Informe No. 101.4.2.19-2024

FECHA DE EMISIÓN DEL INFORME	Día:	26	Mes:	09	Año:	2024
Aspecto Evaluable (Unidad Auditable):	Auditoría Proceso Gestión de Tecnologías de la Información.					
Líder de Proceso / Jefe(s) Dependencia(s):	Luis Eduardo Ramírez Jerez Jefe Oficina de Tecnologías de la Información y las Comunicaciones					
Objetivo de la Auditoría:	Evaluar de manera integral la infraestructura de TI, la seguridad de la información, la gestión de riesgos, la gestión de activos, la gestión de proyectos, el cumplimiento normativo, la continuidad del negocio y la gestión de servicios de TI en la universidad.					
Alcance de la Auditoría:	El alcance de esta auditoría interna abarcó la evaluación y verificación del cumplimiento y la gestión a cargo únicamente del Proceso de Gestión de Tecnologías de la Información y las comunicaciones de la Universidad Colegio Mayor de Cundinamarca, donde se evaluó la gestión de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) en cada una de sus responsabilidades relacionadas con los siguientes temas: ***A.*** *Gestión de activos de TI* ***B.*** *Infraestructura de TI* ***C.*** *Gestión de servicios de TI* ***D.*** *Gestión de proyectos de TI* ***E.*** *Cumplimiento normativo* ***F.*** *Seguridad de la información* ***G.*** *Gestión de riesgos* ***H.*** *Continuidad del negocio y recuperación ante desastres.*					
Criterios de la Auditoría:	**Regulación y normas externas:** • Ley 1955 de 2019, Articulo 147, párrafo 1. – Circular_01_de_2022_Presidencia_de_la_Republica – Directiva_02_de_2022_Presidencia_de_la_Republica – Directiva_03_de_2022_Presidencia_de_la_Republica					

	• Decreto 620 de 2020 – ARTÍCULO 2.2.17.5.6. Seguridad de la información y Seguridad Digital ▪ Estándares actualizados definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). · Modelo de Arquitectura Empresarial (MAE) · Modelo de Gestión y Gobierno de TI (MGGTI) · Modelo de Gestión de Proyectos (MGPTI) – ARTÍCULO 2.2.24.3.12. Nivel Operativo. NTC-ISO/IEC 27001:2022 – Requisitos, Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales

Reunión de Apertura						Ejecución de la Auditoría				Reunión de Cierre					
Día	28	**Mes**	06	**Año**	2024	**Desde**	08/07/2024 D / M / A	**Hasta**	22/08/2024 D / M / A	**Día**	26	**Mes**	09	**Año**	2024

Jefe oficina de Control Interno	Auditor Líder
AFRANIO SOTO MONTERO	NICOLAS ALEJANDRO VILLAMIL GUTIERREZ

RESUMEN EJECUTIVO

PRINCIPALES SITUACIONES DETECTADAS/ RESULTADOS DE LA AUDITORÍA / RECOMENDACIONES

HALLAZGO GENERAL

1. **Deficiencias en la entrega de información para la Auditoría de Gestión de TI.** De acuerdo con el artículo séptimo, numeral 2, de la Resolución No. 1709 de 2021, que adopta el Estatuto de Auditoría Interna en la Universidad, los líderes de proceso tienen la responsabilidad de reportar la información requerida para los ejercicios de aseguramiento de manera oportuna y en las condiciones técnicas y metodológicas solicitadas por la Oficina de Control Interno. Se evidenció que la Oficina de Tecnologías de la Información y las

