OBJETO: "CONTRATAR SERVICIOS ESPECIALIZADOS PARA APOYAR LA DEFINICIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - MSPI, EN UNA (1) INSTITUCION EDUCATIVA OFICIAL DEL DEPARTAMENTO DEL TOLIMA "	
Contratista/ Cooperante/ Proveedor:	IDENTIAN S.A.S
NIT/ CC:	900.678.711-3
	Del 26/10/2025 al 26/11/2025

Este documento hace parte de los productos a entregar en el marco del Contrato No 2767 del 11 de agosto de 2025, dentro del cual se incluyen los entregables 5, 6, 7 y 8 del Anexo 2, realizados en la ciudad de Espinal del Departamento del Tolima y requeridos para la segunda facturación y pago.

1. OBJETIVO

Presentar el informe sobre la ejecución de las actividades realizadas para apoyar los entregables 5, 6, 7 y 8 del Modelo de Seguridad y Privacidad de la Información (MSPI) en una institución educativa oficial del departamento del Tolima, describiendo las acciones desarrolladas en cumplimiento de los entregables 5, 6, 7 y 8 del Contrato No 2767 del 11 de agosto de 2025.

2. ACTIVIDADES DESARROLLADAS DE LOS ENTREGABLES 5, 6, 7 y 8

Durante el mes de octubre del 2025, se realizaron las siguientes actividades:

ENTREGABLE	ACTIVIDADES REALIZADAS y EVIDENCIAS	EVIDENCIAS
Riesgos de seguridad de la información para la institución educativa.	Para desarrollar estos entregables se realizaron las siguientes actividades: 1. Análisis del inventario y clasificación de los activos de información de la institución San Isidoro – Espinal. 2. Para los activos de información identificados y clasificados como	Se entregó la documentación que contiene la descripción los riesgos y controles de seguridad de información para la institución Educativa San Isidoro – Espinal. Los riesgos y controles identificados fueron socializados el día 1 de diciembre de 2025.

ENTREGABLE	ACTIVIDADES REALIZADAS y EVIDENCIAS	EVIDENCIAS
	reservados, se realizaron el análisis, evaluación y los controles que permita establecer las iniciativas y actividades que permitan mitigar riesgos y proteger los activos críticos sensibles de la Institución Educativa. 3. Los riesgos y controles identificados fueron socializados el día 1 de diciembre de 2025.	Se revisaron , determinaron y explicaron las medidas y controles que deben tener para proteger: - La Información de Matrículas, desde la inscripción hasta la graduación, para garantizar el registro único y la cobertura del sistema educativo nacional. - Información de Convivencia Escolar con seguimiento de casos de acoso, violencia escolar y vulneración de derechos de niños, niñas y adolescentes en la Institución Educativa. - Información para el Monitoreo, la Prevención y el Análisis de la Deserción Escolar. - Información de notas, constancias de estudio, paz y salvo, carnets estudiantiles, menciones de honor. - Información académica personal del estudiante, celular, acudientes, Tarjeta de identidad, foto, RH, dirección, teléfono, información del acudiente; salud y actividad social, capacidades y talentos; discapacidades si las tiene y hobbies. -Alimentación escolar; PAE; beneficiario y los que repiten (relocalizados). - Archivo físico donde se conservan la documentación confidencial y datos personales estudiantes, docentes y personal administrativo.
Gestión y manejo de incidentes de seguridad de la información para para la institución educativa.	Se diseño el procedimiento que permitirá la gestión y manejo de incidentes de seguridad de la información para la institución educativa. Este documento fue socializado el 1 de diciembre del 2025 a los docentes y personal administrativo de la institución educativa.	Se entregó el procedimiento de Gestión y manejo de incidentes de seguridad de la información para para la institución educativa. Con este procedimiento le permitirá a los docentes y personal administrativo reportar cualquier evento que afecte la información de la Institución Educativa. También, permitirá identificar, reportar, analizar, contener, erradicar, recuperar

