PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ESE UNIVERSITARIA DEL ATLÁNTICO

TABLA DE CONTENIDO

1. INTRODUCCIÓN

En un entorno donde la información se ha convertido en un recurso estratégico para la operación eficiente de las organizaciones, garantizar su seguridad y privacidad es fundamental. La E.S.E. Universitaria del Atlántico reconoce la importancia de proteger los datos de sus pacientes, colaboradores y operaciones internas frente a riesgos que podrían comprometer su confidencialidad, integridad y disponibilidad. El **Plan de Seguridad y Privacidad de la Información (PSPI) 2025** pretende fortalecer la gestión de la seguridad de la información mediante acciones concretas, alineadas con las normativas vigentes, como la Resolución 500 de 2021 y la Ley 1581 de 2012, además de los estándares internacionales en la materia.

El Modelo Integrado de Planeación y Gestión (MIPG), actúa como un marco de referencia que orienta a las entidades y organismos públicos en la dirección, planificación, ejecución, seguimiento, evaluación y control de sus actividades. Su objetivo es producir resultados que respondan a los planes de desarrollo y aborden las necesidades y problemas de los ciudadanos, garantizando integridad y calidad.

MIPG se convierte en una herramienta fundamental para el desarrollo e implementación del PSPI porque proporciona un marco general para la gestión y la planificación, ambos modelos promueven una cultura de seguridad y responsabilidad dentro de la Entidad. La implementación de un PSPI efectivo es visto como un componente dentro del MIPG, donde la seguridad de la información se convierte en un proceso clave que debe ser gestionado de manera integrada con otros procesos organizacionales. La colaboración entre ambos es esencial para lograr objetivos organizacionales efectivos y seguros.

Así las cosas, se presenta a continuación un Plan diseñado para abarcar todos los aspectos de la seguridad física, lógica y normativa, buscando no solo mitigar riesgos, sino también establecer una cultura organizacional de protección de datos, asegurando el cumplimiento de las responsabilidades legales y éticas de la E.S.E., proporcionando confianza a todos sus usuarios y partes interesadas.

2. ALCANCE

El Plan de Seguridad y Privacidad de la Información 2025 de la E.S.E. Universitaria del Atlántico abarca todos los procesos, sistemas, infraestructuras tecnológicas y personal que participan en la gestión de la información dentro de la entidad. Contempla los siguientes componentes de un Modelo de Seguridad de la Información:

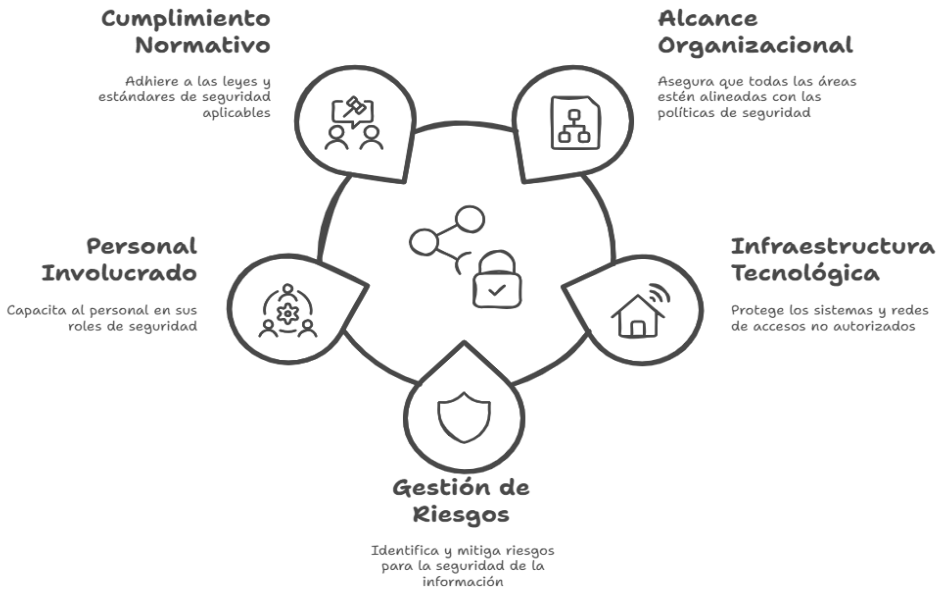

Imagen 1. *Componentes de un Modelo de Seguridad de la Información.*

3. OBJETIVOS

3.1. GENERAL

Proteger la confidencialidad, integridad y disponibilidad de la información en la E.S.E Universitaria del Atlántico, estableciendo un marco estratégico que garantice la gestión adecuada de los riesgos asociados, cumpliendo con las normativas vigentes y promoviendo una cultura de seguridad y privacidad entre todos los colaboradores.

