INFORME EJECUTIVO	Código: EIM-FR-29 Versión: 02 Página: 1 de 2

Unidad auditable: Gestión TIC	**Auditores:** William Echavarría Lotero Juan Pablo Taborda Hernández
Informe Dirigido a: Comité Institucional de Coordinación de Control Interno	
Objetivo: Verificar la gestión del Modelo de Seguridad y Privacidad de la Informaciòn de la Institución Universitaria, a través de la evaluación del cumplimiento de los lineamientos internos y externos aplicables al modelo, con el objetivo de establecer invitaciones o recomendaciones de mejora que contribuyan a la adecuada gestión contemplados en los planes de acción, que conllevan al cumplimiento de las metas semestrales o anuales.	
Alcance: 1. Riesgos de gestión, corrupción y seguridad digital 2. Planes de mejoramiento auditorías internas y externas 3. Indicadores de gestión y de Plan de Desarrollo 4. Modelo de Seguridad y Privacidad de la Informaciòn	

1. Observaciones (Hallazgos)

Observación No. 01: Incumplimiento de la Norma ISO/IEC 27001:2022

Criterio:
La Norma ISO/IEC 27001:2022 establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Entre los apartados relevantes se encuentran:

- Contexto de la organización
- Liderazgo
- Planificación
- Soporte
- Operación
- Evaluación del desempeño

Condición:
Se evidenció que la institución no ha implementado ni aplica los requisitos establecidos en la Norma ISO/IEC 27001:2022, careciendo de un SGSI formalmente documentado y operativo.

Causa:
- Desconocimiento o falta de capacitación sobre la norma.
- Ausencia de planeación estratégica en materia de seguridad de la información.
- Insuficiencia de recursos humanos y financieros destinados a la gestión de seguridad de la información.

Efecto:
- Posibles sanciones legales y administrativas.
- Riesgo reputacional institucional.
- Exposición elevada a incidentes de ciberseguridad y pérdida de información sensible.

Exposición al riesgo: Tipo: Estratégico
Nivel: Alto

Observación No. 02: Incumplimiento de la Resolución 00500 del 2021

Criterio:
La Resolución 00500 de 2021, emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), establece los lineamientos y estándares para la implementación de la Estrategia de Seguridad Digital en entidades públicas.

Condición:
Se evidenció la ausencia de una Estrategia de Seguridad Digital alineada con los lineamientos de la Resolución 00500 de 2021, así como la falta de mecanismos de monitoreo y seguimiento asociados.

Causa:

- Falta de capacitación sobre la normativa aplicable.
- Escasos recursos financieros y humanos para el desarrollo de la estrategia.
- Desconocimiento de los requerimientos específicos establecidos por MinTIC.

Efecto:

- Riesgo de incumplimiento normativo y posibles sanciones.
- Aumento del riesgo reputacional.
- Mayor vulnerabilidad ante ciberataques e incidentes de seguridad digital.

Exposición al riesgo: Tipo: Estratégico
Nivel: Alto

Observación No. 03: Incumplimiento de la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7

Criterio:
La Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7, emitida por el Departamento Administrativo de la Función Pública (DAFP), establece los lineamientos para la identificación, análisis, valoración y tratamiento de los riesgos institucionales.

Condición:
Se evidenció desactualización en la política, guías y matrices asociadas a la administración de riesgos, lo cual impide una gestión oportuna y efectiva de los mismos.

Causa:

- Falta de capacitación del personal responsable.
- Limitación de recursos humanos y técnicos para la actualización y mantenimiento del sistema de gestión de riesgos.

Efecto:

- Aumento del riesgo reputacional institucional.
- Posible materialización de riesgos no gestionados adecuadamente.
- Deficiencias en la toma de decisiones estratégicas.

Exposición al riesgo: Tipo: Estratégico
Nivel: Alto

Recomendaciones de mejora:

Con relación al autodiagnóstico

4.1 Se considera como buenas prácticas diligenciar en su totalidad todos los espacios en blanco dispuesto en el autodiagnóstico, con el objetivo de facilitar la identificación del nivel de madurez de seguridad de la información en el que se encuentra la Institución.