Comunicaciones (OTIC) no entregó información correspondiente a 9 de los 39 requerimientos solicitados mediante el memorando No. 20241010010283, incluyendo documentos como registros de incidentes de seguridad, indicadores de desempeño de servicios de TI, encuestas de satisfacción de usuarios, registro de lecciones aprendidas de proyectos, registro de cumplimiento normativo, procedimientos de gestión de incidentes de seguridad, plan de implementación del SGSI, plan de continuidad del negocio para TI, procedimientos de recuperación ante desastres y registros de pruebas de continuidad. Adicionalmente, se observó que la OTIC entregó documentación no relacionada directamente con varios requerimientos de la auditoría, incluyendo temas de gestión de servicios de TI, gestión de proyectos, y cumplimiento normativo. Esta situación se origina por la inexistencia de parte de la documentación solicitada en la OTIC y por dificultades en la interpretación de los requerimientos de la auditoría. Como consecuencia, se obstaculiza una evaluación completa de la gestión de TI, lo que puede resultar en la no detección de aspectos relevantes en la gestión de servicios de TI, seguridad de la información y ciberseguridad. Esto podría afectar la toma de decisiones sobre la priorización de servicios de TI y potencialmente impactar la disponibilidad y calidad de los servicios tecnológicos para la comunidad universitaria.

HALLAZGOS ESPECÍFICOS

A. GESTIÓN DE ACTIVOS DE TI

2. **Deficiencias en la gestión integral de activos de TI.** De conformidad con los lineamientos MGGTI.LI.GO.01, MGGTI.LI.GO.10, MGGTI.LI.ST.01, MGGTI.LI.ST.02, y MGGTI.LI.ST.09 de la Guía de Dominio de Gobierno de TI y Gestión de Servicios de TI, se debe implementar un esquema de Gobierno TI que incluya políticas, un catálogo actualizado de servicios tecnológicos y planes de mantenimiento. Se evidenció que la OTIC carece de una estructura integral para la gestión de activos de TI, incluyendo:
    a. Ausencia de una definición formal y aprobada de los perfiles de cargo (y/o funciones) y competencias para el personal que realiza y/o lidera los procesos de TI de la OTIC,
    b. Ausencia de una matriz de roles y responsabilidades claramente definida,
    c. Falta de una metodología para la clasificación de activos de TI basada en su dependencia e impacto,
    d. Ausencia de un método de identificación y valoración de activos de información,
    e. Inexistencia de un repositorio centralizado para la gestión de activos de TI, y
    f. Deficiencias en la gestión del ciclo de vida completo de los activos de TI.

Esta situación se origina por la ausencia de un enfoque estructurado y holístico en la gestión de activos de TI, debido a la reciente creación de esta oficina y la ausencia de políticas y procedimientos formales alineados a sus procesos de TI y la falta de liderazgo estratégico. Como consecuencia, la universidad enfrenta múltiples riesgos, incluyendo: gestión ineficiente de activos críticos, posibles brechas de seguridad, dificultades en la priorización de recursos para la protección y mantenimiento de activos, potencial incumplimiento normativo, y exposición a interrupciones operativas significativas que podrían afectar la disponibilidad y calidad de los servicios académicos y administrativos.

B. INFRAESTRUCTURA DE TI Y C. GESTIÓN DE SERVICIOS DE TI

3. **Vulnerabilidades en la seguridad y gestión de la infraestructura y servicios de TI.** De conformidad con los lineamientos MGGTI.LI.ST.13, MGGTI.LI.ST.10, MGGTI.LI.ST.05, MGGTI.LI.ST.04, y MGGTI.LI.ST.11 de la Guía de Dominio de Gestión de Servicios de TI, se deben implementar controles de seguridad, monitorear los recursos y servicios de TI, garantizar su alta disponibilidad, y contar con mecanismos de respaldo. Se evidenciaron múltiples deficiencias, incluyendo:
    a. Fallas en los controles y políticas de monitoreo y restricción de navegación segura,
    b. Deficiencias en el control de instalación de software no autorizado,
    c. Ausencia de un sistema de monitoreo proactivo para infraestructura y servicios de TI,
    d. Insuficientes controles de seguridad para el acceso a los servicios de TI,
    e. Ausencia de un proceso de endurecimiento (hardening) de sistemas,
    f. Falta de redundancia en sistemas críticos como el de climatización del Centro de Cómputo,
    g. Ausencia de un programa de pruebas planificado para sistemas de energía de respaldo, y
    h. Deficiencias en la gestión de respaldos y pruebas de restauración.

