Aspecto Evaluable (Unidad Auditable): Auditoría Interna Específica a la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en la Universidad de Pamplona.	**Fecha**		
	13	03	2025

Objeto: Verificar la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), así como el cumplimiento de los lineamientos y estándares de seguridad de la información en la Universidad de Pamplona, eficacia de los controles, nivel de cumplimiento de la legislación aplicable y adopción de buenas prácticas que garanticen confidencialidad, integridad, disponibilidad y privacidad de la información.

Alcance: Implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en la Universidad de Pamplona.

Criterio: Normativa interna y externa de obligatorio cumplimiento, directrices del MinTIC, Función Pública (FURAG) (MIPG), así como, las normas técnicas de calidad NTC 5854 e ISO/IEC 27001, RESOLUCIÓN 1519 DE 2020 y el Documento Maestro del Modelo de Seguridad y Privacidad de la Información y sus guías de orientación.

Principales situaciones detectadas/Resultados de la Evaluación

Teniendo en cuenta el objetivo principal de la auditoría que es, verificar la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), así como el cumplimiento de los lineamientos y estándares de seguridad de la información en la Universidad de Pamplona, eficacia de los controles, nivel de cumplimiento de la legislación aplicable y adopción de buenas prácticas que garanticen confidencialidad, integridad, disponibilidad y privacidad de la información, además de, dar respuesta y verificar sí:

- ✓ ¿La entidad ha implementado el Modelo de Seguridad y Privacidad de la Información (MSPI)?
- ✓ ¿La entidad elaboró un diagnóstico de seguridad y privacidad de la información, construido a través de la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI)?
- ✓ ¿Existe la política de seguridad y privacidad de la información en la entidad?
- ✓ ¿Se ha evaluado la efectividad de las acciones de seguridad y privacidad de la información (incluyendo acciones de imagen o confianza)?
- ✓ ¿Se da Accesibilidad a la web, conforme a la Norma Técnica Colombiana (NTC) 5854 que establece los requisitos de accesibilidad que son aplicables a las páginas web, que se presentan agrupados en tres niveles de conformidad: A, AA, y AAA?.

Conforme a lo anterior, se procedió a evaluar el proceso y actividades llevadas a cabo por el Centro de Investigación Aplicada y Desarrollo de Tecnologías de Información - CIADTI adscrito a la Vicerrectoría de Bienestar y Extensión, para dar cumplimiento a la Ley, normas aplicables y a los lineamientos y directrices del MinTic, en materia de infraestructura tecnológica, sistemas de información y seguridad y privacidad de la información en la Universidad de Pamplona.

Con el fin de dar respuesta a los interrogantes planteados anteriormente, la Profesional Universitario adscrita al CIADTI Ingeniera María

Victoria Bautista Bochagá, da respaldo al trabajo realizado por el Centro frente a los requerimientos de la normativa y documentación que se está construyendo para la implementación de un Sistema de Seguridad y Privacidad de la Información, bajo la norma de calidad NTC ISO 27001.

Preguntas	Hallazgos
¿La entidad ha implementado el Modelo de Seguridad de la Información (MSPI)?	**Respuesta:** A la fecha no se ha implementado el MSPI en la Universidad de Pamplona conforme los lineamientos del MinTic. **Justificación:** El CIADTI de la Universidad de Pamplona estableció el Diseño para la implementación de la Seguridad y Privacidad de la Información bajo la NTC ISO 27001, con el fin de dar cumplimiento a los lineamientos normativos para la optimización efectiva de los Sistemas de Información en la Universidad de Pamplona, a través de iniciativas y proyectos que soporten el Direccionamiento Estratégico, para una adecuada administración de la infraestructura tecnológica hardware, software y seguridad de la información, mediante las mejores prácticas de arquitectura institucional, proyectos TI y gestión de servicios. **Evidencia:** Documento borrador “Diseño para la Implementación del Sistema de Seguridad y Privacidad de la Información”.
¿La entidad elaboró un diagnóstico de seguridad y privacidad de la información, construido a través de la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI)?	**Respuesta:** El diagnóstico elaborado no se hizo bajo la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI). **Justificación:** El CIADTI elaboró el autodiagnóstico para identificar el estado actual en materia de Seguridad de la Información con base en los requerimientos de la NTC ISO 27001.