Con relación a las Necesidades y expectativas de los interesados

4.2 Se considera como buenas prácticas la identificación de las partes interesadas internas y externas del Sistema de Gestión de Seguridad de la Información, donde se incluya los requisitos legales, reglamentarios y contractuales, con el objetivo de garantizar que se cumplan los requisitos, las necesidades e implementación del SGSI.

Con relación al alcance del Modelo de Seguridad y Privacidad de la Información - MSPI

4.3 Se considera como buenas prácticas generar el alcance del MSPI, donde se incluya procesos, tramites, servicios, sistemas de información, activos de información, infraestructura de TIC, recurso humano y financiero, (…), y registrarlo en el Sistema de Información Isolucion, este alcance se puede definir en un manual o política, esto asegura la protección de los datos, activos (…).

4.4 Se considera como buenas prácticas, analizar la pertinencia de incluir el Sistema de Gestión de Seguridad de la información, en el Acuerdo Directivo 015 de 2025, en el Subsistema de Gestión Integral – SGI.

Con relación a la Política de seguridad y privacidad de la información

4.5 Se considera como buenas prácticas actualizar la política, de acuerdo a lo requerido en el habilitador del producto tipo, con el objetivo de dar cumplimiento a lo requerido por Min TIC en cuanto su estructura.

4.6 Se considera como buenas prácticas generar un manual, de acuerdo a lo requerido en el habilitador del producto tipo, con el objetivo de dar cumplimiento a lo citado por Min TIC, se debe tener en cuenta su temática y registrarlo en el Sistema de Información Isolucion.

4.7 Se considera como buenas prácticas, realizar seguimiento o revisiones periódicas de las fechas que se tienen propuestas en los planes, que están integrados con el Plan de Acción Integral Institucional y que su ejecución es responsabilidad de Gestión TIC, en caso de evidenciar que estas no se van a cumplir, reevaluar con antelación las fechas.

Con relación a Roles y responsabilidades

4.8 Se considera como buenas prácticas definir e identificar los roles, perfiles y responsabilidades, donde se incluya responsable de seguridad de la información, oficial de protección de datos, funciones del Comité Institucional de Gestión y Desempeño, responsabilidades de la Dirección Jurídica, Gestión Talento Humano, Dirección de Evaluación y Control, Gestión TIC, funcionarios y contratistas, arquitectura de seguridad de la información, del equipo de proyecto de implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, de proveedores y terceros y registrarlo en el Sistema de Información Isolucion, esto garantiza la correcta implementación del Modelo.

Con relación a la identificación de activos de información e infraestructura critica cibernética

4.9 Se considera como buenas prácticas actualizar el inventario, de acuerdo a lo requerido en el habilitador del producto tipo y en los nombres de los procesos, con el objetivo de dar cumplimiento a lo requerido por Min TIC en cuanto su estructura.

4.10 Se considera como buenas prácticas una vez se tenga la actualización del inventario, llevar para aprobación por los lideres de dependencias y por el Comité Institucional de gestión y Desempeño y documentarlo.

4.11 Se considera como buenas prácticas generar procedimiento y documento metodológico de inventario y clasificación de activos de información, que contenga la hoja de ruta.

4.12 Se considera como buenas prácticas generar un procedimiento para la eliminación segura de información contenida en activos físicos y digitales, asegurando que los datos no puedan ser recuperados una vez descartados. Estos procedimientos deben considerar el tipo de activo (papel, disco duro, dispositivos USB, nube), su nivel de clasificación, y el medio de eliminación (desmagnetización, destrucción física, borrado certificado, etc.). La eliminación debe estar documentada y respaldada por registros auditables.

Con relación a la Valoración de los riesgos de seguridad de la información

4.13 Se considera como buenas prácticas actualizar la política, la guía y las matrices relacionadas con la administración del riesgo en la Institución, teniendo en cuenta la Guía para la Gestión Integral del Riesgo en Entidades Públicas del 2025 versión 7, emitida por el Departamento Administrativo de la Función Pública del 2025, también es importante que en esta actualización se incluya un capítulo de los riesgos de seguridad y privacidad de la información, en donde se abarque todo su alcance.

4.14 Se considera como buenas prácticas, capacitar y/o sensibilizar a los funcionarios y contratistas de la institución en el tema de riesgos, como la identificación, valoración, tratamiento y monitoreo de riesgos, igualmente donde se de claridad que no toda la responsabilidad es del proceso de Gestión TIC, es compartida, toda vez que los mapas de riesgos y el tratamiento es aprobado por los lideres de dependencias.

