INSTITUCIÓN UNIVERSITARIA
MAYOR DE CARTAGENA

AVANZA
HACIA LA EXCELENCIA

Cartagena de Indias - Centro histórico
Cr 3 # 35-95 Calle de la Factoría.
Umayorctg umayorctg UMAYOR

INFORME AUDITORIA DE SOPORTE Y DESARROLLO TECNOLÓGICO

2024

OFICINA ASESORA DE CONTROL INTERNO

CONTENIDO

INTRODUCCION

La Oficina Asesora de Control Interno, en desarrollo al Plan Anual de Auditorías, aprobado por el Comité de Coordinación de Control Interno Institucional para la vigencia 2024, realizó auditoria al Proceso de Soporte y Desarrollo Tecnológico, con el objetivo de verificar el cumplimiento de las normas y requisitos vigentes legales de su competencia.

El presente informe tiene como objetivo proporcionar un análisis detallado sobre las actividades del Proceso de Soporte y Desarrollo Tecnológico conforme al alcance determinado en la apertura de la auditoria; esto con el fin de evaluar el impacto y los avances obtenidos en esta área clave de la organización. En un entorno organizacional cada vez más digitalizado, el desarrollo tecnológico se convierte en un elemento esencial para garantizar la eficiencia operativa, la innovación y la competitividad.

Este documento abarca tanto los esfuerzos en la gestión, el soporte técnico brindado a usuarios internos y externos, como los avances en el desarrollo de nuevas soluciones tecnológicas. De igual manera, se destacan los proyectos implementados, los desafíos enfrentados y las estrategias adoptadas para optimizar el uso de las tecnologías.

A través de este análisis, se busca identificar las áreas de oportunidad para mejorar los servicios y el proceso y, establecer las bases para una planificación futura orientada a la innovación y a la mejora continua. Además, se exponen las recomendaciones para fortalecer la unidad tecnológica, asegurando su alineación con los objetivos estratégicos de la organización y la satisfacción de sus usuarios.

Los resultados servirán para proporcionar a la alta dirección, así como a las partes interesadas, una visión clara y objetiva de los resultados de la auditoría, permitiendo la toma de decisiones que contribuyan a mejorar la eficiencia, la transparencia y el cumplimiento dentro de la organización.

I. Objetivos

1.1. Objetivo General:

Evaluar y verificar el grado de cumplimiento de las políticas, procedimientos, estrategias, normas internas y externas en la gestión realizada por el proceso de Soporte y Desarrollo Tecnológico, con el fin de medir la eficacia, la eficiencia, y garantizar el cumplimiento y aplicación de la normatividad vigente, de acuerdo al rol de evaluación y seguimiento y el rol de enfoque hacia la prevención; teniendo en cuenta que se orienta hacia una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de la Institución con el fin de cumplir sus objetivos organizacionales

1.2. Objetivos Específicos:

- Verificar el cumplimiento a las políticas de riesgos y sus controles.
- Lograr resultados de auditoría oportunos con el fin de informar y tomar las acciones correctivas y preventivas a que haya lugar.

II Alcance

- Verificación y evaluación del proceso en el último semestre 2023 y primer semestre 2024.
- Evaluar la gestión de riesgo de gestión, corrupción, fraude, tecnológico entre otros.
- Evaluar la efectividad de los controles a través del análisis de su diseño, ejecución y no materialización de los riesgos.

III Marco Legal

- Ley 87 de 1993**,** por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones"

- La Constitución Política de Colombia (1991)

- Ley 1712 de 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.

- Ley 1266 de 2008, Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

- Ley 1273 de 2009, por medio de la cual se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

- Ley 1581 de 2012, que proporcionando directrices específicas para la protección de datos personales.

- Ley 1474 de 2011 por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

- Ley 23 de 1982, sobre derechos de autor.

- Ley 1915 de 2018, la cual se modifica el régimen de derecho de autor, incluyendo la protección digital de contenidos y datos relacionados con derechos de autor.

- Ley 599 de 2000, por la cual se expide el Código Penal.

- Decreto 707 de 2022, por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- Decreto 1360 de 1989, por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor.

- Decreto 1499 de 2017 “Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015

- Decreto 1008 de 2018, por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones

- Decreto 886 de 2014, el cual establece sanciones por incumplimiento de la Ley 1581 de 2012 en cuanto a la protección de datos personales.

