	ESE UNIVERSITARIA DEL ATLANTICO FORMATO PLANES INSTITUCIONALES Y ESTRATEGICOS	CODIGO: FT - PE - 002 VIGENCIA: Enero - 2026 VERSION: 3

1. PLAN: PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | **2. PERIODO: 2026**

3. OBJETIVO: Garantizar la confidencialidad, integridad y disponibilidad de la información de la E.S.E. Universitaria del Atlántico mediante la implementación de controles y acciones que permitan gestionar los riesgos, asegurar el cumplimiento de la normativa vigente y fortalecer las prácticas de seguridad y privacidad entre los colaboradores.

4. ÍTEM	5. OBJETIVO ESPECIFICO	6. ACTIVIDAD	7. RESPONSIBLE	8. CRONOGRAMA DE ACTIVIDADES												9. META	10. INDICADOR	11. METODOLOGÍA DE CÁLCULO / UNIDAD DE MEDIDA	12. SOPORTE DE VERIFICACION
				ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC				
1	•Establecer controles para mitigar los riesgos identificados.	Implementar controles técnicos, administrativos y procedimentales para mitigar los riesgos identificados, de acuerdo con la matriz de riesgos institucional.	Director TICS													90%	Porcentaje de implementación de controles para mitigación de riesgos	(Número de controles implementados / Número de controles definidos) × 100	Matriz de riesgos actualizada, planes de tratamiento del riesgo, informes de seguimiento, actas de implementación y evidencias documentales.
2	•Proteger los datos personales conforme a la normativa vigente.	Implementar y fortalecer los controles y procedimientos para la protección de los datos personales, garantizando el cumplimiento de la Ley 1581 de 2012, sus decretos reglamentarios y las políticas institucionales de tratamiento de la información.	Director TICS													90%	Nivel de cumplimiento en la protección de datos personales	(Número de requisitos de protección de datos implementados / Número total de requisitos aplicables) × 100	Política de tratamiento de datos personales, registros de bases de datos, autorizaciones de titulares, informes de auditoría, actas de seguimiento y evidencias documentales.
3	· Garantizar la continuidad y confia	Implementar y mantener mecanismos de respaldo, recuperación y control de la información que garanticen su continuidad, disponibilidad y confiabilidad ante incidentes o fallas operativas	Director TICS													90%	Nivel de cumplimiento de los mecanismos de continuidad y confiabilidad de la información	(Número de mecanismos implementados y operativos / Número total de mecanismos definidos) × 100	Políticas y procedimientos de respaldo y recuperación, bitácoras de copias de seguridad, planes de continuidad, pruebas de restauración, informes técnicos y actas de seguimiento.
4	•Fortalecer la cultura de seguridad de la información.	Diseñar e implementar un programa de sensibilización y capacitación en seguridad de la información dirigido a los servidores y contratistas de la entidad, con el fin de fortalecer las buenas prácticas en el manejo de la información.	Director TICS													90%	Nivel de fortalecimiento de la cultura de seguridad de la información	(Número de actividades de sensibilización ejecutadas / Número de actividades programadas) × 100	cronogramas de capacitación, listas de asistencia, material de divulgación, y evidencias documentales

Aprobó: **MIGUEL ANGEL RODRIGUEZ HERAZO**
Cargo: **DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES**
Área: **TICS**