4.15 Se considera como buenas prácticas, generar documento donde se defina que riesgos se gestionarían de los activos, si todos o solo aquellos que tenga un nivel de criticidad alta.

4.16 Se considera como buenas prácticas, que en la matriz de riesgos de seguridad digital se tengan en cuenta los controles establecidos en el anexo A 27001:2022.

Con relación al Plan de tratamiento de los riesgos de seguridad de la información

4.17 Se considera como buenas prácticas revisar y ajustar el plan de tratamiento de riesgos, de manera que se alinee con la identificación de activos de información y a la matriz de riesgos, también es importante tener en cuenta los controles establecidos en el anexo A 27001:2022 y actualizar el nombre del responsable de ejecutar las actividades.

4.18 Se considera como buenas prácticas y con el objetivo de que el documento de Declaración de aplicabilidad sea comprensible, se propone el siguiente formato: Nº del control – nombre del dominio – descripción del control – descripción de implementación o la justificación de exclusión.

4.19 Se considera como buenas prácticas una vez se tenga la actualización de la Declaración de aplicabilidad, llevar para socialización y aprobación por los lideres de dependencias y por el Comité Institucional de gestión y Desempeño y documentarlo.

Con relación al Soporte

4.20 Se considera como buenas prácticas generar y registrar en el Sistema de Información Isolucion, el seguimiento de los indicadores del PETI, que permitan medir el estado actual y real de la gestión del plan en mención.

4.21 Se considera como buenas prácticas, realizar seguimiento o revisiones periódicas de las fechas que se tienen propuestas en los planes y que su ejecución es responsabilidad de Gestión TIC, en caso de evidenciar que estas no se van a cumplir, reevaluar con antelación las fechas.

4.22 Se considera como buenas prácticas agilizar la elaboración del acta, donde se llevó a cabo la aprobación del PETI, una vez se tenga iniciar con su socialización y respectiva publicación en la página web o Isolucion.

Con relación a la Competencia, toma de conciencia y comunicación

4.23 Se considera como buenas prácticas fortalecer los esquemas actuales de concientización, educación y comunicación con respecto a la seguridad y privacidad de la información, en la que todos los funcionarios conozcan la política, las implicaciones de no aplicar las reglas de seguridad y privacidad e incluir formación en el Modelo de Seguridad y Privacidad de la Información - MSPI.

4.24 Se considera como buenas prácticas, capacitar al personal clave en los principios, controles y requerimientos de la norma, promoviendo la cultura de seguridad de la información.

4.25 Se considera como buenas prácticas, generar un plan de comunicaciones del MSP Modelo de Seguridad y Privacidad de la Información - MSPI.

Con relación a la Información documentada

4.25 Se considera como buenas prácticas, integrar en un acervo documental los documentos que se van generando del MSP (Actas, actos administrativos, informes, políticas entre otras.

Con relación al Control y planeación operacional

4.26 Se considera como buenas prácticas generar la Estrategia de seguridad digital, de acuerdo a lo requerido en la Resolución 00500 2021, con el objetivo de dar cumplimiento a lo citado por Min TIC y registrarlo en el Sistema de Información Isolucion.

4.27 Se considera como buenas prácticas generar las políticas enunciadas en los numerales 8.1 y 8.2 pagina 29 y 30 del presente informe, con el objetivo de dar cumplimiento a lo requerido por Min TIC y registrarlo en el Sistema de Información Isolucion.

Con relación a la Definición de indicadores de gestión

4.28 Se considera como buenas prácticas generar indicadores de seguridad de la información, que permitan medir el estado actual de la gestión y madures del Modelo de Seguridad y Privacidad de la Información - MSPI.