3.2. ESPECÍFICOS

- Diseñar y ejecutar un cronograma estructurado basado en el ciclo de mejora continua para lograr la adopción integral del MSPI en todos los procesos y áreas de la E.S.E.
- Implementar y verificar controles de seguridad y privacidad previstos en el MSPI, fundamentados en los riesgos identificados, para garantizar una gestión efectiva de la seguridad de la información.
- Establecer un programa de formación y sensibilización dirigido a los colaboradores de la E.S.E., que permita fomentar una cultura organizacional orientada a la seguridad y privacidad de la información.
- Realizar auditorías periódicas y análisis de cumplimiento para evaluar la eficacia del MSPI, identificando áreas de mejora y asegurando la alineación con las normativas vigentes.

4. RESPONSABLES DEL DESARROLLO DEL PLAN

4.1. COMITÉ DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Liderará la planificación, implementación, monitoreo y evaluación del Plan. Este comité incluye representantes de áreas claves, como:

- **Director de TIC**: Responsable de supervisar las iniciativas tecnológicas y garantizar la implementación técnica de las medidas de seguridad.

- **Director Talento Humano**: Diseñar, implementar y gestionar estrategias de capacitación, sensibilización y asignación de roles para fomentar una cultura organizacional alineada con las políticas de seguridad y privacidad de la información.

- **Dirección Financiera**: Garantizar la asignación y administración eficiente de los recursos financieros necesarios para implementar las medidas del Modelo de Seguridad y Privacidad de la Información, asegurando su sostenibilidad económica.

- **Jefe Oficina Asesora de Planeación**: Encargado de alinear las actividades del Plan con los objetivos estratégicos de la E.S.E.

- **Jefe Oficina Control Interno**: Monitoreará el cumplimiento del Plan y la efectividad de los controles establecidos.

- **Jefe Oficina Asesora Jurídica**: Velar por el cumplimiento legal y normativo del Plan de seguridad y privacidad de la información, incorporando cláusulas y lineamientos en todos los procesos contractuales y asesorando en casos de implicaciones legales.

- **Líder de Proceso de Gestión Documental**: Asegurará la correcta gestión de la información física y digital, conforme a las normativas de seguridad.

- **Líder de los procesos de los Sistemas de Gestión de Calidad**: Verificará la integración de las medidas de seguridad en los procesos de mejora continua.

4.2. EQUIPO DE SEGURIDAD DE LA INFORMACIÓN TICS

Este equipo ejecutará las actividades operativas del Plan, como la implementación de controles técnicos, gestión de riesgos, y monitoreo de incidentes.

4.3. DIRECTORES Y COORDINADORES DE ÁREAS

Garantizarán la aplicación de las políticas y controles de seguridad dentro de sus respectivas áreas. Participarán en actividades de sensibilización y en la evaluación de riesgos asociados a los procesos bajo su responsabilidad.

4.4. PERSONAL ADMINISTRATIVO Y ASISTENCIAL:

Cumplirá con las políticas, procedimientos y capacitaciones relacionadas con el Plan. Su participación es clave para fomentar una cultura de seguridad de la información.

4.5. PROVEEDORES Y TERCEROS CONTRATISTAS:

Serán responsables de cumplir con las cláusulas contractuales relacionadas con la seguridad y privacidad de la información en los servicios proporcionados.