- Documento CONPES 3854, Política Nacional de Seguridad Digital.

- Documento CONPES 3975, Política Nacional para la Transformación Digital e Inteligencia Artificial, del 8 de noviembre de 2019. El Consejo Nacional de Política Económica y social (CONPES).

- Directiva Presidencial 02 del 2 de abril de 2019. Simplificación de la interacción digital los ciudadanos y el Estado.

- Norma Técnica Colombiana NTC- ISO/IEC Colombiana 27001:2013. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

• IV Criterios

Para el alcance y despliegue de esta auditoría, se tomó como referente el marco legal vigente, así como lo reglamentado por la Institución y que es aplicable al proceso. El desarrollo de esta se da a través de la confrontación legal con los soportes documentales y digitales facilitados por el proceso de Soporte y Desarrollo Tecnologico y, la utilización de las siguientes herramientas:

- Prueba de recorrido / Entrevistas
- Inspección y análisis de los documentos requeridos.

Lo anterior, permitió evaluar el proceso y poder entender con mayor exactitud el desarrollo de las actividades a cargo de la oficina auditada.

V. Metodología

Aplicación del procedimiento de auditoría interna y utilización de la Guía de auditoría interna basada en riesgos para entidades públicas versión 4 y 6, emitida por el Departamento Administrativo de la Función Pública.

- Solicitud de Información
- Concluir y documentar resultados.

Cartagena de Indias - Centro histórico
Cr 3 # 35-95 Calle de la Factoría.
Umayorctg umayorctg UMAYOR

VI. Aspectos reflejados en el desarrollo del proceso y resultados de la auditoria

El Proceso de Soporte y Desarrollo Tecnológico en las entidades públicas juega un rol importante en la transformación del panorama de la educación y otros sectores, convirtiéndose en un componente esencial para el desarrollo de la sociedad moderna. La integración de estas tecnologías ofrece numerosas ventajas que impulsan la eficiencia, la competitividad y la innovación. A continuación, se destacan algunas de las razones clave por las cuales la implementación de las Tecnologías de la Información y Comunicación es fundamental:

1. **Mejora de la eficiencia y productividad**: Permiten automatizar procesos, lo que reduce el tiempo y los recursos necesarios para llevar a cabo tareas repetitivas o manuales. Esto se traduce en un aumento significativo en la eficiencia y la productividad, tanto a nivel individual como organizacional.

2. **Acceso a la información en tiempo real**: Las tecnologías facilitan el acceso a la información en cualquier momento y desde cualquier lugar. Esto permite una toma de decisiones más informada y rápida, optimizando los procesos y mejorando la competitividad y acreditación de las organizaciones.

3. **Comunicación y colaboración mejoradas**: Permiten una interacción más fluida, tanto dentro de las organizaciones como entre sus públicos de interés.

4. **Fomento de la innovación**: La implementación de tecnologías avanzadas abre puertas a nuevas oportunidades y modelos operativos. El uso de herramientas digitales el big data y la computación en la nube, entre otras, fomenta la innovación y facilita la creación de productos y servicios novedosos.

5. **Mejora de la calidad del servicio**: En sectores como la educación, permiten una mejora significativa en la calidad del servicio.

6. **Reducción de costos operativos**: Puede ayudar a reducir los costos operativos al optimizar el uso de recursos, mejorar la gestión de inventarios, y automatizar procesos, lo que permite a las empresas ofrecer productos y servicios de manera más económica y eficiente.

7. **Desarrollo sostenible**: Juegan un papel fundamental en la promoción de prácticas sostenibles, como la gestión eficiente de recursos, la optimización de la cadena de suministro y la reducción de la huella de carbono. Además, facilitan la creación de soluciones tecnológicas que ayudan a abordar problemas globales, como el cambio climático.

8. **Acceso a recursos y materiales educativos**: permite que los estudiantes tengan acceso a una vasta cantidad de recursos educativos, como bibliotecas digitales, tutoriales en línea y contenidos especializados. Este acceso amplía las posibilidades de aprendizaje y permite a los estudiantes profundizar en sus áreas de interés.