Pronunciamiento del Auditado y consideraciones del Equipo Auditor

La directora del proceso auditado dio respuesta al informe Prefinal de auditoría, mediante comunicación interna con radicado No. 2025001362 el día 13 de noviembre de 2025. A continuación, se relaciona los pronunciamientos:

Pronunciamiento del auditado:

"**Respetado director Echavarría,**

Cordial saludo

1. RESPUESTA A LAS OBSERVACIONES (HALLAZGOS)

En atención al informe de auditoría interna emitido por la Dirección de Evaluación y Control el 6 de noviembre de 2025, correspondiente a la verificación del Modelo de Seguridad y Privacidad de la Información (MSPI), y dentro del término establecido para el pronunciamiento del auditado, el proceso Gestión TIC, adscrito a la Dirección de Planeación y Aseguramiento de la Calidad, presenta la siguiente respuesta frente a los tres hallazgos u observaciones formuladas en el documento.

Observación No. 01: Incumplimiento de la Norma ISO/IEC 27001:2022 Análisis y respuesta:

La Norma ISO/IEC 27001:2022 es un estándar internacional de carácter voluntario que establece los lineamientos y requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Sin embargo, en el sector público colombiano su adopción no es de obligatorio cumplimiento.

En el ámbito nacional, el Modelo de Seguridad y Privacidad de la Información (MSPI), promovido por el Ministerio TIC, establece las directrices que deben seguir las entidades públicas en esta materia. Dicho modelo incorpora los principios de la Norma ISO/IEC 27001, pero no requiere su adopción ni certificación formal.

La Institución Universitaria Pascual Bravo ha venido implementando gradualmente el Modelo de Seguridad y Privacidad de la Información (MSPI), conforme a los lineamientos oficiales del Marco de Referencia de Arquitectura TI del Estado Colombiano y las actualizaciones publicadas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) durante los años 2024 y 2025.

En este contexto, la Institución adelanta actualmente los proyectos de Arquitectura Empresarial (MAE) y Modelo de Seguridad y Privacidad de la Información (MSPI), como resultado de una gestión institucional planificada, los cuales se encuentran incluidos en los instrumentos de planeación institucional, tales como el Modelo Integrado de Planeación y Gestión (MIPG) y el Plan Estratégico de Tecnologías de la Información (PETI), asegurando su desarrollo coordinado y alineado con los objetivos estratégicos institucionales.

Por lo anterior **No procede la observación como incumplimiento**, dado que la norma ISO/IEC 27001:2022 no es de cumplimiento obligatorio para la Institución. La gestión del proceso se enmarca dentro del modelo nacional vigente (MSPI), en proceso de adopción institucional.

Observación No. 02 – Incumplimiento de la Resolución 00500 de 2021 Análisis técnico y jurídico:

La Resolución 00500 de 2021, expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), tiene por objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), la Guía de Gestión de Riesgos de Seguridad de la Información, el procedimiento para la gestión de

incidentes de seguridad digital, y los estándares para la Estrategia de Seguridad Digital en entidades públicas.

Según su artículo 2 (Ámbito de aplicación), la resolución aplica a los sujetos obligados definidos en el artículo 2.2.9.1.1.2 del Decreto 1078 de 2015, es decir, a las entidades que conforman la Administración Pública, de conformidad con el artículo 39 de la Ley 489 de 1998, lo que incluye a las entidades del orden nacional y territorial, así como a los establecimientos públicos y las instituciones universitarias estatales.

Por tanto, **la Institución Universitaria Pascual Bravo**, en su calidad de entidad pública de carácter territorial, sí se encuentra dentro del ámbito de aplicación de la
Resolución 00500 de 2021; sin embargo, debe precisarse que esta norma no exige una adopción inmediata o certificación, sino una implementación progresiva conforme a las capacidades técnicas, humanas y presupuestales de cada entidad, articulada con el Modelo de Seguridad y Privacidad de la Información (MSPI).

En este sentido, la Institución no ha incumplido la norma, sino que se encuentra en fase de implementación gradual de los componentes del MSPI, según la hoja de ruta definida en el Plan Estratégico de Tecnologías de la Información (PETI) 2023– 2026, adoptado bajo el marco del Decreto 612 de 2018, y en el Plan de Seguridad y Privacidad de la Información – vigencia 2025, el cual contempla el desarrollo de la Estrategia de Seguridad Digital Institucional.

La Dirección de Planeación y Aseguramiento de la Calidad y el proceso Gestión TIC reconoce la aplicabilidad de la Resolución 00500 de 2021, sin embargo, la observación no puede catalogarse como un incumplimiento, dado que la entidad avanza conforme a lo dispuesto por el MinTIC en la implementación gradual del Modelo de Seguridad y Privacidad de la Información, priorizando las acciones de planeación, diagnóstico y formulación de la estrategia.