ENTREGABLE	ACTIVIDADES REALIZADAS y EVIDENCIAS	EVIDENCIAS
		y documentar los incidentes de seguridad de la información que afecten a estudiantes, docentes, personal administrativo, infraestructura tecnológica, datos académicos o servicios críticos de la Institución Educativa San Isidoro - Espinal.
Guía de ciberseguridad y seguridad de la información para la institución educativa.	Se diseñaron las guías de ciberseguridad y seguridad de la información para la institución educativa San Isidoro - Espinal, que permitirán establecer los lineamientos necesarios para la proteger la información, entre ellas contenidos de sensibilización y los lineamientos para el personal y estudiantes.	Se diseñaron dos guías de ciberseguridad y seguridad de la información. La primera guía está orientada a presentar los conceptos y definiciones principales de la seguridad y privacidad de la información, entre ellas están las siguientes: - Principios de la seguridad de la información - Amenazas internas y externas de la información - Explicación de cómo controlar los malware, Phishing, Ingeniería social, secuestro de información (ransomware), denegación de servicio, botnet, exploit, entre otros. - Riesgos en redes sociales y chats - Navegación segura en Internet - Activos de información - Riesgos de la Seguridad de la información - Uso del correo electrónico - Escritorios limpios - Contraseñas seguras - Control de acceso - Suplantación de usuarios - Sesiones abiertas - Respaldo y/o Backup de la información La segunda guía está orientada a presentar el modelo de seguridad y privacidad de la información, y para ello, se presentaron las siguientes definiciones: • Política de Responsabilidades frente a la Seguridad de la Información

ENTREGABLE	ACTIVIDADES REALIZADAS y EVIDENCIAS	EVIDENCIAS
		- Define deberes de docentes, administrativos, estudiantes y contratistas. - Ejemplo: cuidado de contraseñas, custodia de equipos, reporte de incidentes. • Política de Uso Aceptable de Activos de Información - Reglas sobre el uso de computadores, internet institucional, correo, dispositivos móviles. - Incluye pautas para estudiantes y personal. • Política de Clasificación y Manejo de la Información - Diferencia entre información pública, interna y confidencial (ejemplo: datos académicos y personales de estudiantes). - Establece controles básicos de acceso y archivo. • Política de Control de Acceso - Quién tiene acceso a qué información (bases de datos, historiales, carpetas digitales). - Manejo de usuarios y contraseñas en sistemas internos. • Política de Seguridad Física y del Entorno - Controles sobre acceso a salas de informática, archivos físicos y equipos. - Incluye medidas básicas contra robos, incendios, daños ambientales. • Política de Escritorio Limpio y Pantalla Limpia - Buenas prácticas: no dejar información sensible a la vista, bloquear pantallas. - Sencilla de implementar y de gran valor pedagógico. • Política de Cumplimiento y Manejo de Datos Personales • Alineada con la Ley 1581 de 2012 (Ley de Protección de Datos Personales de Colombia,).

ENTREGABLE	ACTIVIDADES REALIZADAS y EVIDENCIAS	EVIDENCIAS
		• Reglas sobre el tratamiento de datos de estudiantes y familias. • Política de Gestión de Incidentes de Seguridad - Procedimiento básico para reportar incidentes (pérdida de documentos, fuga de información, accesos indebidos). - La institución reporta y la Secretaría coordina con autoridades competentes. • Política de Seguridad de Recursos Humanos - Confidencialidad en contratos, inducción a docentes/administrativos, cláusulas disciplinarias. • Política para Usuarios y Estudiantes en el uso de TIC - Buenas prácticas en uso de plataformas educativas, correo institucional, redes sociales. - Promueve formación ciudadana digital. • Política Para Manejo De Gestión De Proveedores - Exigir a proveedores el conocimiento y aceptación de las políticas y procedimientos de seguridad y privacidad de la información de la institución educativa. - Incluir en los contratos con los proveedores cláusulas que garanticen el cumplimiento de los requisitos, obligaciones y responsabilidades en materia de protección de la información de la institución educativa. - Incluir cláusulas de auditoría, revisión y monitoreo de cómo el proveedor maneja la información.
Sensibilización de seguridad de la información y ciberseguridad	Se realizó un taller de sensibilización de seguridad de la información y ciberseguridad para los directivos, personal administrativo y docentes de la entidad educativa el día 1 de	Se generaron videos que soportan y evidencian la realización del taller de sensibilización en la instalación educativa San Isidoro – Espinal

ENTREGABLE	ACTIVIDADES REALIZADAS y EVIDENCIAS	EVIDENCIAS
	diciembre en la instalación Educativa San Isidoro, desde las 6:30 AM y 9:00 AM,	Se generó la firma de asistencias del rector, líder académico, secretarias, líder de convivencia y el responsable de la gestión administrativa, financiera y humana de la Institución Educativa. Se realizó la presentación de las guías de ciberseguridad y modelo de seguridad y privacidad de la información. Se resalta el compromiso del rector de la institución educativa San Isidoro - Espinal, ya que generó la participación de un gran numero de docentes y personal administrativo de la Institución Educativa, y esta generó el interés y participación del personal.