizada de accesos y amenazas. También deberá conectarse con herramientas de administración de parches como WSUS/SCCM o Altiris para auditoría y reportes, así como con soluciones de gestión de vulnerabilidades como Nessus, Tenable IO, Crowdstrike o Trend Micro. La cobertura estará enfocada en el dominio evaluado, asegurando precisión en los hallazgos. Finalmente, deberá integrarse con sistemas de tickets y mensajería como Jira, Aranda, Slack, Teams y correo electrónico para facilitar la gestión y comunicación operativa.

Monitoreo de Datos Filtrados

La solución debe permitir registrar y monitorear credenciales expuestas en hasta dos (2) dominios y subdominios, exportando a múltiples formatos (texto, CSV, JSON) y normalizándolos en un modelo consistente. El sistema evitará almacenar contraseñas en claro, trabajando únicamente con hashes y metadatos para garantizar seguridad. Los hallazgos estarán limitados a dominios verificados, aplicando de duplicación para reducir alertas redundantes, por un periodo de doce (12) meses.

La plataforma debe ofrecer vistas con filtros por identidad, dominio, fuente y severidad, además de búsquedas por identidad o hash. Mostrará métricas como tendencias de hallazgos y rankings de identidades más expuestas, así como sitios más frecuentes de exfiltraciones. También permitirá exportar datos en un clic (CSV/Excel) y marcar resultados como falsos positivos con justificación. Los hallazgos seguirán un flujo estándar de estados con línea de tiempo y evidencias adjuntas y deberá permitir habilitar comentarios operativos para colaboración entre analistas.

La solución deberá integrarse tener un notificador de casos con los hallazgos, permitiendo a los equipos el escalamiento por incumplimiento de SLA. Permitirá envío de hallazgos a una bóveda de evidencias para validación de credenciales lo que permitirá a la entidad reflejar el resultado en el estado de severidad. Se podrán documentar flujos de rotación o invalidación de credenciales cuando se envian las detecciones, registrando hitos de ejecución. El sistema mostrará la edad de exposición, distribución por severidad, inventario de hallazgos y paneles ejecutivos con indicadores. Además, soportará RBAC (modelo de control de acceso), para roles, permisos y auditoría de acciones de cada uno de los usuarios.

La plataforma deberá incluir acciones para gestionar hallazgos, identificar escalas de severidad y presentar vistas de casos críticos. Ofrecerá indicadores de exposición por identidad o dominio, etiquetado configurable y ofuscación parcial de datos sensibles. Debe contar con la posivilidad de exportar reportes ejecutivos o técnicos a un solo click multilenguaje (español/inglés). Asimismo, soportará autenticación multifactor, segregación de datos por cliente y políticas de retención de

información.

La solución garantizará el cifrar datos sensibles en reposo con AES 256 y en tránsito con TLS 1.2 - 1.3 o superior con controles de ordenamiento y descarga de evidencias con verificación de integridad. Mostrará contadores agregados, filtros por identidades, datos contextuales hacia otros módulos. Al identificar un hallazgo, se evidenciará indicadores que le den a la entidad un observatorio del estado de riesgo de la entidad. Se incluirán notificaciones automáticas de requerirse, métricas de cumplimiento de SLA, reportes ejecutivos en PDF y vistas guardadas. Todo con trazabilidad de cambios, índices de exposición y auditoría en eliminaciones.

Boveda De Datos Exfiltrados

La solución debe validar por medio de dos (2) dominios sus credenciales, usuarios y URLs obtenidos de exposiciones externas, siempre bajo políticas aprobadas y limitadas a dos dominios, durante doce (12) meses. Toda validación se realizará en entornos controlados, con autorización previa registrada mediante sello de tiempo y responsable asignado. El sistema impedirá el uso indebido de credenciales, limitando los chequeos a pruebas de existencia o autenticidad sin abuso de sesiones. Además, soportará listas administrables de destinos permitidos o prohibidos.