    Esta situación se origina por la implementación inadecuada de controles de seguridad, la falta de inversión en herramientas de monitoreo, y la ausencia de procesos de gestión proactiva de servicios e infraestructura. Como consecuencia, la universidad está expuesta a riesgos críticos de seguridad, incluyendo posibles brechas de datos, accesos no autorizados, compromisos de sistemas, y potenciales violaciones de cumplimiento normativo. Además, aumenta el riesgo de interrupciones no planificadas en los servicios de TI, daños a equipos críticos, y pérdida de datos, lo que podría resultar en interrupciones prolongadas de servicios académicos y administrativos críticos, pérdidas financieras significativas, y un impacto negativo en la reputación de la institución.

C. GESTIÓN DE PROYECTOS DE TI

4. **Deficiencias significativas en la gestión y seguimiento de proyectos de TI.** Según los lineamientos MGPTI.LI.CES.05, MGPTI.LI.EJC.02, y MGPTI.LI.EJC.01 de la Guía de Dominio de Contexto Estratégico y Ejecución y Control, las entidades deben seleccionar una metodología adecuada para gestionar proyectos de TI, evaluar periódicamente su desempeño, y contar con un repositorio para la documentación de proyectos. Se evidenció que la OTIC:
    a. Carece de una metodología formalmente definida para la gestión de proyectos de TI,
    b. Presenta inconsistencias significativas en el seguimiento y reporte de avances de los proyectos, y
    c. No cuenta con un repositorio centralizado y estructurado para la documentación de los proyectos.

    Esta situación se debe a la ausencia de lineamientos claros por parte de la Jefatura de la OTIC, la falta de procedimientos estandarizados para el seguimiento y control de proyectos, y la falta de implementación de herramientas y procesos para la gestión documental de los proyectos. Como consecuencia, existe un alto riesgo de desviaciones significativas en alcance, tiempo y costos de los proyectos de TI, toma de decisiones basada en información inexacta, un potencial detrimento patrimonial y fracaso en la implementación de iniciativas estratégicas de TI. Esto podría resultar en una utilización ineficiente de recursos, retrasos en la modernización de los sistemas de la universidad, y una disminución en la capacidad de la institución para alcanzar sus objetivos estratégicos a través de la tecnología.

D. SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE RIESGOS DE TI

5. **Deficiencias en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) y en la gestión de riesgos de TI.** De conformidad con el lineamiento MGGTI.LI.ST.13 de la Guía de Dominio de Gestión de Servicios de TI, se deben implementar controles de seguridad informática y gestionar los riesgos asociados a la infraestructura tecnológica. Se evidenciaron múltiples deficiencias, incluyendo:
    a. Inconsistencias en la documentación y avance del MSPI,
    b. Ausencia de una metodología aprobada para la identificación de activos de información,
    c. Ausencia de una metodología aprobada para gestionar los riesgos de TI, Seguridad de la información y Ciberseguridad,
    d. Identificación incompleta de riesgos de TI,

e. Falta de evaluación de controles de TI para los riesgos identificados, y
f. Metodología de riesgos inadecuada para activos de TI.

Esta situación se origina por la falta de un proceso riguroso de implementación del MSPI, deficiencias en la priorización de las actividades de seguridad de la información, y la ausencia de un enfoque sistemático y exhaustivo para la identificación y gestión de riesgos de TI. Como consecuencia, la universidad está expuesta a un incremento significativo en el riesgo de brechas de seguridad no identificadas, incumplimiento de estándares de seguridad, y una falsa sensación de seguridad. Esto podría resultar en la exposición de datos sensibles, incumplimiento de regulaciones de protección de datos, dificultades para implementar controles de seguridad apropiados, y una exposición incrementada a amenazas tecnológicas, comprometiendo potencialmente la disponibilidad, integridad y confidencialidad de los sistemas e información de la universidad.