Ahora bien, al revisar el proceso de Soporte y Desarrollo Tecnológico y específicamente los procedimientos de PR-ST-004 Administración copias de seguridad y restauración y PR-ST-006 Administración de licencias se observó lo siguiente:

Política de Seguridad de la Información

Como punto positivo de la gestión se resalta el cumplimiento e implementación de la Política de Seguridad de la Información. Es de recordar que, si bien la era digital ha facilitado el crecimiento y la prosperidad de las empresas, también ha provocado que sean más vulnerables a los ataques de ciberseguridad, especialmente en un entorno en el que la mayor parte de nuestras acciones cotidianas las realizamos en línea, por tanto, esta política que abarca estrategias claves como el mantenimiento preventivo y correctivo de equipos, protección de recursos informativos, copias de seguridad digital y restauración, uso de software , seguridad digital, tratamiento de datos personales, usos de licencias de software, gestión de incidentes de ciberseguridad, entre otros, es fundamental para el aseguramiento y protección de la información de la entidad.

Sin embargo, la oficina auditada no aportó evidencia de la socialización de esta política con la comunidad Umayor, lo que quebranta en cierta forma la efectividad, ya que si no se informa a quienes son los responsables de alguna de las actividades contenidas en el documento y general a los receptores de las medidas, su ejecución no podrá darse eficiencia requerida.

Decisiones basadas en datos

En cuanto a decisiones basadas en datos, se destaca que la entidad, a través de la oficina de Soporte y Desarrollo Tecnológico ha adquirido una licencia de Microsoft llamada Power Bi. Esta es una herramienta de análisis de datos, orientado a proporcionar visualizaciones interactivas, siendo una colección de servicios de software, aplicaciones y conectores que funcionan conjuntamente para convertir orígenes de datos sin relación entre sí, en información coherente, interactiva y atractiva visualmente

Datos Abiertos:

Son información pública dispuesta en formatos que permiten su uso y reutilización bajo licencia abierta y sin restricciones legales para su aprovechamiento. Lo anterior, se rige por la Ley 1712 de 2014 - Transparencia y Acceso a la Información

Pública Nacional, el cual define los datos abiertos en el numeral sexto como "*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".* De este modo, la Ley establece la obligatoriedad de las entidades públicas de divulgar datos abiertos, salvo las excepciones de acceso a la información.

Conforme a lo anterior la Guía para el uso y aprovechamiento de Datos Abiertos en Colombia establece el ciclo para el proceso de apertura, mejora y uso de datos abiertos, permitiendo que los responsables definan acciones a tomar en cada una de las fases estratégicas: construcción de plan de apertura, estructuración, comunicación y monitoreo, la implementación y seguimiento a estas actividades determinará la calidad de datos y usos de impacto.

En tal sentido y bajo los lineamientos de la guía en mención y las disposiciones del Decreto 767 de 2022 del Ministerio de las Tecnologías de la Información y las Comunicaciones se observó:

1. La entidad cuenta con el formato Inventario de Información Portal WEB donde los dantos están clasificados por el nivel (dependencia a cuál pertenece) y la descripción, pero falta el enlace (donde está publicado), y la vigencia en el cual fue creado. Así mismo, se logró evidenciar que el formato no se encuentra acorde al cambio de carácter de la entidad, ya que hace referencia a la Institución Tecnológica Colegio Mayor de Bolívar

2. No se evidencia Plan de apertura, mejora y uso de datos abiertos de la Institución. De acuerdo con la Guía para el uso y aprovechamiento de Datos Abiertos en Colombia del Ministerio de Tecnologías de la Información y las Comunicaciones Versión 6, en el numeral 4.1.1.2.1 el cual establece que se deberá complementar la matriz de los activos de información para el plan de apertura, mejora y uso de datos con sus respectivas variables.

3. Estrategias de comunicación, difusión, sensibilización y posicionamiento de los datos abiertos de la entidad: Se socializa mediante la página web de la Institución, a través de los cuales se realiza la promoción de los datos publicados para que la ciudadanía y usuarios en general los puedan usar y consultar.

De acuerdo a la Guía para el uso y aprovechamiento de Datos Abiertos, se sugiere ejecutar una "Encuesta de percepción de uso de Datos Abiertos" para conocer la opinión y percepción de los usuarios en cuanto al uso que se da a la información

institucional y estadística publicada. Lo anterior, con el fin de integrar a los diferentes actores y posicionar los datos abiertos de la Institución Universitaria Mayor de Cartagena.