La plataforma deberá recibir casos desde el monitoreo de datos filtrados dejando en evidencia su integración, normalizando los datos y delimitando alcance por dominios o unidades verificadas. Permitirá validaciones pasivas (como caducidad o bloqueo) y activas mínimamente invasivas en laboratorios autorizados. Limitará intentos y ritmo de validación para evitar bloqueos, además de definir listados de datos filtrados para test. Los datos sensibles estarán protegidos con AES 256 en reposo, TLS 1.2 - 1.3 en tránsito y ofuscación en la interfaz. Las evidencias quedarán registradas con hash, sello de tiempo y descarga íntegra.

Cada caso mantendrá línea de tiempo con acciones, aprobaciones, rechazos, cierres, etc., pudiendo etiquetar con evidencias la situación de cada dato filtrado. Los estados abarcarán validado, no válido, no concluyente. Se permitirá reasignación de estados a los datos identificados con registro de falsos positivos y cierres automáticos tras rotación de credenciales. Los resultados se integrarán con identificación de datos exfiltrados y concentrador de pentest/vulnerabilidades para planes de remediación.

La plataforma integrará a sistemas de notificaciones por correo al propietario y equipo ante cambios críticos. Soportará reglas de orquestación, autoasignaciones y plantillas de comunicación para responsables de aplicaciones. Ofrecerá indicadores de tiempo de validación, tasa de validez y tasa de falsos positivos, además de tendencias de casos mensuales. Mostrará distribución de hallazgos por fuente, dominio y criticidad, con búsquedas o acciones masivas. Asimismo, permitirá vistas guardadas, filtros compartidos y ordenamientos por severidad, prioridad o antigüedad.

La solución contará con auditoría detallada de validaciones, exportable en CSV o PDF, con control de cambios en evidencias y decisiones. Restringirá el alcance de identificación a los dominios de validación y bloqueará destinos no autorizados. Permitirá la retención durante la vigencia del contrato acorde con las políticas de retención y asistente de activación rápida. Finalmente, soportará español e inglés en el tablero de gestión, con enlaces directos a evidencias y módulos relacionados para

trazabilidad completa.

Monitoreo De Ejecutivos Y C-Levels

La solución deberá contemplar el registro y monitoreo de hasta 100 cuentas VIP, por doce (12) meses, tanto internas como externas, diferenciadas por correo, dominio y rol crítico. Permite la carga masiva de cuentas mediante archivos CSV con validación de formato y la asignación de niveles de riesgo desde la interfaz. Además, cada perfil VIP puede registrar atributos clave de seguridad como la habilitación de MFA, privilegios IAM (admin, financiero, ejecutivo, etc.) y etiquetas personalizadas por unidad de negocio, país o proyecto. El sistema debe validar que los correos pertenezcan a dominios autorizados o estén justificados en caso de externos. Ofrecer un resumen consolidado de VIP críticos con y sin MFA, aportando visibilidad inmediata del estado de seguridad.

La plataforma debe incluir un tablero de correlación de amenazas diseñado específicamente para VIP, con indicadores como totales de eventos en las últimas 24 horas, promedios de correlación y niveles de exactitud. Este tablero se alimenta de señales externas provenientes de la dark web, foros, canales de mensajería, bases de datos de filtraciones y repositorios públicos. Los umbrales de correlación y confianza deben ser configurables, permitiendo escalar automáticamente a alertas cuando el riesgo lo amerite. Cada correlación se respalda con evidencia que incluye hash y sello temporal, garantizando trazabilidad y confianza. Adicionalmente, se ofrece una línea de tiempo por VIP con eventos correlados, cambios de riesgo y acciones tomadas.

Alertas VIP deberá soportar estados como nueva detección, investigando, confirmada, mitigada, resuelta entre otras. Debe permitir marcar falsos positivos con justificación y adjuntos, asignar propietarios y equipos, y configurar escalamiento automático por SLA vencido según severidad. El sistema debe enviar notificaciones a correo y canales de colaboración como Slack o Teams si se requiere. Incluye playbooks de respuesta específicos para VIP con acciones como notificar al CISO (Profesional de seguridad de la información), notificar el forzar reset de credenciales, notificar el revocar tokens, entre otros. Estos playbooks se pueden activar, desactivar y versionar con control de cambios, midiendo métricas como tasa de éxito y tiempo promedio de ejecución.