E. CONTINUIDAD DE NEGOCIO Y RECUPERACIÓN ANTE DESASTRES

6. **Ausencia de documentación esencial para la continuidad del negocio y recuperación ante desastres en TI.** De acuerdo con el lineamiento MGGTI.LI.ST.04 - Continuidad y disponibilidad de los Servicios de TI de la Guía de Dominio de Gestión de Servicios de TI, se debe garantizar la continuidad y disponibilidad de los servicios de TI. Se evidenció la inexistencia del plan de continuidad del negocio para TI, procedimientos de recuperación ante desastres y registros de pruebas de continuidad. Esta situación sugiere una grave deficiencia en la preparación para eventos disruptivos, posiblemente debido a la falta de priorización de la resiliencia operativa por parte de la Jefatura de la OTIC. La ausencia de estos documentos y procedimientos expone a la universidad a un alto riesgo de interrupción prolongada de servicios críticos en caso de un incidente mayor, lo que podría resultar en pérdidas financieras significativas, interrupción de actividades académicas, y daño severo a la reputación institucional. Además, la falta de pruebas documentadas de continuidad sugiere que, incluso si existen planes de recuperación por parte del proveedor de servicios de hosting (iFX), su eficacia no ha sido verificada, aumentando aún más el riesgo de fallo en situaciones de crisis.

RECOMENDACIONES

RECOMENDACIÓN GENERAL:

Implementar un programa integral de mejora de la gestión documental y procesos de TI en la OTIC. Establecer un repositorio centralizado para la documentación de TI, utilizando las herramientas colaborativas existentes. Desarrollar un proceso formal de generación, revisión y actualización de documentos, asignando roles y responsabilidades claros.

Crear una matriz de mapeo entre los requerimientos comunes de auditoría y la documentación de TI existente. Implementar un sistema de revisión por pares para las respuestas a auditorías y solicitudes de información. Complementar estas acciones con un programa de capacitación continua para el personal de la OTIC, enfocado en la importancia de la documentación, los procesos de TI y su impacto en la gestión efectiva de los servicios tecnológicos. Establecer revisiones trimestrales para evaluar el progreso y ajustar el programa según sea necesario.

RECOMENDACIONES ESPECIFICAS:

1. GESTIÓN DE ACTIVOS DE TI

Para abordar las deficiencias en la gestión de activos de TI, se recomienda implementar un marco de gobierno de TI que incluya una matriz RACI (Responsible, Accountable, Consulted, Informed) claramente definida para la definición y gestión de los procesos de TI de la OTIC. Este marco debe establecer roles y responsabilidades específicos para cada aspecto de la gestión de activos, desde la adquisición hasta la disposición final. Paralelamente, es crucial desarrollar una metodología de clasificación de activos basada en su criticidad e impacto en los procesos institucionales. Esta metodología debe incluir criterios claros para evaluar la importancia de cada activo y determinar los niveles apropiados de protección y mantenimiento. Adicionalmente, se debe implementar un repositorio centralizado para la gestión de activos de TI, utilizando herramientas existentes o soluciones de código abierto para minimizar costos. Este repositorio debe integrarse con los procesos de gestión de cambios y configuración para mantener un inventario actualizado y preciso de todos los activos de TI.

Implementar un proceso automatizado de gestión del ciclo de vida de cuentas de usuario de correo electrónico, incluyendo la revisión periódica y desactivación de cuentas inactivas en servicios de almacenamiento en la nube para optimizar el uso de recursos.

2. INFRAESTRUCTURA DE TI

Para fortalecer la gestión de la infraestructura de TI, se recomienda implementar un sistema de monitoreo proactivo utilizando herramientas de código abierto o aprovechando mejor las capacidades de los sistemas existentes. Este sistema debe configurarse para alertar sobre problemas potenciales antes de que afecten a los usuarios finales. Además, es importante establecer procedimientos documentados para la gestión de la capacidad y la disponibilidad de los servicios de TI, incluyendo la planificación regular de la capacidad y la realización de pruebas de carga. Se debe también implementar un proceso formal de gestión de parches y

actualizaciones para todos los sistemas críticos, asegurando que se mantengan actualizados y protegidos contra vulnerabilidades conocidas.

Establecer y mantener un sistema de etiquetado e identificación estandarizado para todos los componentes de infraestructura, incluyendo una revisión periódica para asegurar su precisión y actualización.