	Evidencia: 1. Procedimiento borrador de Gestión de Activos de Información. 2. Matriz de Activos de Información - https://www.datos.gov.co/Educaci-n/Registro-de-Activos-de-Informaci-n/ygic-g3nc/about_data
¿Existe la política de seguridad y privacidad de la información en la entidad?	**Respuesta:** A la fecha no se cuenta con el Acto Administrativo de aprobación de la Política de Seguridad y Privacidad de la Información en la Institución. **Justificación:** El CIADTI elaboró la Política de Seguridad y Privacidad de la Información, y el proyecto de acto administrativo para la revisión, análisis y aprobación por parte de la Alta Dirección. **Evidencia:** 1. Documento borrador de la Política de Seguridad y Privacidad de la Información. 2. Documento borrador del acto administrativo que permitiría la adopción de la Política de Seguridad y Privacidad de la Información.
¿Se ha evaluado la efectividad de las acciones de seguridad y privacidad de la información (incluyendo acciones de imagen o confianza)?	**Respuesta:** No. **Justificación:** El CIADTI elaboró el documento borrador *"DISEÑO PARA LA IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN EL CENTRO DE INVESTIGACION APLICADA Y DESARROLLO DE TECNOLOGIAS DE INFORMACION (CIADTI) DE LA UNIVERSIDAD DE PAMPLONA BAJO LA NTC ISO 27001".* Una vez la Alta Dirección de la aprobación, se procederá al inicio de la implementación del SSPI teniendo como alcance inicial el CIADTI para evaluar su efectividad y eficacia y después ser replicado a nivel institucional.

	Evidencia: Documento borrador “Diseño para la Implementación del Sistema de Seguridad y Privacidad de la Información”.
¿Se da Accesibilidad a la web, conforme a la Norma Técnica Colombiana (NTC) 5854 que establece los requisitos de accesibilidad que son aplicables a las páginas web, que se presentan agrupados en tres niveles de conformidad: A, AA, y AAA?.	**Respuesta:** En levantamiento de información. **Justificación:** Tras realizar el autodiagnóstico general de la Política de Gobierno Digital utilizando la herramienta proporcionada por el Modelo Integrado de Planeación y Gestión (MIPG), el CIADTI ha identificado que se está llevando a cabo un proceso de levantamiento de información con el objetivo de rediseñar e implementar soluciones digitales. Este proceso incluye, además, un análisis exhaustivo del portal web oficial, con la finalidad de incorporar nuevos servicios, funcionalidades y criterios establecidos en la Política de Gobierno Digital. Así mismo, el análisis contempla la adaptación de los sistemas de información según la caracterización de usuarios, y la implementación de criterios de accesibilidad web de acuerdo con los niveles A y AA, tal como se establece en la Norma Técnica Colombiana NTC 5854, garantizando así la inclusión y el acceso a la información por parte de todos los usuarios **Evidencia:** 2021-06-10_Autodiagnostico_gobierno_digital Rtas.xlsx

Con el fin de asegurar el cumplimiento normativo y garantizar una adecuada gestión de la seguridad y privacidad de la información, se revisa el marco legal aplicable, así como los lineamientos y directrices que en materia de Seguridad y Privacidad de la Información ha establecido el Gobierno Nacional a través del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTic, el Modelo Integrado de Planeación y Gestión (MIPG) y la normativa técnica de ICONTEC, con el objetivo de verificar la alineación de los procesos y procedimientos institucionales con los estándares nacionales e internacionales. Esta revisión busca identificar posibles brechas, establecer acciones correctivas y garantizar que los sistemas de información de la institución cumplan con los requisitos legales y los mejores estándares de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información.