5. MARCO LEGAL Y NORMATIVO

El Plan de Seguridad y Privacidad de la Información para la E.S.E. Universitaria del Atlántico estará fundamentado en las siguientes disposiciones legales y normativas, que establecen los lineamientos y obligaciones relacionadas con la protección de la información:

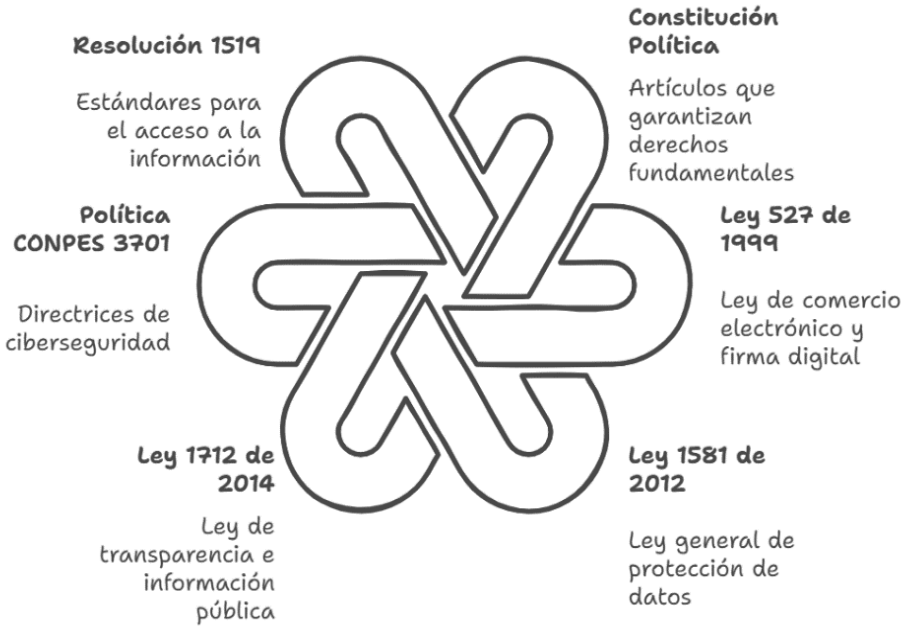

Imagen 2. *Marco legal integral para la protección de datos.*

Normatividad Constitucional		
Constitución Política de Colombia	**Artículo 15**	Reconoce como derecho fundamental el *Habeas Data*.
	Artículo 20	Garantiza la libertad de información y acceso a datos públicos.
Normas Generales sobre Seguridad y Protección de Datos		
Ley 1581 de 2012	Régimen general de protección de datos personales.	
Decreto 1377 de 2013	Reglamenta parcialmente la Ley 1581 de 2012.	
Ley 1266 de 2008	Regula el manejo de información financiera y crediticia en bases de datos personales.	
Ley 1273 de 2009	Crea el bien jurídico de "Protección de la Información" y establece delitos informáticos.	
Decreto 886 de 2014	Reglamenta el artículo 25 de la Ley 1581 de 2012, relacionado con la transferencia internacional de datos.	
Normas sobre Transparencia y Acceso a la Información Pública		
Ley 1712 de 2014 (Ley de Transparencia)	Regula el acceso a la información pública bajo principios de seguridad y confidencialidad	
Resolución 1519 de 2020	Define estándares y directrices para la publicación de información pública, accesibilidad web, seguridad digital y datos abiertos	
Directiva 026 de 2020	Establece lineamientos para el diligenciamiento del Índice de Transparencia y Acceso a la Información (ITA)	
Normas sobre Seguridad Digital y Tecnologías de la Información		
Ley 1341 de 2009	Promueve el desarrollo y uso de las tecnologías de información y comunicación (TIC)	
Decreto 1078 de 2015	Compendio reglamentario del sector TIC, incluye aspectos de gobierno electrónico y seguridad digital	
Decreto 1008 de 2018	Establece lineamientos generales para la política de Gobierno Digital	
Ley 1480 de 2011	Protección al consumidor en transacciones electrónicas	
Normas Relativas al Manejo de Archivos Electrónicos		
Ley 594 de 2000	(Ley General de Archivos): Regula la organización y conservación de archivos públicos y privados.	

Decreto 2609 de 2012	Reglamenta el expediente electrónico en las entidades públicas
Política Pública Nacional	
CONPES 3701 de 2011	Lineamientos para Ciberseguridad y Ciberdefensa
CONPES 3854 de 2016	Política Nacional de Seguridad Digital
CONPES 3975 de 2019	Política Nacional de Transformación Digital e Inteligencia Artificial
Normas Sectoriales Específicas	
Circular Externa 005 de 2017	(Superintendencia de Salud): Obligación de las E.S.E. de proteger la información de los pacientes en la historia clínica
Ley 1150 de 2007	Seguridad en la información electrónica durante la contratación pública