Ahora bien, al revisar la Plataforma Nacional de Datos Abiertos de Colombia - datos.gov., se identificó que la institución no tiene suministro de información lo que la aleja de los incentivos propuestos por el gobierno, a aquellas entidades que usen la herramienta de impulso de la transferencia y toma de decisiones basada en datos públicos, entre los que se destaca, por la naturaleza y misionalidad de la Institución Universitaria Mayor de Cartagena, Datos a la U, que le permite a profesores y estudiantes, , promover el uso de datos en la academia, visibilizando los trabajos realizados por los equipos académicos de cualquier nivel de formación y generar reconocimiento.

Plan Estratégico de Tecnologías de Información y Comunicación – PETIC

Al revisar la información aportada se logró evidenciar que la unidad auditada actualizó recientemente el Plan y que este fue aprobado en el Comité Institucional de Gestión y Desempeño; no obstante, en la lectura de este, se identificó que la socialización, fase 4, se limita a la presentación a la alta dirección y no se describen las actividades de comunicación y sensibilización para socializar y apropiar el PETIC en la institución, como manifiesta la Guía Técnica de como estructurar el PETI Versión 1.0, en su ítem 2.9 Plan de Comunicaciones del PETI.

No obstante, en el mismo alcance del documento se indica que "*El PETIC (Plan Estratégico de Tecnologías de la Información y de las Comunicaciones), es un documento que* ***busca alinear los procesos de UMAYOR con las tecnologías****, cuyo objetivo es generar valor y cumplir eficientemente cada una de las metas propuestas. Este documento contiene las definiciones de las estrategias y los proyectos de renovación tecnológica para cada una de las áreas de UMAYOR a las cuales el equipo de Soporte y Desarrollo Tecnológico, soportará en el periodo del año 2022 a 2026, definiéndose los aspectos de arquitectura, sistemas de información y servicios a cada uno de los procesos* ***que desarrollan los usuarios internos en las diferentes dependencias de UMAYOR como también externos a la entidad.****"* (cursiva y negrita fuera del texto)

Conforme a lo anterior, este plan busca alinear los procesos y definir ciertos aspectos que al final serán desarrollados por los usuarios internos en las dependencias de la institución y los externos, por ende, deberá realizarse la socialización y sensibilización, con el fin de asegurar la efectividad y logro de los objetivos establecidos en esta estrategia.

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información – TRSPI

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Umayor es *"un documento estratégico que establece las acciones necesarias para mitigar, aceptar, transferir o evitar los riesgos identificados en los sistemas de información de la institución universitaria. Este plan se diseña en cumplimiento de los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), enmarcado en las políticas nacionales de seguridad digital, privacidad y protección de datos personales."*

Al revisar el TRSPI, se logró evidenciar la gestión y compromiso de la oficina auditada para avanzar en el cumplimiento de la Política de Seguridad Digital, estableciendo objetivos claros para fortalecer las actividades y metas, enfocadas a la seguridad y privacidad, alineados a la normatividad vigente.

No obstante a lo anterior, a la fecha no se cuenta con un inventario de activo de información, entendiéndose activo de información, "*como un recurso o elemento que contiene información con valor para la organización debido a su utilización en algún proceso o que tiene relación directa o indirecta con las funciones de la entidad: software, hardware, personas (roles), físicos (instalaciones, áreas de almacenamiento de expedientes, centros de procesamiento de datos), intangibles (imagen y reputación).*", conforme a la Función Pública Documento Técnico Marzo de 2020 - Seguridad de la Información

Referente a esta omisión, se debe indicar que es necesario que las entidades públicas identifiquen los activos de información y los documenten en un inventario de activos. De esta manera, podrá conocer que es lo que se debe proteger y así garantizar su buen funcionamiento interno y éste entorno al ciudadano.

Ahora bien, tal identificación y valoración debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso donde aplique la gestión del riesgo de seguridad de la información; pero es la oficina de Soporte y Desarrollo Tecnológico la encargada de orientarlo y consolidar el inventario en mención.

Como punto importante, se destaca que en el cronograma del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información ya se encuentra considerado para el año 2025 la implementación del inventario señalado.

Uso de Licencias de Software en conexidad con los Derechos de Autor

Las licencias de software es un contrato que proporciona directrices legalmente vinculantes para el uso y la distribución de software, es decir, se trata de un acuerdo

en el que el fabricante del software le otorga a una persona, empresa u organización un permiso para utilizar su producto.