3. SEGURIDAD DE LA INFORMACIÓN

Establecer un comité de supervisión del MSPI liderado por el Oficial de Seguridad de la Información y el Jefe de la OTIC para revisar y validar trimestralmente la documentación, los roles asignados y el progreso real de la implementación del Modelo de Seguridad y Privacidad de la Información, asegurando su alineación con la última versión de la NTC-ISO/IEC 27001:2022 y los objetivos estratégicos de la universidad.

Para mejorar la seguridad de la información, es imperativo desarrollar y aplicar una política integral de seguridad que aborde las vulnerabilidades identificadas. Esta política debe incluir directrices claras sobre el control de acceso, la gestión de software, y la seguridad física de los activos de TI. Se recomienda implementar un proceso de revisión periódica de los controles de seguridad, incluyendo auditorías regulares de los permisos de usuario y las configuraciones de los sistemas. Además, es crucial establecer un programa de concientización en seguridad de la información para todos los empleados, enfocado en temas como la navegación segura, el uso apropiado de los recursos de TI, y la identificación de amenazas de seguridad. Para abordar las deficiencias en el control de instalación de software, se debe implementar un proceso de gestión de cambios que incluya la aprobación y documentación de todas las instalaciones de software en los sistemas de la universidad.

4. GESTIÓN DE SERVICIOS DE TI

Desarrollar y mantener un catálogo de servicios de TI documentado y estructurado, que incluya descripciones claras, niveles de servicio, componentes de TI claves y responsables para cada servicio ofrecido por la OTIC.

Implementar un proceso formal de planificación de capacidad y disponibilidad para los servicios de TI, que incluya revisiones periódicas y proyecciones de crecimiento para asegurar la asignación proactiva de recursos.

Establecer un repositorio centralizado para la documentación de proyectos de TI, utilizando herramientas colaborativas existentes o sistemas de gestión de documentos para mejorar la accesibilidad y trazabilidad de la información de los proyectos.

5. GESTIÓN DE PROYECTOS DE TI

Para mejorar la gestión de proyectos de TI, se recomienda adoptar una metodología de gestión de proyectos estandarizada, como PRINCE2 o una versión adaptada de PMBOK, que se ajuste a las necesidades y recursos de la universidad. Esta metodología debe incluir procesos claros para la iniciación, planificación, ejecución, monitoreo y cierre de proyectos. Es crucial establecer un comité de gobierno de proyectos de TI que supervise todos los proyectos significativos, asegurando la alineación con los objetivos estratégicos de la universidad y la adecuada asignación de recursos. Además, se debe implementar un sistema de gestión de portafolio de proyectos, utilizando herramientas simples como hojas de cálculo compartidas o plataformas de colaboración existentes, para mejorar la visibilidad y el seguimiento de todos los proyectos de TI.

6. GESTIÓN DE RIESGOS DE TI

Para fortalecer la gestión de riesgos de TI, se recomienda desarrollar y aplicar una metodología de evaluación de riesgos específica para TI, que se integre con el marco general de gestión de riesgos de la universidad. Esta metodología debe incluir procesos para la identificación, evaluación, tratamiento y monitoreo continuo de los riesgos de TI. Es importante establecer un registro de riesgos de TI que se revise y actualice regularmente, con responsables claros para cada riesgo identificado. Además, se debe implementar un proceso de evaluación de impacto en la privacidad y la seguridad para todos los nuevos sistemas y cambios significativos en los sistemas existentes.

7. CONTINUIDAD DE NEGOCIO Y RECUPERACIÓN ANTE DESASTRES

Para mejorar la preparación ante eventos disruptivos, es crucial desarrollar y documentar un plan de continuidad del negocio para TI y procedimientos de recuperación ante desastres. Estos planes deben estar basados en un análisis de impacto en el negocio (BIA) que identifique los sistemas y servicios críticos de la universidad. Se recomienda establecer un programa regular de pruebas y ejercicios de continuidad, comenzando con pruebas de escritorio y avanzando gradualmente hacia simulacros más complejos. Es importante también desarrollar y mantener documentación detallada de los procedimientos de recuperación para cada sistema crítico, asegurando que esta información esté accesible en caso de un evento disruptivo.