En consecuencia, la observación no debe catalogarse como un incumplimiento, dado que la Institución avanza en la implementación del MSPI conforme a los lineamientos del MinTIC.

Tampoco se considera necesario reclasificarla como acción de mejora, ya que los aspectos mencionados se encuentran incorporados en los planes institucionales vigentes —

principalmente en el MIPG y en el Plan Estratégico de Tecnologías de la Información (PETI)—, los cuales establecen su desarrollo dentro de la planeación institucional, evitando duplicidad de esfuerzos.

Observación No. 03 – Incumplimiento de la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7

En atención al hallazgo relacionado con el incumplimiento de lo dispuesto en la versión 7 de la Guía para la Gestión Integral del Riesgo en Entidades Públicas, emitida recientemente por el Departamento Administrativo de la Función Pública, la Institución se permite presentar las siguientes consideraciones:

Actualmente, la gestión del riesgo se desarrolla conforme a una anterior versión de la guía, a través de esta versión, la Institución ha consolidado un sistema formal de administración del riesgo que garantiza la identificación, valoración, tratamiento y seguimiento de los riesgos institucionales.

Con la publicación de la versión 7 en el segundo semestre del año 2025, el DAFP introdujo ajustes metodológicos y conceptuales dirigidos a articular la gestión pública del riesgo con el MIPG, fortalecer la gobernanza institucional e implementar herramientas más avanzadas, sin embargo, esta nueva versión tiene un carácter orientador y no cuenta, hasta la fecha, con una disposición normativa que establezca su adopción como de obligatorio cumplimiento inmediato para todas las entidades públicas.
Por lo anterior, la actualización debe asumirse como un proceso gradual de transición, acorde con la planeación institucional, los recursos disponibles y las capacidades internas. En ese sentido, la Institución ha avanzado en la actualización de su Política de Administración del Riesgo y en la formulación de un plan de implementación que permitirá incorporar de manera progresiva los lineamientos establecidos en la nueva versión de la guía.

Estas acciones reflejan el compromiso institucional con la mejora continua y con la adopción de las buenas prácticas promovidas por el DAFP. Por tanto, la situación señalada no corresponde a un incumplimiento normativo, sino a un proceso de ajuste y fortalecimiento en curso, que garantiza la continuidad de la gestión del riesgo y su alineación con los lineamientos nacionales.

La Institución reitera su disposición para continuar avanzando en la implementación de la Guía Versión 7 y mantener una comunicación permanente con la Dirección de Evaluación y Control, con el fin de socializar los avances y resultados que se obtengan durante el proceso de actualización.

https://drive.google.com/file/d/13b4Furu1K2FlGQrqGcMA2G9nWVtIPQ94/view?usp=sharing

https://drive.google.com/file/d/1WiTtmHmA68HjyF_c6ac2aE9h-HQCqPVb/view?usp=sharing

https://drive.google.com/file/d/1WhdPoNkFCOTsiXwkaIlL3K3o2W_9G0Pk/view?usp=sharing

La Dirección de Planeación y Aseguramiento de la Calidad y el proceso Gestión TIC reconoce la importancia de fortalecer la gestión de la seguridad de la información y la administración del riesgo institucional. Sin embargo, **los tres hallazgos señalados no constituyen incumplimientos normativos**, sino aspectos en desarrollo o en proceso de implementación gradual, conforme a los marcos legales y técnicos aplicables al sector público territorial.

Por tanto, se solicita que las observaciones **sean revaluadas**, teniendo en cuenta el análisis técnico y jurídico aquí presentado.

2. RECOMENDACIONES DE MEJORA

En atención a las recomendaciones de mejora emitidas en el informe de auditoría interna al Modelo de Seguridad y Privacidad de la Información (MSPI), La Dirección de Planeación y Aseguramiento de la Calidad y el proceso Gestión TIC, presenta a continuación la respuesta consolidada, teniendo en cuenta que la implementación del modelo se encuentra articulada al MIPG y al Plan Estratégico de Tecnologías de la Información (PETI) 2023–2026, los cuales definen las acciones, responsables y cronogramas establecidos para su desarrollo.