MARCO LEGAL REFERENCIADO:

Ley 1712 de 2014 / Decreto 1494 de 2015

Ley 1712 del 2014 por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones, establece en su artículo 5°, corregido por el artículo 1 del Decreto 1494 del 13 de julio de 2015 "Por el cual se corrigen yerros en la Ley 1712 de 2014" menciona los sujetos obligados, que así mismo ratifica la Resolución 1519 del 24 de agosto de 2020, por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos, cuyo objetivo es expedir los lineamientos que deben atender los sujetos obligados para cumplir con la publicación y divulgación de la información señalada en la Ley 1712 del 2014, estableciendo los criterios para la estandarización de contenidos e información, accesibilidad web, seguridad digital, datos abiertos y formulario electrónico para Peticiones, Quejas, Reclamos, Sugerencias y Denuncias (PQRSD).

Decreto 1078 de 2015

Decreto 1078 del 26 de mayo de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones" última fecha de actualización: 22 de diciembre de 2023.

Establece:

SECCIÓN 2 ELEMENTOS DE LA POLITÍCA DE GOBIERNO DIGITAL:
"3.2. Seguridad y Privacidad de la Información: Este habilitador busca que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. (SECCIÓN 2 ELEMENTOS DE LA POLITÍCA DE GOBIERNO DIGITAL ARTÍCULO 2.2.9.1.2.1. Estructura)".

CAPITULO 4 DERECHOS Y OBLIGACIONES DE LOS ACTORES
"7. Implementar sistemas de gestión de seguridad y controles que permitan disminuir y gestionar el riesgo asociado a la integridad, confidencialidad y disponibilidad de la información para lo cual adoptarán el cumplimiento de estándares de amplio reconocimiento nacionales o internacionales de acuerdo con los lineamientos del Modelo de seguridad y privacidad de la información de la política de Gobierno Digital".

Decreto 415 de 2016

El Decreto 415 de 2016, establece los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones a través del posicionamiento de los líderes de áreas TI.

El 22 de marzo de 2016, el Gobierno Nacional informó que mediante el Decreto 415 de 2016, estableció los lineamientos para la implementación de la figura de Director de Tecnologías y Sistemas de Información, quien será pieza clave en la construcción de un Estado más eficiente y transparente gracias a la gestión estratégica de las Tecnologías de la Información y las Comunicaciones (TIC).

Es así, como las entidades estatales tendrán un Director de Tecnologías y Sistemas de Información responsable, entre otras asignaciones, de la planeación y ejecución de los planes, programas y proyectos de tecnologías y sistemas de información y que deberá acogerse a los lineamientos que en la materia defina el MinTIC.

Resolución 1519 del 2020

El 17 de diciembre de 2020, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) publicó la Resolución 1519 de 2020 para cumplir con la Ley 1712 de 2014. Esta resolución establece criterios para la estandarización de información, accesibilidad, seguridad, datos abiertos, y PQRS.

La Resolución 1519 del 2020 contiene cuatro anexos, el primero desarrolla las directrices de accesibilidad web; el segundo incorpora nuevos estándares de transparencia y divulgación de contenidos; el tercero dispone medidas en materia de seguridad digital; y el cuarto dispone condiciones sobre datos abiertos.

Otras normas relacionadas

- ✓ Ley 1581 de 2012, o Ley de Protección de Datos Personales, establece disposiciones generales para la protección de datos personales.
- ✓ Política Nacional de Seguridad Digital CONPES 3854 de 2017.
- ✓ Lineamientos de Política para Ciberseguridad y Ciberdefensa CONPES 3701 de 2011.
- ✓ Ley 1680 del 20 de noviembre 2013, por la cual se garantiza a las personas ciegas y con baja visión, el acceso a la información, a las comunicaciones, al conocimiento y a las tecnologías de la información y de las comunicaciones.
  Artículo 9°. Accesibilidad y usabilidad. Todas las páginas web de las entidades públicas o de los particulares que presten funciones públicas deberán cumplir con las normas técnicas y directrices de accesibilidad y usabilidad que dicte el Ministerio de Tecnologías de la Información y las Comunicaciones.

