INFORME DE SUPERVISION N.º 02

CONTRATO DE PRESTACIÓN DE SERVICIOS No. 2026-05

Contratante	Empresa Departamental para la Salud
Nit.	810.004.090-1
Contratista	JORGE WALTER SALAZAR AGUDELO
Nit. /C.C.	75.145.200 de Manizales
Valor	$ 19.633.320
Objeto	Administración y soporte de página WEB de la EMPRESA DEPARTAMENTAL PARA LA SALUD – EDSA y a los proyectos de seguridad de la información y gobierno digital.
Plazo	El plazo del contrato a partir de su legalización y hasta 31 de diciembre de 2026
Supervisor	Luisa Fernanda Quiñones Diaz – Profesional Administrativa y de Atención al Cliente
Suscripción del contrato	28/01/2026
Disponibilidad presupuestal	351 del 23 de enero de 2026
Registro Presupuestal	754 del 28 de enero de 2026
Pólizas	N/A
Impuesto de timbre	N/A

Se procede por parte del supervisor del contrato a verificar los aspectos relacionados con su cumplimiento y se verifica la entrega de los siguientes documentos:

1. Informe de las actividades realizadas durante el mes de **FEBRERO** de 2026, que contiene las siguientes acciones:

- **Políticas De Gobierno Digital**: Se publica en la página web institucional la información reglamentada por la Resolución 3564 de 2015: Reglamenta aspectos

relacionados con la Ley de Transparencia y Acceso a la Información Pública y la Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública.

- **Cumplir con los criterios de accesibilidad y usabilidad de la página web institucional de acuerdo con lo establecido en la Guía Interactiva de la Norma Técnica de Accesibilidad 5854.** Se cumple con los criterios de accesibilidad y usabilidad de la página web institucional de acuerdo con lo establecido en la Guía Interactiva de la Norma Técnica de Accesibilidad 5854 al **16%**

- **Contar con un formulario en su página Web para la recepción de peticiones, quejas, reclamos y denuncias**. Se cuenta con un formulario en la página web para la recepción de peticiones, quejas, reclamos y denuncias, el cual funciona sin inconvenientes.

- **Formular el Plan Estratégico de Tecnologías de Información (PETI), de acuerdo con el marco de referencia de Arquitectura Empresarial del Estado y según la Disponibilidad presupuestal.** Se formuló el Plan Estratégico de Tecnologías de Información (PETI), de acuerdo con el marco de referencia de Arquitectura Empresarial del Estado para la vigencia 2026. Con algunas actividades sujetas a Disponibilidad presupuestal **al 100%**

- **Actualizar la guía para la definición del portafolio de servicios de TI del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI, según la Disponibilidad presupuestal.** Seguridad y Protección de Datos: se Implementó Backup Automáticos para proteger la información relacionada con los documentos donde reposan las legalizaciones de las rifas. **al 16%**

- **Implementar dentro de sus sistemas de información la guía de estilo y las especificaciones técnicas de usabilidad definidas por la Entidad y el Ministerio de TIC.** Adopción de Principios de Accesibilidad Web, Actualizaciones según auditoria ITA por procuraduría según cumplimiento Transparencia y acceso a la información pública **al 16%**

- **Implementar un programa de correcta disposición final de los residuos tecnológicos**. Actualmente se gestiona con la empresa ColobiaNet Solutions SAS NIT 900.712.192.6 para la recolección y almacenamiento y tratamiento de residuos de aparatos eléctricos y Pilas. Programa de residuos tecnológicos en construcción **al 16%**

- **Implementar la política de reducción del uso del papel.** Actualmente la política se encuentra publicada y en implementación

- **Incorporar soluciones tecnológicas para la gestión de documentos con base en: a. El análisis de los procesos de la Entidad, b. La reducción del uso del papel, c. Criterios de seguridad, disponibilidad y conservación de los documentos. d. Establecer el plan de mantenimiento de servicios tecnológicos. e. Generar un documento de diagnóstico, donde se identifica de manera clara el estado actual de la entidad en la implementación de Seguridad y Privacidad de la Información.** Se implementa copias automáticas de programa Fortuner y de documentación vital para el funcionamiento de la entidad, se guardan en disco externo fuera de la entidad y copias en Google Drive. Se automatizan copias.