La gestión de evidencias y auditorías deberá estar presentada en indicadores en el tablero de gestión. El sistema debe registrar todas las acciones sobre perfiles VIP, adjunta evidencias en alertas con permisos, y notificaciones para ejecutivos afectados. Se soportará idioma español e inglés para todo el módulo incluidos los informes que se puedan descargar, y se ofrecen filtros avanzados por riesgo, MFA, privilegios, tags, estado o fecha. Los indicadores deberán incluir tiempos de detección, notificación y contención, así como porcentaje de alertas atendidas en SLA y tendencias mensuales. Todo el módulo es exportable a CSV, Excel o PDF.

La plataforma garantizará seguridad y usabilidad. Implementando RBAC para restringir acceso, permitir marcar cuentas como altamente riesgosa. Se integrará con el monitoreo de datos filtrados y boveda de datos filtrados, asegurando trazabilidad y mitigación integral. Deberá soportar vistas ejecutivas y operativas, widgets de riesgo agregado y asignación automática de propietarios por reglas. Se contempla que tenga retención configurable durante la ejecución del servicio permitiendo la ofuscación de datos personales y un asistente de configuración inicial que permite activar el módulo en menos de una hora.

Inspector De Phising

Permitir registrar hasta dos (2) dominios y subdominios para monitoreo continuo durante doce (12) meses, con opción de habilitar o deshabilitar supervisión 24/7 desde la interfaz. El sistema incluirá listas blancas para evitar falsos positivos y genera permutaciones de dominios para identificar look-alike y typosquatting así como otras técnicas para detección de phishing por medio de palabras claves parametrizables. Se analizará información pública como WHOIS de sitios fraudulentos automaticamente y deberá realizar capturas de pantalla y HTML con hash y sello de tiempo de los sitios fraudulentos, también deberá evalúar similitud visual y textual. Cada hallazgo recibe un puntaje de riesgo consistente con umbrales definidos.

Las detecciones generarán alertas en vivo cuando superan el umbral configurado. Para que los analistas pueden clasificar hallazgos como legítimos, sospechosos o maliciosos con un click, marcarlos como falsos positivos con justificación o adjuntar evidencias adicionales. Cada caso debe conserva una línea de tiempo de eventos y cambios de estado. La solución integrará plantillas de derribo dirigidas a registradores, proveedores de hosting, autoridades de certificados y organismos como ICANN. Dichas plantillas deben ser personalizables, soportar español e inglés y permitir adjuntar automáticamente evidencias como WHOIS y HTML como mínimo. El envío siempre requiere aprobación de analista para asegurar control.

El proceso de derribo o takedown deberá realizarse desde la misma plataforma y quedará registrado con estados como borrador, enviado, reconocido, resuelto o rechazado, incluyendo sellos de fecha y hora para medir tiempos operativos. Se soportará reenvío y escalamiento documentado, así como exportación de todas las solicitudes en un solo archivo para auditoría. El sistema generará indicadores clave como tiempo a reconocimiento, tiempo a resolución, tasa de derribos exitosos y tasa de falsos positivos. Además, se presentan métricas de distribución por severidad y estado, número de dominios protegidos, amenazas detectadas, evidencias recolectadas y tendencia mensual de detecciones, derribos y resoluciones.

Se debe de poder hacer derribos o takedown hasta para 300 sitios que se llegén a identificar suplantado la imagen, marca, dominio, logo, nombre u actividad económica de la Federación Colombiana de Municipios.

El módulo operará eficientemente. Notificando a interesados por correo y a canales de colaboración como Slack o Teams en alertas críticas. Ofreciendo gestión de casos por reglas y deep links a hallazgos específicos. Soportará acciones masivas, vistas guardadas, comentarios internos con menciones, y control de confidencialidad en evidencias. Además, registra auditoría completa de descargas, cambios de configuración y acciones sobre hallazgos.