El Ministerio de Tecnologías de la Información y las Comunicaciones mediante Resolución No. 500 del marzo 10 de 2021, "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital", a partir de la norma genera un documento de lineamientos de buenas prácticas en Seguridad y Privacidad para las entidades del Estado.

El Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

Detalles del MSPI

El MSPI se basa en la norma ISO 27001, versión 2013.
El MSPI se actualizó en 2022, tras la actualización de la norma ISO 27001.
El MSPI se revisó y derogaron los lineamientos, guías y estándares que no se alineaban con la nueva norma.
El MSPI se implementó para proteger, preservar y administrar la información que circula en el mapa de operación.
El MSPI se implementó para prevenir incidentes y propender por la continuidad de los servicios.
El MSPI se implementó para dar cumplimiento a los requisitos legales, reglamentarios, regulatorios y a los de las normas técnicas colombianas.

MinTIC elaboró el Modelo de Seguridad y Privacidad de la Información – MSPI con el objetivo de formalizar al interior de los sujetos obligados un sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (5) fases las cuales permiten que las Entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información. Por ello, los sujetos obligados deben abordar las siguientes fases:

1. Diagnóstico: Realizar un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI. Se recomienda usar este diagnóstico al iniciar el proceso de adopción, con el fin de que su resultado sea un insumo

para la fase de planificación y luego al finalizar la Fase 4 de mejora continua.

2. Planificación: Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.

3. Operación: Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.

4. Evaluación de desempeño: Determinar el sistema y forma de evaluación de la adopción del modelo.

5. Mejoramiento Continuo: Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

Fuente: Anexo 1 Modelo de Seguridad y Privacidad de la Información:
chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-162621_Modelo_de_Seguridad_y_Privacidad__MSPI.pdf

Una vez culminada las actividades del MSPI, se evalúa la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación que debe incluir la correcta interacción entre el MSPI, MIPG y los requerimientos de la Ley 1581 de 2012 “Protección de datos personales”, Ley 1712 de 2014 “Ley de Transparencia y Acceso a la Información Pública”, Decreto 2106 de 2019 o cualquier norma que las reglamente, adicione, modifique o derogue.

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información, con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea.

MIPG

3ª. Dimensión: Gestión con valores para resultados
El propósito de esta dimensión es permitirle a la entidad realizar las actividades que la conduzcan a lograr los resultados propuestos y a materializar las decisiones plasmadas en su planeación institucional, en el marco de los valores del servicio público.
3.3 Relación Estado Ciudadano
3.3.4 Política Gobierno Digital

3.4.1 Política de Transparencia, acceso a la información pública y lucha contra la corrupción
3.4.2 Política de Seguridad Digital

Para realizar un buen diagnóstico MinTic recomienda realizar el autodiagnóstico General de la Política de Gobierno Digital, a través de la herramienta dispuesta por el Modelo Integrado de Planeación y Gestión (MIPG).

El autodiagnóstico de seguridad y privacidad de la información es una herramienta que permite identificar el nivel de madurez de la implementación de un modelo de seguridad y privacidad, 2021-06-10_Autodiagnostico_gobierno_digital.xlsx.

Este archivo hace parte de un conjunto de herramientas de Autodiagnóstico que permitirán a cada entidad desarrollar un ejercicio de valoración del estado de las políticas en las cuales se estructura el Modelo Integrado de Gestión y Planeación, con el propósito de que la entidad logre contar con una línea base respecto a los aspectos que debe fortalecer, los cuales deben ser incluidos en su planeación institucional. Esta herramienta puede ser utilizada en el momento en que la entidad lo considere pertinente, sin implicar esto reporte alguno a Función Pública, al Ministerio de Tecnologías de la Información y las Comunicaciones o a otras instancias del Gobierno u organismos de Control.

"Los resultados obtenidos en esta herramienta no son comparables con los resultados del Índice de Gobierno Digital, el cual se estima de manera anual en el marco de la operación estadística Medición del Desempeño Institucional."