- **Establecer la política de seguridad y privacidad de la información.** Revisión de Políticas Específicas del SGSI, En el marco del proceso de mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) y conforme a los lineamientos establecidos en el ciclo PHVA del Modelo de Seguridad y Privacidad de la Información, se inició la revisión técnica de las políticas específicas vigentes de la entidad.

  Las políticas actualmente en evaluación incluyen, entre otras: Política de Dispositivos Móviles, Política de Uso Aceptable de Activos, Política de Usos Tecnológicos de Comunicación y Acceso a Internet, Política de Control de Acceso, Política de Uso de Controles Criptográficos, Política de Escritorio Limpio y Pantalla Limpia, Política de Copias de Respaldo, Política de Transferencia de Información, Política de Desarrollo Seguro, Política de Relación con Proveedores, Política Cero Papel, El objetivo de esta revisión es: Verificar su alineación con la normativa vigente.
  Evaluar su coherencia con los riesgos actuales identificados en la organización, Determinar cuáles requieren actualización, fortalecimiento o ajustes técnicos, Confirmar cuáles continúan vigentes sin necesidad de modificación.

  Este ejercicio permite garantizar que las políticas del SGSI se mantengan actualizadas, pertinentes y acordes con el contexto interno y externo de la entidad, asegurando el fortalecimiento continuo de la seguridad de la información.

- **Construir documento o manual con las políticas de seguridad y privacidad de la información. Se implementa copias automáticas de programa Fortuner y de documentación vital para el funcionamiento de la entidad, con el fin de mitigar**

una eventual perdida de información, manejo de permisos para manejo de archivos y programas. Programa de residuos tecnológicos en construcción.

- **Desarrollar una metodología de gestión de activos que le permita generar un inventario de activos de información.** Se estableció el plan de mantenimiento de servicios tecnológicos.

- **Definir una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, así como la declaración de aplicabilidad.** Para la adecuada estructuración e implementación de esta metodología se requiere la asignación de recursos técnicos, operativos y financieros que actualmente no se encuentran disponibles en la entidad. Por el momento esta actividad no se ejecuta en este periodo

- **Definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) de la entidad.** Sensibilizar a los empleados sobre la importancia de la seguridad de la información en sus funciones diarias.

Crear una campaña de comunicación interna con mensajes clave y recordatorios constantes.

- **Identificar los riesgos inherentes de seguridad digital, se debe tener en cuenta las amenazas y las vulnerabilidades asociadas a cada activo. Una vez identificados los riesgos inherentes de seguridad digital para cada activo identificado, se deben determinar la probabilidad e impacto de los criterios establecidos, durante la fase de planeación. •** Se venía realizando la identificación de riesgos inherentes en seguridad digital mediante la herramienta Wazuh, incluyendo análisis de amenazas y vulnerabilidades asociadas a ataques cibernéticos, errores humanos y fallas tecnológicas. No obstante, la actividad no pudo continuar debido a que el equipo de cómputo que operaba como servidor se encuentra deshabilitado por daño técnico. La reimplementación del servicio quedará sujeta a la disponibilidad presupuestal de la entidad.

- Establecer los criterios para definir el o los tratamientos de los riesgos, dependiendo del nivel residual obtenido de seguridad digital. Revisión de criterios como:

- Cifrado de datos sin clave robusta, Aplicar 2FA obligatorio en accesos críticos., Habilitar cifrado de datos en dispositivos sensibles (Vera Crypt). Certificado SSL

2. Cuenta de cobro del 25 de febrero de 2026

3. Declaración juramentada para efectos tributarios, sistema de determinación del impuesto sobre la renta de las personas naturales.

4. Planilla de seguridad social N° 35900048 correspondiente al mes de enero de 2026.

De esta manera se ha constatado que el contratista ha dado cumplimiento a las obligaciones suscritas en el contrato.

RESUMEN DE PAGOS

VALOR TOTAL DEL CONTRATO	$ 19.633.320
VALOR DEL ACTA N° 2	$ 1.636.110
VALOR EJECUTADO	$ 3.272.220
VALOR SIN EJECUTAR	$ 16.361.100
SALDO A FAVOR DEL CONTRATISTA	$ 16.361.100

Para constancia se firma en la ciudad de Manizales a los veinticinco (25) días del mes de febrero de 2026.

LUISA FERNANDA QUIÑONES DIAZ
Profesional administrativa y de atención al cliente