Tabla 1. *Normatividad PSPi*

6. MARCO CONCEPTUAL Y TEÓRICO

6.1. DEFINICIONES

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema.
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **Autorización**: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
- **Bases de Datos Personales**: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida.
- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos**: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).
- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- **Datos Personales Mixtos**: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles**: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI.
- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)
- **Gestión de incidentes de seguridad de la información:** procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado

de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **Modelo de Seguridad y Privacidad de la Información (MSPI):** El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- **Privacidad**: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25).
- **Responsabilidad Demostrada:** Conducta desplegada por los responsables o encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Seguridad de la información**: Preservación de la confidencialidad, integridad, y disponibilidad de la información.

- **Sistema de Gestión de Seguridad de la Información SGSI**: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

6.2. ABREVIATURAS

- **SI:** Seguridad de la información
- **GDA:** Gestión Documental y Archivo
- **ITEP:** Índice de Transparencia en Entidades Públicas
- **MSPI:** Modelo de Seguridad y Privacidad de la Información
- **PROC:** Procedimientos documentados
- **RRHH:** Recursos humanos
- **SGSI:** Sistema de Gestión de Seguridad de la Información

7. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La E.S.E. Universitaria del Atlántico desarrolla su Plan de Seguridad y Privacidad de la Información en alineación con los marcos legales y conceptuales establecidos por el Estado, asegurando el cumplimiento de los objetivos definidos en este plan. El PSPI se articula en cinco fases principales, detalladas a continuación:

- FASE I: DIAGNÓSTICO
- FASE II: PLANIFICACIÓN
- FASE III: IMPLEMENTACIÓN
- FASE IV: EVALUACIÓN DE DESEMPEÑO

- FASE V: MEJORA CONTINUA

Imagen 3. *Fases PSPI*

FASE	OBJETIVO	ACTIVIDADES
DIAGNÓSTICO	Identificar el estado actual de la entidad en relación con los requerimientos del Modelo de Seguridad y Privacidad de la Información (MSPI).	• Evaluación del cumplimiento normativo vigente. • Análisis de brechas frente al MSPI. • Identificación de riesgos asociados a la seguridad de la información. • Levantamiento del inventario de activos de información críticos.

PLANIFICACIÓN	Establecer las bases del MSPI mediante la definición de políticas, objetivos, procesos y procedimientos de seguridad que gestionen eficazmente los activos de información.	• Redacción y aprobación de la política de Seguridad y Privacidad de la Información. • Definición de objetivos alineados con las políticas globales de la entidad. • Diseño de procesos y procedimientos para la gestión de la seguridad de la información. • Identificación de recursos necesarios para implementar el MSPI.
IMPLEMENTACIÓN	Operar el MSPI conforme a lo planificado, ejecutando los procesos y procedimientos definidos.	• Implementación de controles de seguridad en los activos de información. • Capacitación del personal sobre políticas y procedimientos de seguridad. • Configuración y despliegue de herramientas tecnológicas para proteger la información. • Gestión de incidentes de seguridad de forma efectiva.
EVALUACIÓN Y DESEMPEÑO	Monitorear y evaluar el desempeño del MSPI, verificando su eficacia frente a los objetivos establecidos.	• Realización de auditorías internas del MSPI. • Medición del cumplimiento de los procesos contra los objetivos y políticas definidos. • Revisión de los resultados por parte de la dirección. • Identificación de oportunidades de mejora basadas en la experiencia práctica y los resultados de las auditorías.
MEJORA CONTINUA	Garantizar la sostenibilidad y mejora continua del MSPI a través de ajustes derivados de las auditorías internas y la retroalimentación de la dirección.	• Implementación de acciones correctivas y preventivas basadas en los resultados de las auditorías.

		• Actualización de políticas y procedimientos según cambios normativos o tecnológicos. • Promoción de una cultura organizacional orientada a la seguridad de la información. • Documentación de mejoras realizadas para asegurar la trazabilidad.

Tabla 2. *Fases PSPI*

8. CICLO DE OPERACIÓN DEL MSPI

La E.S.E. Universitaria del Atlántico adopta y aplica el modelo de seguridad y privacidad de la información mediante un ciclo de operación compuesto por cinco (5) fases descritas anteriormente, diseñado para gestionar de manera integral la protección de los activos de información de la entidad. Este modelo contempla seis (6) niveles de madurez, los cuales representan la evolución progresiva en la implementación de prácticas orientadas a la gestión eficiente de la seguridad y privacidad de la información.