El Decreto 1360 de 1989 artículo 1 indica que de conformidad con lo previsto en la Ley 23 de 1982 sobre Derechos de Autor, el soporte lógico (software) se considera como una creación propia del dominio literario. Esto otorga al autor derechos exclusivos de carácter moral y patrimonial, permitiéndole disponer del programa según su voluntad, siempre dentro de los límites legales.

De acuerdo al Centro Colombiano de Derechos de Autor "*Cualquier persona que pretenda utilizar una creación protegida, deberá contar, salvo las excepciones legales, con la autorización previa y expresa del autor, de sus derechos habientes o de los titulares de los derechos patrimoniales en el caso de tratarse de una obra sobre la cual operó la transferencia de los mismos. Sin su consentimiento, la utilización de la obra podría llegar a ser calificada judicialmente como ilícita por vulnerar derechos sobre la creación protegida, siendo probable la aplicación de sanciones de tipo civil y penal*" (cursiva fuera del texto)

En este sentido, el no contar con licencias de software autorizadas o vigentes, se constituye en una violación a los derechos de autor, delito que se encuentra tipificado el Código Penal Colombiano y que además configura un riesgo reputacional para las entidades de orden público y en algunos casos, podría aumentar la vulnerabilidad de la seguridad de la información quedando la institución propensa a ataques de ciberseguridad.

Al revisar la Matriz de Administración de Software y Licencias se identificó el vencimiento de la licencia del software ESET Antivirus, quebrantándose las políticas internas de seguridad de la información y materializándose posiblemente un riesgo reputacional y sancionatorio de tipo penal, así como traumatismos y reprocesos internos por no contar con una licencia vigente. Adicional se aporta captura de pantalla con las alertas del vencimiento.

Observaciones

Las observaciones se realizarán teniendo cuenta los riesgos contemplados en el Proceso de Soporte y Desarrollo Tecnológico y los requisitos legales.

1. La oficina auditada no aportó evidencias de socialización de la Política de Seguridad de la Información, lo que configura como una limitación para verificar el cumplimiento del alcance y objetivos contemplados en la política en mención, posiblemente por inobservancia de las directrices internas y que podría generar, desconocimiento de documento, falta de aplicabilidad y apropiación por parte de los funcionarios de la entidad, lo que podría generar, perdida de privacidad y seguridad de la información, así como de los activos informáticos tanto de hardware como de software frente amenazas internas o externas y accidentales.

2. La institución no cuenta con un Plan de apertura de Datos Abiertos. Lo anterior, se genera posiblemente, por desconocimiento de la norma en lo referente al Decreto 1081 de 2015 artículo 2.1.1.2.1.11 y la Ley 1712 de 2014 artículo 11 literal k publicación de Datos Abiertos y la Guía para el Uso y Aprovechamiento de Datos Abiertos en Colombia, que genera falta de confianza institucional por incumplimiento normativo y falta de accesibilidad y aprovechamiento de la información.

3. En el Inventario de Información Portal WEB están clasificados por el nivel (dependencia a cuál pertenece) y la descripción, pero no cuenta con un el

enlace de donde está publicado y la vigencia en el cual fue creado. Lo anterior, se genera posiblemente por el cumplimiento a los controles establecidos para la mitigación de riesgos, así mismo, por desconocimiento de la norma en lo referente al Decreto 1081 de 2015 artículo 2.1.1.2.1.11 y la Ley 1712 de 2014 artículo 11 literal k publicación de Datos Abiertos, lo que genera falta desconfianza institucional por no publicación de la información reglamentada por ley.

4. En el formato del documento Inventario de Información Portal WEB no se encuentra acorde al cambio de carácter de la entidad, ya que hace referencia a la Institución Tecnológica Colegio Mayor de Bolívar. Lo anterior, se genera posiblemente por el cumplimiento a los controles establecidos para la mitigación de riesgos de gestión dispuestos en el proceso Sistema Integrado de Gestión “Uso de documentos obsoletos por parte del personal y Desactualización del SIG” lo que genera falta de confianza institucional y posibles hallazgos en auditorias internar y externas.

5. Al Revisar el Plan Estratégico de Tecnologías de Información y Comunicación – PETIC, se identificó que la socialización, fase 4, se limita a la presentación a la alta dirección y no se describen las actividades de comunicación y sensibilización para socializar y apropiar el PETIC en la institución, como manifiesta la Guía Técnica de como estructurar el PETI Versión 1.0, en su ítem 2.9 Plan de Comunicaciones del PETI, así como el alcance de documento PETIT Umayor, posiblemente por inobservancia o desconocimiento de la norma, lo que quebranta la efectividad de los logros establecidos en la estrategia y la implementación adecuada de los Política de Gobierno Digital.