Entre los propósitos que busca está:

Habilitar y mejorar la provisión de servicios digitales de confianza y calidad.
Lograr procesos internos seguros y eficientes.
Fortalecer las capacidades de gestión de tecnologías de información.

Fortalecimiento de la Seguridad y Privacidad de la Información y el Empoderamiento de los ciudadanos mediante un Estado abierto, buscando aplicar:

- ✓ Criterios de accesibilidad web, de nivel A y AA de conformidad, definidos en la NTC5854 en todas las secciones de su portal Web oficial.
- ✓ Que la entidad publique en la sección "transparencia y acceso a la información pública" de su portal web oficial información actualizada sobre Normatividad general y reglamentaria
- ✓ Política de Gobierno Digital
- ✓ Política de Seguridad Digital

El ICONTEC, como Organismo Nacional de Normalización en Colombia, trabaja en la elaboración de normas y guías técnicas para mejorar la calidad de vida de los colombianos.

Estas normas están encaminadas a que, la calidad de vida de las personas sea cada vez mejor, proteger el ambiente y definir las características que deben cumplir los productos y servicios con estándares de calidad requeridos, para que respondan con seguridad a las necesidades de los ciudadanos.

En este sentido se encuentra la NTC 5854 que establece los requisitos de accesibilidad que se deben implementar en las páginas web en los niveles de conformidad A, AA y AAA.

De acuerdo a la revisión de la normativa aplicable y de obligatorio cumplimiento se permite determinar las siguientes oportunidades de mejora a tener en cuenta:

Oportunidades de Mejora:

Identificar, incorporar y aplicar nuevos conocimientos sobre regulaciones vigentes, tecnologías disponibles, métodos y programas de trabajo, para mantener actualizada la efectividad de sus prácticas laborales.

Tener en cuenta al momento de la Planificación el Formulario Único de Reporte de Avances de la Gestión (FURAG) herramienta en línea de reporte de avances de la gestión, como insumo para el monitoreo, evaluación y control del desempeño institucional, el cual se solicita y evalúa el la aplicación de los lineamientos establecidos en normas de calidad, leyes y decretos aplicables al Estado Colombiano.

Establecer el normograma del Centro de Investigación Aplicada y Desarrollo de Tecnologías de Información – CIADTI de manera global, así como documentar el proceso y todos sus quehaceres como apoyo transversal a los procesos académicos, investigativos y administrativos de la Universidad de Pamplona.

Aplicabilidad de los lineamientos y directrices de las normas emanadas por el Gobierno Nacional y el Ministerio de Tecnologías de la Información y las Comunicaciones.

Realizar un trabajo mancomunado entre el CIADTI, la Oficina de Comunicación y Prensa y la Oficina de Atención al Ciudadano y Transparencia, para dar cumplimiento a los lineamientos del MinTiC.

Si bien, no todas las normas técnicas de calidad son de obligatorio cumplimiento y muchas de ellas son voluntarias, es fundamental que los lineamientos y directrices que estas establecen sean tenidos en cuenta para garantizar la mejora continua de los procesos institucionales.

Con el objetivo de establecer acciones específicas que aseguren el cumplimiento de dichas normas se deberá diseñar el ***FAC-49 Plan de Gestión del Cambio y Mejora Continua*** para abordar las oportunidades de mejora que permitan integrar el Modelo de Seguridad y Privacidad de la Información (MSPI), con las normas técnicas de calidad NTC 5854 y NTC ISO/IEC 27001:2018 y así, dar cumplimiento a lo regulado por MinTic y adoptar en la Universidad de Pamplona el Modelo de Seguridad y Privacidad de la Información que permita contar con una infraestructura tecnológica sólida, eficiente y segura.

Recomendaciones: Véase las oportunidades de mejora como iniciativas para la mejora de aquellos aspectos en los que se pueden trabajar para incrementar la eficacia, eficiencia y satisfacción de las partes interesadas en el ambiente laboral, la optimización de procesos y el incremento de mejores prácticas para el cumplimiento de los objetivos deseados en el Centro de Investigación Aplicada y Desarrollo de Tecnologías de Información – CIADTI.

