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

1. PLAN: PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION | **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	Planificar, implementar y hacer seguimiento a un cronograma estructurado bajo el ciclo de mejora continua (PHVA), que permita la adopción progresiva e integral del Modelo de Seguridad y Privacidad de la Información (MSPI) en todos los procesos y áreas de la E.S.E.	Realizar diagnóstico del estado actual de la seguridad de la información en la E.S.E.UNA.	Director TICS													100%	Diagnóstico del estado actual de la seguridad de la información en la E.S.E. UNA	Diagnóstico del estado actual de la seguridad de la información en la E.S.E. UNA	Informe Diagnostico de situación actual
2	Implementar, verificar y mantener los controles de seguridad y privacidad definidos en el MSPI, con base en los riesgos identificados, garantizando una gestión efectiva de la seguridad de la información y la protección de los datos institucionales.	Implementar la política general de seguridad y privacidad de la información.	Director TICS													60%	Capacitación al personal la ESE UNA que tiene acceso a información administrativa y/o asistencial	Personal Capacitado / Personal vinculado	Acta de capacitación Listado de Asistencia
3	Realizar auditorías y evaluaciones periódicas de cumplimiento, con el fin de medir la eficacia del MSPI, identificar oportunidades de mejora y asegurar su alineación con la normativa vigente y los lineamientos institucionales	Identificar y establecer roles y responsabilidades en materia de seguridad de la información en DGH	Director TICS													100%	Porcentaje de verificación de necesidades reales, roles y permisos del usuario dentro del Sistema de información Dinámica Gerencial	Cantidad de usuarios Verificados/Cantidad de usuarios activos en DGH * 100	Informe de verificación de usuarios en el sistema de información
4	Realizar auditorías y evaluaciones periódicas de cumplimiento, con el fin de medir la eficacia del MSPI, identificar oportunidades de mejora y asegurar su alineación con la normativa vigente y los lineamientos institucionales	Desarrollar un plan de capacitación y sensibilización para el personal en seguridad y privacidad de la información	Director TICS													60%	Capacitación al personal la ESE UNA que tiene acceso a información administrativa y/o asistencial	Personal Capacitado / Personal vinculado	Acta de capacitación Listado de Asistencia
6	Realizar auditorías y evaluaciones periódicas de cumplimiento, con el fin de medir la eficacia del MSPI, identificar oportunidades de mejora y asegurar su alineación con la normativa vigente y los lineamientos institucionales	Realizar auditorías internas de seguridad de la información	Director TICS													100%	Ejecución de auditorías internas de seguridad de la información	(Número de auditorías internas realizadas / Número de auditorías internas programadas) × 100	informes de auditoría interna, actas de cierre, planes de mejora y evidencias documentales de seguimiento.
8	•Implementar, verificar y mantener los controles de seguridad y privacidad definidos en el MSPI, con base en los riesgos identificados, garantizando una gestión efectiva de la seguridad de la información y la protección de los datos institucionales.	Realizar restauración en empresa pruebas de los backups que se realizan a la base de datos para comprobar su integridad y veracidad de los datos ante posibles ataque cibernéticos.	Director TICS													100%	Realizar una restauración semanal de un backups de la base de datos de producción para garantizar la continuidad del servicio	(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.

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