La seguridad y privacidad de la información están alineadas con el componente de TIC para servicios, garantizando el manejo adecuado de la información empleada en los trámites y servicios ofrecidos por la E.S.E UNA, respetando en todo momento las disposiciones legales sobre la protección de datos personales, así como otros derechos establecidos por la normativa vigente que regula el acceso restringido a información pública.

De igual manera, el componente de TIC para Gobierno en Línea se encuentra integrado con el componente de Seguridad y Privacidad de la Información, promoviendo la construcción de una E.S.E. más transparente, colaborativa y participativa. Esto se logra mediante la implementación de controles que aseguran la privacidad y seguridad de la información, permitiendo que las interacciones con los ciudadanos, otras entidades públicas y el sector privado sean confiables y seguras.

A través de la formulación e implementación del modelo de seguridad, la E.S.E. busca preservar la confidencialidad, integridad y disponibilidad de la información, contribuyendo de manera efectiva al cumplimiento de su misión institucional y a la consecución de sus objetivos estratégicos.

Imagen 4. *Niveles de madurez en seguridad y privacidad*

9. PLAN DE IMPLEMENTACIÓN

El Plan se desarrollará en las siguientes fases, incorporando las guías de seguridad de la información del MinTIC en cada actividad:

Fase 1: Diagnóstico y Planificación (Enero - Marzo 2025)
Actividad 1.1: Realizar un diagnóstico inicial del estado actual de la seguridad de la información en la E.S.E.UNA. *Guía MinTIC Aplicable*: Guía 7 - Gestión de Riesgos. **Actividad 1.2**: Identificar y clasificar los activos de información críticos. *Guía MinTIC Aplicable*: Guía 5 - Gestión y Clasificación de Activos de Información. **Actividad 1.3**: Revisar y modificar de ser necesario la política general de seguridad y privacidad de la información.

Guía MinTIC Aplicable: Guía 2 - Política General MSPI.

Fase 2: Diseño y Desarrollo (Abril - Junio 2025)

Actividad 2.1: Diseñar procedimientos de seguridad de la información.

Guía MinTIC Aplicable: Guía 3 - Procedimiento de Seguridad de la Información.

Actividad 2.2: Establecer roles y responsabilidades en materia de seguridad de la información.

Guía MinTIC Aplicable: Guía 4 - Roles y Responsabilidades.

Actividad 2.3: Desarrollar un plan de capacitación y sensibilización para el personal.

Guía MinTIC Aplicable: Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información

Fase 3: Implementación (Julio - Septiembre 2025)

Actividad 3.1: Implementar los controles de seguridad de la información.

Fase 4: Evaluación y Mejora Continua (Octubre - Diciembre 2025)

Actividad 4.1: Realizar auditorías internas de seguridad de la información.

Guía MinTIC Aplicable: **Guía 6 - Auditorías de Seguridad y Privacidad de la Información.**

Acciones:

Verificar el cumplimiento de los controles definidos en la política.

Revisar las brechas identificadas durante la implementación.

Validar si los roles, permisos y perfiles de los usuarios en sistemas como DINÁMICA están actualizados y corresponden a las funciones asignadas.

Evidencia: Informes de auditoría interna con hallazgos y recomendaciones.

Actividad 4.2: Consolidar los indicadores de gestión de seguridad.

Acciones:

Analizar los resultados de los indicadores establecidos (por ejemplo, número de incidentes reportados, tiempo de resolución, cumplimiento de capacitaciones).

Documentar los datos para medir la efectividad del MSPI.

Evidencia: Reporte consolidado de métricas de seguridad.

Actividad 4.3: Realizar simulacros de recuperación ante desastres y continuidad del negocio.

*Guía MinTIC Aplicable: Guía 8 – Gestión de continuidad del negocio***.**

Acciones:

Implementar escenarios de simulación para evaluar la capacidad de respuesta de la organización.

Documentar el tiempo de recuperación y la efectividad de los planes establecidos.

Evidencia: Reporte del simulacro con lecciones aprendidas.

Actividad 4.4: Ejecutar acciones correctivas basadas en los hallazgos de auditoría y simulacros.