El módulo asegurará cumplimiento, seguridad y trazabilidad. Conserva versiones de evidencias, operará en tiempo real para reducir riesgos, debe ofuscar datos sensibles y evitar envíos automáticos sin aprobación. Se integrará con otros módulos para garantizar trazabilidad, vinculando hallazgos de phishing con activos e identidades relevantes. Deberá respetar la escala global de severidad, permitiendo definir políticas de retención y exportar auditorías en CSV o PDF. Incluyendo un asistente de configuración inicial que habilita el módulo en menos de una hora. Además, soportar reportes

ejecutivos con indicadores y anexos técnicos de evidencias todo multilingue (español/ingles).

Takedown

Se deberá permitir el envío de reportes X-ARF multilingües para amenazas como phishing o abuso de marca, con paquetes probatorios adjuntos. Gestiona estados, SLA y recordatorios, con escalamiento por incumplimientos.

Integración con listas y proveedores, registro de acuses, propagación de IOC a controles temporales y soporte de cargas masivas vía CSV/API. Los casos se vinculan para evitar duplicados y medir campañas globales.

Descubrimiento automático de contactos de abuso, localización según país y proveedor, y captura renderizada con línea de tiempo. Se soportan playbooks por tipo de proveedor y escalamiento programado por falta de respuesta.

Ver métricas de efectividad por tipo de amenaza y proveedor, incluyendo tasa de baja, tiempos promedios y causas de rechazo. Se ofrecen reportes comparativos por región y periodo.

Se debe de poder hacer derribos o takedown hasta para 300 sitios que se llegén a identificar suplantado la imagen, marca, dominio, logo, nombre u actividad económica de la Federación Colombiana de Municipios.

Concentrador De Pentesting Vulnerabilidades

Un módulo concentrador de hallazgos de pentestest y vulnerabilidaes para analizar hasta 500 activos mediante un asistente estructurado en secciones de General, Severidad, Puertos y Vulnerabilidades. Admitir ingesta de resultados desde múltiples escáneres como Nessus, **Tenable**, entre otros que pueda usar la entidad durante el tiempo del servicio, normalizando los datos en un modelo unificado con campos de activo, servicio, puerto, CVE, severidad, estado y referencias. La plataforma debe deduplicar hallazgos entre fuentes para calcular vulnerabilidades totales y únicas, manteniendo la fuente de origen visible en cada registro. También soporta importaciones incrementales para actualizar evaluaciones existentes, validando la integridad de los archivos, durante doce (12) meses.

Que permite configurar políticas personalizadas de severidad, con escalas propias y mapeo a CVSS. Asimismo, establece criterios de inclusión o exclusión por puertos y servicios, programando evaluaciones recurrentes con seguimiento en calendario. Presenta vistas consolidadas por activos con distribución de severidad, listados de vulnerabilidades con detalles técnicos, vector CVSS, exploits disponibles y referencias externas. Los analistas pueden aplicar filtros avanzados, ordenar registros por múltiples campos y exportar resultados a CSV o Excel para conciliación o análisis adicional.

La solución debe soportar un ciclo de vida completo de estados (nueva, en análisis, confirmada, mitigada, remediada, falso positivo, aceptada), con trazabilidad de cambios, propietarios asignados y equipos responsables. Permite acciones masivas, integración con Gestión de Vulnerabilidades para planes de mitigación, y mantiener correlación de plugins (pruebas individuales) originales de escáneres. Incorpora RBAC, auditoría completa, cifrado en tránsito y en reposo, ofuscación de datos

sensibles y validación de consistencia en hallazgos. El sistema también deberá mostrar indicadores de productividad, SLA de análisis inicial y porcentaje de vulnerabilidades con dueño y plan en curso.

La solución facilitará la gestión operativa con notificaciones automáticas para vulnerabilidades críticas, configurables por equipo o severidad, además de plantillas predeterminadas para agilizar la creación de evaluaciones. Permitirá exportación de reportes ejecutivos con indicadores y anexos técnicos, incluyendo gráficos y tablas detalladas por activo. Soportará versiones en español e inglés. Además, ofrecerá vistas comparativas entre activos, deep links a vulnerabilidades específicas, y un asistente de configuración inicial para ejecutar la primera evaluación.