Recomendaciones 2.3, 4.2, 4.3 a 4.27
(Autodiagnóstico, partes interesadas, alcance, políticas, roles, activos, riesgos, controles, documentación, capacitación, estrategia e indicadores)

La Dirección de Planeación y Aseguramiento de la Calidad y el proceso Gestión TIC informa que el Modelo de Seguridad y Privacidad de la Información (MSPI) se encuentra actualmente en proceso de implementación institucional, en articulación con el Modelo Integrado de Planeación y Gestión (MIPG) y el Plan Estratégico de Tecnologías de la Información (PETI) 2023–2026.

Por lo anterior, todas las actividades relacionadas con **el autodiagnóstico, la identificación de partes interesadas, la definición del alcance del modelo, la actualización de la política y los manuales, la asignación de roles y responsabilidades, la gestión de activos de información, la valoración y tratamiento de riesgos, la declaración de aplicabilidad, la estrategia de seguridad digital, los documentos de soporte y los indicadores de gestión**, se desarrollarán conforme al cronograma de implementación del MSPI, que ya está dispuesto en los planes institucionales mencionados.

De igual manera, las actividades de capacitación, sensibilización y comunicación sobre seguridad y privacidad de la información hacen parte del Plan Institucional de Capacitaciones por la Dirección de Talento Humano y del componente de Uso y Apropiación del PETI, lo que garantiza su ejecución articulada y progresiva.

En consecuencia, no se requiere generar planes o acciones adicionales, dado que las recomendaciones señaladas ya están incorporadas en los instrumentos institucionales vigentes, los cuales establecen las fases, responsables, recursos y mecanismos de seguimiento correspondientes.

Recomendaciones 4.20, 4.21 y 4.22
(Seguimiento, cronogramas y socialización del PETI)

La Institución cuenta con un instrumento de medición que permite evaluar el avance en la implementación del PETI, verificando el cumplimiento de las metas y actividades definidas. Adicionalmente, el Plan de Desarrollo Institucional incluye un indicador que mide el porcentaje de implementación del Plan Maestro de Infraestructura Tecnológica (PMIT), uno

de los macroproyectos contemplados en el PETI, lo que contribuye al seguimiento del fortalecimiento tecnológico institucional.

No obstante, se identifica como oportunidad de mejora la construcción y registro de los indicadores en el Sistema ISOLUCIÓN, con el fin de fortalecer la trazabilidad, consolidar la información de seguimiento y centralizar los reportes en una única plataforma institucional.

Así mismo, se continuará con el seguimiento periódico de los cronogramas y la socialización oficial del PETI, una vez se disponga del acta de aprobación formal, garantizando su publicación en los medios institucionales correspondientes.

Las recomendaciones de los numerales 4.20, 4.21 y 4.22 se aceptan como acciones de mejora, orientadas a fortalecer el seguimiento, la trazabilidad y la transparencia en la ejecución del PETI y la gestión TIC institucional.

Conclusión General

En atención al informe emitido por la Dirección de Evaluación y Control, y luego del análisis técnico realizado por La Dirección de Planeación y Aseguramiento de la Calidad y el proceso Gestión TIC, se concluye que las observaciones presentadas no corresponden a incumplimientos normativos, sino a aspectos asociados al estado de avance del Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra en proceso de implementación progresiva.

Las acciones relacionadas con el desarrollo del MSPI están incorporadas en los instrumentos institucionales vigentes, particularmente en el Modelo Integrado de Planeación y Gestión (MIPG) y el Plan Estratégico de Tecnologías de la Información (PETI) 2023–2026, que establecen la hoja de ruta, los responsables y el cronograma de ejecución.

En consecuencia, las observaciones y recomendaciones fueron atendidas mediante los planes institucionales existentes, evitando la duplicidad de acciones y asegurando la coherencia, trazabilidad y sostenibilidad de los avances en materia de seguridad y privacidad de la información.

Finalmente, La Dirección de Planeación y Aseguramiento de la Calidad y el proceso Gestión TIC reitera su compromiso con la mejora continua, la implementación efectiva del MSPI y el fortalecimiento de la seguridad digital institucional, en cumplimiento de los lineamientos del Ministerio TIC y las políticas internas de la Institución Universitaria Pascual Bravo".