Conclusiones: La adopción de un sistema de gestión de la seguridad de la información es una decisión estratégica para una organización. El establecimiento y su implementación están influenciado por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizativos utilizados y el tamaño y estructura de la organización.

La Norma técnica NTC 5854 y la ISO 27001, son normativas que se consideran de alto nivel en lo que respecta a la gestión de seguridad de la información y la privacidad. La ISO 27001 es un estándar ampliamente reconocido para la gestión de la seguridad de la información, mientras que la NTC 5854 es una norma colombiana. Ambas buscan proporcionar un marco de buenas prácticas y asegurar que las organizaciones gestionen de forma adecuada sus activos de información y reduzcan los riesgos de seguridad.

Teniendo en cuenta la jerarquía de las normas en Colombia, la Constitución Política y que se establece de acuerdo al poder de las entidades que las emiten, es importante recordar que en Colombia, el MinTic tiene un mandato específico para regular las políticas públicas relacionadas con las Tecnologías de la Información y las Comunicaciones, incluyendo la política de Gobierno Digital y otros marcos de seguridad informática.

Por tanto, los lineamientos del MinTIC prevalecen en el ámbito nacional, ya que están enfocados en la implementación de políticas públicas y cumplimiento normativo en el país, lo que es obligatorio para las entidades que dependen del Estado o que están bajo regulación de este tipo de organismos. La ISO 27001 o la NTC 5854 pueden ser complementarias, proporcionando una estructura robusta para cumplir con los requisitos de seguridad de la información, pero los lineamientos de MinTIC deberán ser priorizados en lo que respecta a cumplimiento legal y normativo en Colombia.

Sobre la importancia de implementar el Modelo de Seguridad y Privacidad de la Información en la Universidad de Pamplona según los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones, asegurará que la Universidad esté alineada con las regulaciones nacionales y no esté expuesta a riesgos legales o de sanciones por no cumplir con las políticas del gobierno.

Así mismo, mejora de la gestión de la seguridad de la información, por cuanto el Modelo se encuentra alineado a la ISO 27001 y a la NTC 5854, normas fundamentales para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) que asegure la protección de la confidencialidad, integridad y disponibilidad de la información en la Universidad. Con el modelo del Gobierno Digital de MinTIC, se busca precisamente la optimización y digitalización de los servicios públicos, lo cual requiere asegurar que los sistemas de información sean confiables y estén protegidos frente a amenazas.

Implementar estos lineamientos también incrementa la confianza en la gestión de la información de los estudiantes, docentes y personal administrativo. Esto es crucial para cumplir con los principios de transparencia y acceso a la información establecidos en el marco del Gobierno Digital - Protección de datos y confianza pública.

En la Institución es fundamental proteger tanto la información personal de los estudiantes y empleados como la información académica y de investigación. La implementación del Modelo de Seguridad y Privacidad de la Información ayudará a proteger la infraestructura tecnológica de la Universidad y garantizará que la gestión de datos se realice de manera ética, segura y conforme a las mejores prácticas internacionales y nacionales.

En conclusión, en la Universidad de Pamplona es crucial seguir los lineamientos establecidos por MinTIC, ya que son obligatorios en el marco legal colombiano, mientras que las normas internacionales como ISO 27001/NTC 5854 proporcionan una estructura robusta para garantizar la seguridad de la información en un nivel organizacional más amplio. Implementar el Modelo de Seguridad y Privacidad según la Política de Gobierno Digital no solo asegura el cumplimiento de la normativa colombiana, sino que también proporciona un alto nivel de protección y confianza en los servicios digitales de la universidad en materia de infraestructura tecnológica, sistemas de información y seguridad y privacidad de la información.

Elaborado por:	Aprobado por:
Maritza Constanza Gamboa Auditor Interno – Oficina de Control Interno de Gestión	**Yessica Yovanna Márquez Amaya** Jefe Oficina de Control Interno de Gestión