Gestionador De Hallazgos De Pentest Hacking

La solución de deberá contar con un backlog que permita visualizar los casos en estados abiertos, mitigados y remediados para hasta 500 activos. Ofrecerá vistas en tarjetas o tablas, coherencia gráfica con la escala de severidad, filtros avanzados y búsquedas por múltiples criterios, por doce (12) meses. También permitirá guardar y compartir vistas personalizadas, ordenar por diversos parámetros y asignar responsables de forma manual o automática. La trazabilidad debe estar garantizada con registros de cambios y visibilidad del propietario en todo momento.

La plataforma deberá gestionar prioridades por prioridades con plazos máximos parametrizables, calcular SLA, generar alertas de vencimiento y registrar indicadores de cumplimiento. Permitirá configurar recordatorios y escalamiento automático, con métricas de desempeño como MTTR, TTR de mitigación y remediación. Además, mostrará tendencias mensuales, distribución por edades de vulnerabilidades y ranking de activos críticos. El sistema dará soporte a reportes ejecutivos, anexos técnicos y exportación de métricas a CSV o Excel.

Cada hallazgo contará con planes de mitigación y remediación que incluyan hitos generados por inteligencia artificial, responsables, fechas y evidencias con validación de integridad. Se podrá dar seguimiento a su avance mediante semáforos y porcentajes completados, además de registrar comentarios, menciones y adjuntos. El detalle incluirá descripción técnica, vector CVSS, referencias, activo afectado y si existe exploit documentado. Asimismo, se permitirá aceptar riesgo, marcar falsos positivos o cerrar casos con evidencias verificadas. Todas las transiciones de estado estarán reguladas y auditadas.

La solución deberá integrarse con sistemas de gestión de incidentes o problemas si así se requiere. También permitirá generar notificaciones automáticas por correo o mensajería al detectar estados críticos. Contará con reglas simples “no-code” para autoasignación, etiquetado o escalamiento. Además, ofrecerá control de acceso por roles, auditoría completa de acciones, cifrado TLS 1.2 -1.3, ofuscación de datos sensibles y validación de flujos definidos por la organización.

Finalmente, la plataforma deberá asegurar facilidad de uso y alto rendimiento, soportando miles de registros con paginación eficiente. Ofrecerá deep links, panel de trabajo por analista, alertas visuales, excepciones con control de vencimiento y gestión de retención legal. Se permitirá configurar severidades y prioridades personalizadas, reglas de enrutamiento por unidad de negocio. Adicionalmente, incluirá soporte multilenguaje (español/ingles).

Hacking Etico Y Pentest

Permitir correlacionar hallazgos con catálogos como CISA KEV y EPSS, aplicando deduplicación, agrupamiento y mapeo a marcos OWASP, CWE y OWASP ASVS. También administra reglas de alcance, excepciones y riesgos aceptados.

Incluyendo cálculo de impacto empresarial combinando severidad técnica y dependencia del servicio, con soporte para CVSS 3.1 y métricas ambientales. El flujo contempla responsables automáticos, SLAs y RE-TESTS PROGRAMADOS.

Comparativos entre ciclos, panel de riesgos por aplicación, plantillas de informes ejecutivos y técnicos y heatmaps de riesgo. El sistema también integra filtros avanzados y búsquedas por CVE, CWE o propietario.

Trazabilidad con registro de comunicaciones, control de calidad, pruebas reproducibles y anexos. Además, contemplar exportación programada, control de acceso granular y catálogos de playbooks de remediación.

Validacion De Credenciales

Validar credenciales expuestas en fuentes como foros, paste sites y dark web, asegurando anonimización y técnicas de k-anonymity (modelo de protección de datos). Detecta reutilización de contraseñas y tokens comprometidos, priorizando por rol y criticidad.

Deduplicación por usuario, dominio y fecha, cálculo de prioridad operativa, y registro inmutable de evidencias con hash y sello de tiempo. Se incluye saneamiento automático de adjuntos para evitar exposición de PII.