CONCLUSIONES DE LA AUDITORÍA

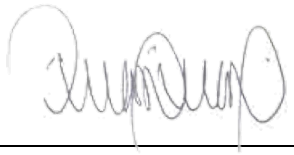
La evaluación de la gestión de TI en la universidad identifica oportunidades de mejora en todas las áreas auditadas. Los procesos, controles y prácticas de TI actuales presentan aspectos que requieren atención prioritaria en términos de seguridad de la información, continuidad de negocio y cumplimiento normativo. Se recomienda una intervención estructurada para abordar estas áreas, desarrollar la implementación y madurez de los procesos de TI y alinearlos con las prácticas del sector y los requerimientos normativos aplicables propuestos por el MinTIC.

A. **Infraestructura de TI:** La infraestructura de TI presenta aspectos que requieren atención en seguridad, disponibilidad y eficiencia. Se identificaron oportunidades de mejora en los controles de seguridad, incluyendo el acceso web y la instalación de software. La redundancia en sistemas críticos y las pruebas de sistemas de respaldo son áreas que requieren revisión para minimizar potenciales interrupciones de servicio.
B. **Seguridad de la Información:** El estado de la seguridad de la información presenta oportunidades de mejora. Se identificaron aspectos a fortalecer en los controles de acceso a servicios de TI, procesos de endurecimiento de sistemas y seguridad física de la infraestructura. Estas áreas requieren atención para reducir potenciales riesgos de seguridad y protección de datos.
C. **Gestión de Riesgos:** La gestión de riesgos de TI presenta áreas de oportunidad para alinearse con las prácticas del sector. Se identificó la necesidad de implementar procesos sistemáticos para la identificación y evaluación de riesgos, así como de adaptar la metodología de riesgos a los activos de TI específicos de la universidad.
D. **Gestión de Activos:** La gestión de activos de TI presenta oportunidades de mejora. Se recomienda implementar una metodología para la clasificación de activos basada en criticidad e impacto, así como un método de identificación y valoración de activos de información. La implementación de un repositorio centralizado y procesos formales para la gestión del ciclo de vida de los activos podría fortalecer la gestión operativa y de seguridad.
E. **Gestión de Proyectos:** La gestión de proyectos de TI presenta áreas de oportunidad en la implementación de una metodología establecida y en el seguimiento y control. La implementación de un repositorio centralizado para la documentación de proyectos podría mejorar la trazabilidad y el aprendizaje organizacional.
F. **Cumplimiento Normativo:** Se identificaron oportunidades de mejora en la adherencia a los lineamientos establecidos por el MinTIC en el Modelo de Gestión y Gobierno de TI (MGGTI) y el Modelo de Gestión de Proyectos de TI (MGPTI). La implementación de documentación crítica y la adhesión a las guías de dominio en áreas como gestión de servicios, seguridad y continuidad de negocio podrían fortalecer el cumplimiento normativo.

G. **Continuidad de Negocio:** La preparación para la continuidad del negocio y recuperación ante desastres en TI presenta áreas de oportunidad. Se recomienda la implementación de documentación esencial como el plan de continuidad de negocio para TI, procedimientos de recuperación ante desastres y registros de pruebas de continuidad para fortalecer la resiliencia operativa, cibernética y organizacional.

H. **Gestión de Servicios de TI:** La gestión de servicios de TI presenta oportunidades de mejora y fortalecimiento que involucren aspectos técnicos propios de la Seguridad de la Información y la ciberseguridad. La implementación de un catálogo de servicios documentado, procesos formales de gestión de cambios y fortalecimiento de la gestión de respaldos y pruebas de restauración podrían mejorar la calidad y confiabilidad de los servicios ofrecidos a la comunidad universitaria.

Para constancia se firma en Bogotá D.C., a los 26 días de septiembre de 2024.

APROBACIÓN DEL INFORME DE AUDITORÍA		
Nombre Completo	**Responsabilidad (cargo)**	**Firma**
AFRANIO SOTO MONTERO	Jefe Oficina de Control Interno Supervisor	
NICOLAS ALEJANDRO VILLAMIL GUTIÉRREZ	Auditor Líder