Pronunciamiento del equipo auditor:

Una vez analizada la respuesta y realizada la visita en sitio el 12 de noviembre de 2025, con el objetivo de socializar y concluir con respecto al informe prefinal de auditoría, el equipo auditor determino reformular el criterio de los hallazgos 1 y 3 y unificar los hallazgos 1 y 2 en el presente informe final de auditoría, de la siguiente manera:

OBSERVACIONES (HALLAZGOS) DE AUDITORÍA

Observación No. 01: Incumplimiento de la Resolución 00500 de 2021 y Decreto 767 de 2022

Criterio: Resolución 00500 de 2021 y Decreto 767 de 2022, los cuales establecen lineamientos, responsabilidades y requisitos para la gestión de la seguridad y privacidad de la información en las entidades públicas.

Condición:
Se evidenció que la institución no ha implementado ni aplica los requisitos establecidos en la Resolución 00500 de 2021 y Decreto 767 de 2022.

Causa:

- Desconocimiento o falta de capacitación sobre la norma.
- Ausencia de planeación estratégica en materia de seguridad de la información.
- Insuficiencia de recursos humanos y financieros destinados a la gestión de seguridad de la información.

Efecto:

- Posibles sanciones legales y administrativas.
- Riesgo reputacional institucional.

- Exposición elevada a incidentes de ciberseguridad y pérdida de información sensible.

Exposición al riesgo: Tipo: Estratégico
Nivel: Alto

Observación No. 02: Incumplimiento Guías para la administración del riesgo y el diseño de controles en entidades públicas versión 5 del 2020, versión 6 del 2022 y actualmente se encuentra vigente la Guía para la Gestión Integral del Riesgo en Entidades Públicas del 2025 versión 7 -

Criterio:
Incumplimiento Guías para la administración del riesgo y el diseño de controles en entidades públicas versión 5 del 2020, versión 6 del 2022 y actualmente se encuentra vigente la Guía para la Gestión Integral del Riesgo en Entidades Públicas del 2025 versión 7, las cuales establecen los lineamientos para la identificación, análisis, valoración y tratamiento de los riesgos de gestión, corrupción, seguridad digital y fiscales.

Condición:
Se evidenció desactualización en la política, guías y matrices asociadas a la administración de riesgos, lo cual impide una gestión oportuna y efectiva de los mismos.

Causa:

- Falta de capacitación del personal responsable.
- Limitación de recursos humanos y técnicos para la actualización y mantenimiento del sistema de gestión de riesgos.

Efecto:

- Aumento del riesgo reputacional institucional.
- Posible materialización de riesgos no gestionados adecuadamente.
- Deficiencias en la toma de decisiones estratégicas.

Exposición al riesgo: Tipo: Estratégico
Nivel: Alto

Conclusiones finales:

La Institución Universitaria Pascual Bravo cuenta con un Plan Estratégico de Tecnologías de la Información (PETI) vigente hasta 2026, lo que brinda un marco temporal claro para continuar fortaleciendo la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

La Institución dispone de estudios previos encaminados a la formalización de roles clave en Tecnologías de la Información, como el Oficial de Seguridad y Privacidad de la Información, y actualmente recibe acompañamiento del cuerpo directivo para avanzar en su definición y ubicación dentro de la estructura organizacional.

La Institución Universitaria Pascual Bravo cuenta con la política de seguridad y privacidad de la información (Acuerdo Directivo 031 del 16 de diciembre de 2021) constituye un insumo inicial importante; sin embargo, se encuentra en proceso de fortalecimiento para integrar elementos adicionales requeridos por el MSPI.

La Institución Universitaria Pascual Bravo cuenta con un avance de porcentaje en la implementación del MSPI de dominios 61% sobre 100 y clausulas 34% sobre 100, lo cual se refleja el compromiso de la Institución en consolidar y fortalecer progresivamente la implementación del modelo.

La Institución se encuentra avanzando en la elaboración de documentos esenciales tales como el alcance del MSPI, el manual de seguridad y privacidad, la definición detallada de roles, la estrategia de seguridad digital y políticas específicas para controles puntuales— los cuales se encuentran actualmente en fase de construcción, de acuerdo con lo verificado durante la visita en sitio.

Cordialmente,

WILLIAM ECHAVARRIA LOTERO
Jefe de la Dirección de Evaluación y Control