Acciones:

Resolver debilidades detectadas en los controles de seguridad.

Ajustar los perfiles de usuario en sistemas según los hallazgos.

Evidencia: Informe de acciones correctivas implementadas.

Actividad 4.5: Actualizar la política y procedimientos de seguridad si es necesario.

Guía MinTIC Aplicable: **Guía 2 - Política General MSPI.**

Acciones:

Revisar si la política requiere modificaciones para adaptarse a los cambios tecnológicos, normativos o de contexto organizacional.

Validar la actualización con el Comité de Seguridad de la Información.

Evidencia: Acto administrativo que respalde las modificaciones.

Actividad 4.6: Reforzar las capacitaciones según los hallazgos de la auditoría.

Acciones:

Realizar talleres focalizados en las áreas que mostraron mayor vulnerabilidad.

Asegurar la participación del personal involucrado.

Evidencia: Listado de asistencia y material de capacitación.

Actividad 4.7: Preparar un informe de cierre del ciclo anual del MSPI.

Acciones:

Consolidar toda la documentación de la implementación, auditoría y acciones correctivas.

Presentar los resultados al Comité de Seguridad de la Información y a la Dirección General.

Evidencia: Informe final del MSPI 2025, aprobado y archivado.

Actividad 4.8: Diseñar el plan de trabajo 2026 basado en los resultados de 2025.

Acciones:

Identificar objetivos prioritarios para el siguiente año.

Definir nuevas actividades o controles según el estado de madurez alcanzado.

Evidencia: Plan de trabajo preliminar para 2026.

Actividad 4.9: Promover la cultura de seguridad de la información para cierre de año.

Acciones:

Realizar campañas de sensibilización de fin de año dirigidas a todos los colaboradores.

Difundir buenas prácticas a través de boletines o actividades dinámicas.

Evidencia: Registro de campañas, materiales distribuidos y encuestas de percepción del personal.

10. CUMPLIMIENTO NORMATIVO

La E.S.E. Universitaria del Atlántico se compromete a:

- Garantizar la conformidad con las normativas nacionales e internacionales:
    - Resolución 1519 de 2020 (Accesibilidad digital).

- Ley 1581 de 2012 (Protección de datos personales).
- Resolución 500 de 2021 (Gestión de seguridad).

- Auditorías internas y externas mínimo cada seis meses.
- Presentación de informes de cumplimiento ante el Comité de Seguridad y Privacidad.

11. BIBLIOGRAFIA

Departamento Administrativo de la Función Pública. (2014). *Guía para la administración del riesgo*. Bogotá, Colombia.

Función Pública. (2022). *Guía para la administración del riesgo y el diseño de controles en entidades públicas* (Versión 6). Bogotá, Colombia.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2020). *Guía para la administración del riesgo y diseño de controles en entidades públicas* (Versión 5). Bogotá, Colombia.

Organización Internacional de Normalización (ISO). (2018). *Norma Internacional ISO 31000*. Ginebra, Suiza.

Constitución Política de Colombia [Const.]. (1991). Artículo 15. Recuperado de https://www.corteconstitucional.gov.co/inicio/Constitucion%20politica%20de%20Colombia.pdf

Organización Internacional de Normalización. (2013). ISO/IEC 27001:2013. Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos. Ginebra: ISO. Recuperado de https://www.iso.org/standard/54534.html

Superintendencia de Industria y Comercio. (s.f.). Protección de datos personales. Recuperado de https://www.sic.gov.co/proteccion-de-datos-personales

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Guía para la implementación del Esquema de Seguridad de la Información. Recuperado de https://www.mintic.gov.co/portal/604/articles-55677_recurso_1.pdf

12. FICHA DE CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
01	28/01/2025	Creación del documento.

13. APROBACIÓN DEL DOCUMENTO

ELABORÓ	REVISÓ	APROBÓ
Nombre: Elena Roció El Pilar Moya Ramírez	**Nombre:** María Angélica Ahumada Figueroa	**Nombre:** Comité Institucional de Gestión y Desempeño
Cargo: Apoyo y Asesoría en la gestión de la Coordinación de Tecnologías de la Información	**Cargo:** Director(a) Tecnologías de la Información	**Cargo:** Comité Institucional de Gestión y Desempeño
Fecha: 28/01/2025	**Fecha:** 28/01/2025	**Fecha:** 31/01/2025