Notificaciones en español o inglés si lo requieren. Se gestionarán excepciones, correlación con MFA y acceso condicional, además de procesos masivos por CSV/API para múltiples cuentas.

Panel ejecutivo con métricas, reportes descargables y simulaciones de drills. También soporta políticas de tenant, retención de datos, clasificación de información y reportes de motivos de cierre.

Aseguramiento De Código

Análisis PRs y commits con SAST, SCA, IaC y secretos, bloqueando merges con quality gates configurables. Además, detecta credenciales expuestas, genera SBOM y realiza escaneo de contenedores.

Con múltiples lenguajes de programación, auto-remediación asistida y onboarding masivo de repositorios. Se incluyen políticas por equipo, cacheo de resultados y análisis paralelo para grandes repositorios.

Simulaciones Red Team campañas phishing

Basados en MITRE ATT&CK, incluyendo phishing benigno, C2 controlado y técnicas de living-off-the-land. Permite medir detección con matrices de cobertura y heatmaps por campaña.

Las campañas se planifican con objetivos, ventanas y aprobaciones, generando recomendaciones priorizadas de hardening. Se incluye modo table-top, controles de seguridad y rollback inmediato del escenario.

El alcance se gestiona con listas de inclusión/exclusión, parametrización de escenarios y salvaguarda de datos mediante artefactos sintéticos. Se integra con EDR, SIEM y SOAR para recolección de hits.

Efectividad con KPIs de detección y respuesta, inyecta honeytokens y genera informes automáticos con evidencias verificables. También se sincroniza con inventarios dinámicos y sistemas de ITSM.

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.

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

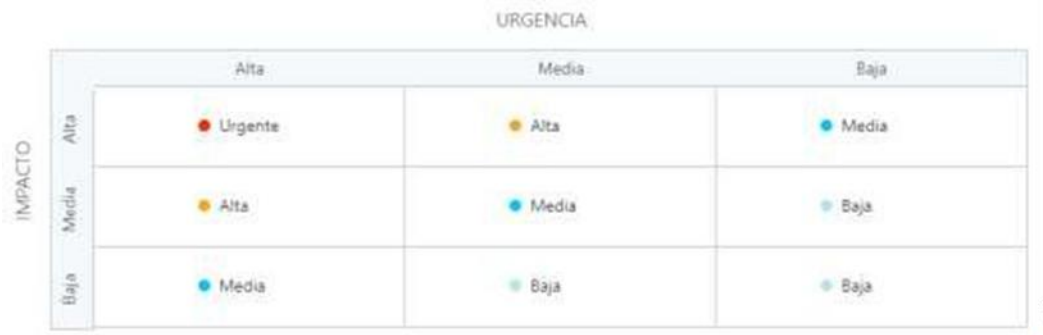
Matriz de prioridades

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 quince (15) días de ejecución, contado a partir del cumplimiento de los requisitos de ejecución y hasta el 27 de diciembre de 2026.

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: 1) certificación de activación de licenciamiento; 2) certificación de prestación de soporte de la herramienta por un año y; 3) certificación de haber realizado satisfactoriamente la transferencia de conocimiento, la cual deberá llevar el visto bueno del supervisor

del contrato.

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° 83 del archivo PAA 2026:

COD. SEGMENTO	COD. FAMILIA	COD. CLASE	COD. PRODUCTO	DESCRIPCIÓN	OBJETO A CONTRATAR
43	23	15	00	Software funcional especifico de la empresa	***Adquisición de una plataforma tecnológica bajo modelo SaaS para la gestión de riesgos y el fortalecimiento de la postura de seguridad, detección temprana de exposiciones de información en entornos digitales incluida Deep y Dark Web, y la prevención de suplantación de marca y phishing para de la Federación Colombiana de Municipios en cumplimiento de la función pública asignada.***
43	23	24	00	programas de desarrollo.	
43	23	29	00	Software para trabajo en redes	
43	23	32	00	Software de seguridad y protección	
43	23	37	00	Software de administración de sistemas.	

6. GARANTÍAS.

- Cumplimiento del contrato: Equivalente al diez por ciento (10%) del valor total del contrato de consultoría, por un término que cubra desde la fecha de suscripción del contrato 1 años y 15 más.