6. La entidad no cuenta con un inventario de activos de la información contraviniendo lo establecido en el Decreto 707 de 2022 elemento 3 Habilitador 3.2 y el Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas V4 numeral 3.1.6 Identificación de activos de información, posiblemente por inobservancia de la norma y falta de controles, lo que podría generar un perdida de la información, riesgos de incidentes; desconfianza institucional, pérdida de credibilidad y sanciones legales.

7. Al revisar la Matriz de Administración de Software y Licencias ve identificó el vencimiento de la licencia del software ESET Antivirus, quebrantándose las políticas internas de seguridad de la información, la Ley 23 de 1982 artículo 1, el Decreto 1360 de 1989 articulo 1 y la Ley 599 de 2022 articulo 271 y 272, posiblemente por desconocimiento o inobservancia de la norma y falta de controles de los riesgos establecidos por el proceso, materializándose posiblemente un riesgo reputacional y sancionatorio de tipo penal.

VIII. Conclusiones

El área de Soporte y Desarrollo Tecnológico dentro de la organización es adecuada y está alineada con los objetivos estratégicos y legales. Se resalta el compromiso del equipo y la entrega oportuna de la información, lo que permitió hacer un análisis y evaluación apropiada a los procesos contemplados en la dependencia auditada.

Es oportuno indicar, que la dependencia ha desplegado acciones para mejorar el cumplimiento de los lineamientos legales, tales como, la aplicación de la Política de Seguridad de la Información, que despliega la implementación de varias políticas fundamentales para el aseguramiento y protección de la información de la entidad. Así como la actualización del Plan Estratégico de Tecnologías de la Información y Comunicación – PETIC y la aplicación de Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información – TRSPI un documento estratégico que establece las acciones necesarias para mitigar, aceptar, transferir o evitar los riesgos identificados en los sistemas de información de la institución universitaria

Como oportunidades de mejora, el área deberá socializar y sensibilizar al personal de las estrategias actualizadas y establecidas, con el fin de garantizar la efectividad de las mismas.

VII. Recomendaciones

Conforme al análisis realizado a la dependencia auditada, la Oficina Asesora de Control Interno, realiza las siguientes recomendaciones:

1. Aplicar medidas de socialización de las estrategias implementadas para el cumplimiento de los lineamientos de la política de seguridad digital.

2. Divulgar, capacitar y sensibilizar a los funcionarios de la entidad, en relación al Plan Estratégico de Tecnologías de la Información y Comunicación – PETIC, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información y la Política de Seguridad de la Información.

3. Verificar la caracterización de los activos de información identificados en el documento Inventario de Información Portal WEB, con el fin de garantizar que cumpla con los criterios establecidos en la Ley 1712 de 2014.

4. Revisar los documentos contemplados en los procedimientos del proceso y verificar la actualización de los mismos.

5. Iniciar actividades necesarias que busquen implementar el Plan de apertura de Datos Abiertos.

6. Analizar la viabilidad de suministro de información en la Plataforma Nacional de Datos Abiertos de Colombia - Datos.gov, con el objetivo no solo de impulsar la transferencia y toma de decisiones basada en datos públicos sino de poder aplicar en los incentivos propuestos por el gobierno a las entidades que usen la herramienta.

7. Ejecutar en las fechas establecidas el cronograma de actividades del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información, con el fin de cumplir a inicios de 2025 con la creación del inventario de activos de la información

8. Hacer un seguimiento efectivo de licencias adquiridas por la entidad y realizar con anterioridad los procesos de renovación de las mismas. Evitando que estas sean adquiridas o renovadas tiempo después de su vencimiento.

ANEXOS

1. Sin anexos.

Para constancia se firma en Cartagena D.T. y C., a los diecinueve (19) días del mes de diciembre del año 2024.

APROBACIÓN DEL INFORME		
Nombre Completo	**Cargo**	**Firma**
Elizabeth Díaz Granados Beleño	Dir. Oficina Asesora de Control Interno.	Original firmado
EQUIPO DE AUDITORES		
Nombre Completo	**Cargo**	**Firma**
Maria Juliana Sierra Serpa Elaboró	Apoyo a la Oficina Asesora de Control Interno	Original firmado