- Calidad del servicio: Equivalente al diez por ciento (10%) del valor total del contrato de consultoría, por un término que cubra desde la fecha de suscripción del contrato 1 años y 15 más.

- Pago de salarios, prestaciones sociales e indemnizaciones laborales: Equivalente al cinco por ciento (5%) del valor total del contrato de consultoría, por un término que cubra desde la fecha de suscripción del contrato 3 años y 15 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. EL CONTRATISTA autoriza a LA FEDERACIÓN el tratamiento de datos personales para dar cumplimiento con lo establecido en la Ley 1581 de 2012, reglamentada por el Decreto 1074 de 2015, 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/"
15. 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.
16. 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.

17. 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.
18. 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 proveedor se compromete a habilitar el licenciamiento y acceso al software y entregar las credenciales de acceso correspondientes dentro de un plazo no mayor a cinco días hábiles siguientes al cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato. La habilitación del licenciamiento y el acceso se considerará como entrega.

2. La plataforma suministrada deberá cumplir integralmente con las características, especificaciones técnicas, funcionalidades y demás requisitos establecidos en la ficha técnica que hace parte del presente proceso contractual.

3. Garantizar la disponibilidad continua del servicio SaaS durante doce (12) meses, asegurando una disponibilidad mínima del 99% y soporte técnico 7x24 en idioma español.

4. La plataforma deberá incorporar funcionalidades de actualización automática diaria de fuentes OSINT, deep web y dark web, orientadas a la identificación temprana de exposiciones de información, indicadores de compromiso y amenazas cibernéticas. La solución deberá permitir la consulta y generación de reportes que evidencien la ejecución de estas actualizaciones.

5. Proveer monitoreo permanente de hasta dos (2) dominios y a todos los subdominios, IP públicas asociadas a los dominios principales, repositorios y credenciales expuestas, con normalización de hallazgos.

6. Deberá tener implementadas medidas de seguridad de la información, garantizando cifrado AES-256 en reposo y TLS 1.2 y 1.3 en tránsito, con autenticación multifactor (OTP o 2FA), control de acceso basado en roles (RBAC) y gestión granular de roles y permisos por usuario, conforme a los estándares de seguridad definidos en la Ficha Técnica.

7. La solución deberá contar con funcionalidades para la generación, almacenamiento y consulta de evidencias asociadas a los hallazgos identificados, incorporando hash criptográfico y sello de tiempo que garanticen la integridad, autenticidad, trazabilidad y preservación de la cadena de custodia de la información.

8. Incorporar un motor de scoring de riesgos que utilice una metodología de evaluación basada en estándares internacionales reconocidos de la industria de ciberseguridad, que podrá ser cualquiera de los siguientes: NIST, CVSS 3.1, MITRE ATT&CK y OWASP, considerando criticidad, explotabilidad, impacto y contexto de negocio, y presentando métricas como time to shield, rankings y tendencias según las políticas de seguridad de la Entidad.

9. Ofrecer tableros ejecutivos y técnicos multilingües (inglés/español) con capacidad de exportar reportes en CSV, Excel o PDF y filtros configurables por severidad, fuente y estado.

10. Integrar la plataforma con sistemas de gestión existentes, incluyendo SIEM (Chronicle, QRadar, Splunk), ITSM (Jira, Aranda, ServiceNow), PAM (CyberArk, BeyondTrust, HashiCorp) y herramientas de vulnerabilidades (Nessus, Tenable, Crowdstrike).

11. El contratista debe realizar la transferencia de conocimiento con un mínimo de tres (3) horas distribuidas por bloque temático, dirigida a un grupo de tres (3) funcionarios designados por la Entidad, mediante sesiones teórico-prácticas con materiales actualizados en español. Las sesiones se estructurarán de acuerdo con cada módulo de la herramienta.

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.

En constancia, se firma en , a los., _____ de _____. de 26.

Firma representante legal del Proponente: _____

Nombre del R.L. _____

Nombre del Proponente: __

Dirección de correo electrónico: principal:

NIT: