UNIVERSIDAD MILITAR NUEVA GRANADA

INFORME DE AUDITORIA CONTROL INTERNO	**Fecha Emisión:** 2024/04/10	GI-MA-F-17
	Revisión No.: 2	Página 1 de 96

FECHA DE EMISIÓN DEL INFORME PRELIMINAR	**Día:**	22	**Mes:**	octubre	**Año:**	2024

FECHA DE EMISIÓN DEL INFORME FINAL	**Día:**	29	**Mes:**	noviembre	**Año:**	2024

1. INFORMACIÓN GENERAL

Macroproceso:	*Planeación estratégica*
Proceso:	*Gestión Estratégica TIC*
Líder de Proceso / Jefe(s) Dependencia(s):	*Capitán (RA) Ricardo Ariza Urango - Jefe Oficina de las Tecnologías y las Comunicaciones*
Representante Alta Dirección	*Rector – MG (R) Javier Alberto Ayala Amaya*
Objetivo de la Auditoría:	*Determinar el nivel de madurez de seguridad de la información, ciberseguridad y privacidad de datos de acuerdo con los principales marcos establecidos, normatividad y legislación relacionada, así como identificar áreas de mejora potencial del sistema de gestión en el marco de la seguridad de la información, ciberseguridad y privacidad de datos.*
Alcance de la Auditoría:	*Gestión Estratégica de TIC y todos los procesos de la organización relacionados a la seguridad de la información, ciberseguridad y privacidad de datos, abordando evidencias del segundo semestre de la vigencia 2023 y lo corrido de la vigencia 2024.* **Sedes:** **Sedes Bogotá** - *Carrera 11 n.° 101-80 (Bogotá, Colombia)* - *Facultad de Medicina y Ciencias de la Salud Transversal 3 n.° 49-00* - *Sede Posgrados calle 94 A # 13 - 54* **Sede Campus Nueva Granada** *Kilómetro 2, vía Cajicá-Zipaquirá*

Criterios de la Auditoría:	• *NTC ISO IEC 27001:2022,* • *NTC ISO IEC 27701:2020,* • *GTC ISO IEC 27032:2023, Marco de Ciberseguridad NIST 2.0,* • *GI-PR-M-13 Manual de procesos y Documentación SIG V16,* • *GI-PR-M-1 Manual Integral de Gestión V19,* • *Documentos legales, reglamentarios y contractuales aplicables al alcance del sistema de gestión integrado y a las normas de requisitos de gestión.*
Auditor Líder	***Germán Andrés Sánchez Ortegón***
Experto técnico	***Miguel Ángel Suárez Benítez***

Reunión de Apertura						**Ejecución de la Auditoría**				**Cierre Proceso de Auditoría**					
Día	23	Mes	09	Año	202	Desde	23/09/2024 D / M / A	Hasta	02/10/2024 D / M / A	Día	07	Mes	10	Año	2024

4. RESULTADOS DE AUDITORÍA

4.1 ASPECTOS RELEVANTES

1. Se evidenció la asignación de recursos para la implementación y el mantenimiento del sistema de gestión de seguridad de la información, ciberseguridad y protección de la privacidad lo cual permite evidenciar un manejo robusto y eficaz que apoya la misión y visión organizacional.

2. Se evidenció que la Universidad cuenta actualmente con un sistema de gestión integrado con las siguientes certificaciones en: NTC ISO 9001:2015, NTC ISO 14001:2015, NTC ISO 45001:2018, Decreto 1072 de 2015 y se tiene previsto obtener para el año 2025 las certificaciones en NTC ISO 21001:2019 y Basura cero. De igual manera se tiene planeado certificarse en el 2025 en NTC ISO IEC 27001:2022, esto permite evidenciar un compromiso real, lo cual refuerza la competitividad, reputación y compromiso de la Universidad con la calidad, la seguridad, la sostenibilidad y la protección de la información, lo que puede atraer más interés y confianza de la comunidad académica y de los sectores externos. De igual manera facilita los procesos de integración en la implementación de los nuevos modelos previstos a futuro.

3. Se evidenció que actualmente se están presentando proyectos de conformación del equipo de trabajo con roles y cargos para el fortalecimiento de la estructura actual de la seguridad, ciberseguridad y la protección de la privacidad:
    - CISO
    - Asesor de Ciberseguridad

- Asesor de Continuidad del Negocio
- Asesor Base de Datos
- Asesor Seguridad de la Información

La conformación de un equipo de trabajo con roles especializados en seguridad, ciberseguridad y protección de la privacidad fortalece la estructura institucional de la Universidad y proporciona un enfoque estratégico y técnico para proteger la información y los activos relacionados de la comunidad académica, adicionalmente permite mitigar los riesgos cibernéticos, asegurar la continuidad operativa, realizar una gestión segura de base de datos y fortalecer el cumplimiento normativo y regulatorio.

4. Se evidenció el inicio de la formación de implementadores y auditores líderes a 50 funcionarios, la realización de actividades complementarias y la ejecución de la Campaña tips Cybertech y el uso de la herramienta FORTINET Training Institute, estas actividades aseguran que la Universidad cuente con un equipo capacitado para gestionar de manera adecuada la seguridad, ciberseguridad y protección de la privacidad y garantice el cumplimiento de las normativas y regulaciones nacionales e internacionales en cuanto a protección de datos, tales como la Ley 1581 de 2012 en Colombia o incluso el GDPR (General Data Protection Regulation, por sus siglas en inglés) Reglamento General de Protección de Datos de la Unión Europea (UE), en caso de tener actividades internacionales. Estas campañas de concienciación son esenciales para involucrar a toda la comunidad universitaria (estudiantes, docentes y administrativos) en la adopción de buenas prácticas en seguridad permitiendo crear una cultura de seguridad. Es importante resaltar que la cultura de seguridad no solo depende del equipo especializado, sino también de la actitud y los conocimientos de cada individuo que interactúa con la información y activos relacionados de la Universidad. Esta formación garantiza que los procesos internos sean auditables y conformes a estándares internacionales.

5. Se evidenció el uso de la herramienta EndPoint Sentinel One, herramienta de ciberseguridad de próxima generación que utiliza inteligencia artificial y aprendizaje automático para detectar, prevenir y responder a una amplia gama de amenazas de manera eficiente. Lo anterior, permite a la Universidad contar con la protección avanzada y automatizada contra amenazas cibernéticas en los dispositivos y sistemas que forman parte de la infraestructura tecnológica de la Institución.

6. Se evidenció la realización de ejercicios de análisis de vulnerabilidad realizado en noviembre del año 2023 y la cobertura de monitoreo con herramientas como AXUR. Estos análisis de vulnerabilidad permiten identificar puntos débiles en la infraestructura tecnológica de la Universidad, tales como servidores, redes, aplicaciones y dispositivos conectados. Esto es fundamental para detectar vulnerabilidades antes de que los atacantes puedan explotarlas. Al evidenciar estos ejercicios, la Universidad demuestra que está tomando medidas proactivas para prevenir incidentes de seguridad, como el robo de datos o ataques de ransomware.

7. Se evidenció la competencia del personal que lidera y participa en el sistema de gestión de seguridad de la información como son el caso del líder del proceso, el CISO (Chief Information Security Officer, por sus siglas en inglés) y el equipo que conforma el proceso, lo cual ha permitido adoptar nuevas tecnologías y mejores prácticas, asegurando que el sistema se mantenga actualizado y efectivo frente a nuevas amenazas. Un equipo competente asegura que la Universidad no solo pueda prevenir y mitigar riesgos, sino también adaptarse y mejorar continuamente, contribuyendo así al éxito y la sostenibilidad de la Institución en un entorno cada vez más digital y complejo.

8. Se evidenció un entorno tecnológico robusto que permite la integración de soluciones de seguridad actualizadas, facilitando una protección constante de los activos de información y garantizando la continuidad operativa de los sistemas. Además, la alta implementación de controles tecnológicos asegura que las políticas y procedimientos de seguridad se apliquen de manera coherente y efectiva, minimizando vulnerabilidades y fortaleciendo la resiliencia ante incidentes de seguridad.

9. Se evidenció la sólida configuración del directorio activo y el control de acceso implementado a través de él, esto garantiza que solo los usuarios autorizados puedan acceder a los sistemas y datos adecuados, minimizando el riesgo de accesos no autorizados y mejorando el control sobre las operaciones internas.

10. Se evidenció una infraestructura diseñada bajo un proceso de virtualización robusto, lo cual permite la optimización de recursos y la flexibilidad, la eficiencia operativa, la reducción de costos, y asegurar una mayor escalabilidad y resiliencia de los sistemas tecnológicos.

11. Se evidenció la buena gestión de accesos, la cual evidencia una adecuada y oportuna desactivación de privilegios a los funcionarios retirados de la organización.

12. Se evidenció la implementación de controles de seguridad física aplicados en las instalaciones, alineadas a prácticas del sector militar, lo cual brinda mayor confianza a las partes interesadas en el manejo de los activos de información.

4.2 RECOMENDACIONES

1. Se evidencia la necesidad de definir el alcance del sistema de seguridad, ciberseguridad y protección de la privacidad, revisar y delimitar de forma precisa el alcance del sistema de gestión para asegurar que cubra todas las áreas críticas y procesos relevantes de la UMNG. Esto ayudará a optimizar los recursos y esfuerzos destinados a la protección de la información y fortalecerá la capacidad de la UMNG para enfrentar amenazas y cumplir con sus objetivos estratégicos.

2. Se evidencia la necesidad de identificar partes interesadas “dañinas” adicionales, ampliar el análisis de las partes interesadas para incluir actores que podrían ser potencialmente

perjudiciales para la organización, con el objetivo de desarrollar estrategias de mitigación más específicas y efectivas. Este enfoque permite una gestión proactiva de los riesgos y ayuda a proteger mejor los activos de información críticos, alineándose con estándares como el Marco de Ciberseguridad NIST, que promueven un análisis robusto de partes interesadas.

3. Se evidencia la necesidad de incluir las siguientes organizaciones, Superintendencia de Industria y Comercio (SIC), Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), Ministerio de Industria y Comercio en las partes interesadas e incorporar a estas autoridades como partes interesadas formales en el sistema de gestión de la seguridad de la información, ciberseguridad y privacidad, para garantizar que las políticas y procedimientos estén alineados con las regulaciones y expectativas locales, fortaleciendo así el cumplimiento normativo y la relación con los entes reguladores.

4. Se evidencia la necesidad de establecer de manera clara y documentada los roles y responsabilidades de la UMNG como controlador y procesador de datos personales. Esto permitirá una mejor delimitación de funciones y responsabilidades, garantizando el cumplimiento de las normativas de privacidad y protección de datos aplicables, y proporcionando una mayor transparencia y confianza a las partes interesadas.

5. Se evidencia la necesidad de focalizar el tema de seguridad, ciberseguridad y protección hacia los objetivos estratégicos, alinear los esfuerzos y políticas de seguridad de la información, ciberseguridad y protección de la privacidad con los objetivos estratégicos de la UMNG, asegurando que estas áreas sean un componente fundamental en la consecución de las metas institucionales y que aporten valor tangible a la organización.

6. Se evidencia la necesidad de actualizar el documento vigente de la política de seguridad de la información incluyendo los temas de seguridad, ciberseguridad y protección de la privacidad. Se debe terminar de finalizar y oficializar el documento de la política de seguridad de la información que actualmente se encuentra en construcción. Esto garantizará que la política esté actualizada y en consonancia con las mejores prácticas y estándares internacionales, permitiendo una mejor implementación y cumplimiento en toda la Universidad.

7. Se evidencia la necesidad de formalizar el rol de CISO como cargo permanente, en lugar de usar la modalidad contractual de orden de prestación de servicios (OPS). Formalizar esta función crítica dentro de la estructura organizacional asegurará la continuidad y la gestión efectiva de los riesgos relacionados con la seguridad, minimizando la dependencia de recursos externos y manteniendo una baja rotación del personal que ocupe este cargo.

8. Se evidencia la necesidad de identificar requisitos de las partes interesadas de seguridad de la información, ciberseguridad y protección de la privacidad de manera detallada por cada tema, esto permitiría ver claramente la definición del contexto independientemente de los otros sistemas implementados actualmente.

9. Se evidencia la necesidad de formalizar el documento de la matriz de riesgos y alinearlo al proceso de gestión de riesgos de seguridad de la información en lo posible a la guía ISO IEC 27005:2022. Esto permitirá una gestión de riesgos más estructurada, basada en un enfoque metodológico y normativo reconocido, mejorando la capacidad de la UMNG para identificar, valorar y tratar los riesgos de manera efectiva.

10. Se evidencia la necesidad de incluir en el documento de trabajo de riesgos la referencia a controles de los modelos (Ej: ISO IEC 27001, ISO IEC 27701, ISO IEC 27032, etc.) en la columna de mitigación, esto facilitaría la aplicación y el seguimiento de controles efectivos y proporcionaría una guía clara para la gestión de riesgos alineada con estándares internacionales ante una eventual evaluación de la conformidad de primera parte, segunda parte o por un organismo de tercera parte.

11. Se evidencia la necesidad de incluir en la planificación del cambio la implementación de la seguridad, ciberseguridad y protección de la privacidad, considerando cambios planificados y no planificados, esto permitirá una mayor adaptación y flexibilidad ante situaciones imprevistas, garantizando que los aspectos de seguridad estén siempre integrados y se pueda reducir o aprovechar el impacto de los cambios al sistema de gestión integrado de la UMNG.

12. Se evidencia la necesidad de legalizar todos los documentos de seguridad, ciberseguridad y protección de la privacidad en la herramienta KAWAK, asegurando que estén debidamente aprobados y actualizados, esto fortalecerá el cumplimiento normativo y garantizará que todos los procedimientos estén respaldados por documentación formal mejorando la transparencia de los temas y el entendimiento y aplicación por parte de los usuarios.

13. Se evidencia la necesidad de desarrollar e implementar indicadores clave de desempeño (KPI) que permitan evaluar la rentabilidad y eficiencia del sistema de gestión de seguridad, ciberseguridad y protección de la privacidad. Estos indicadores ayudarán a medir el impacto y el valor añadido de las medidas implementadas, facilitando la toma de decisiones basada en datos.

14. Se evidencia la necesidad de incluir un cargo específico para la protección de la privacidad en la propuesta que actualmente se encuentra en elaboración. Esto permitirá una supervisión más detallada y efectiva de los temas relacionados con la privacidad y el cumplimiento de normativas.

15. Se evidencia la necesidad de continuar con el proyecto de utilizar Moodle como plataforma de formación en temas de seguridad, ciberseguridad y protección de la privacidad. Esto permitirá una capacitación continua y flexible, contribuyendo al fortalecimiento de la cultura de seguridad y protección de datos en la organización.

16. Se evidencia la necesidad de evaluar la posibilidad de reestructurar el proceso de TIC en áreas especializadas, resaltando el componente estratégico actual como parte del

Macroproceso y posiblemente de apoyo para otros temas. Actualmente, el área de TIC en la Universidad abarca múltiples funciones, como infraestructura, uso y apropiación, sistemas informáticos, y análisis de seguridad de la información. Esta separación permitirá una asignación más clara de responsabilidades y recursos, facilitando el desarrollo de estrategias y controles específicos en cada dominio, en particular en lo que respecta a la ciberseguridad y la privacidad.

17. Se evidencia la necesidad de ampliar la política integral GI-PR-F-8 para incluir SGSI, SGPI y ciberseguridad. Esto garantizará un enfoque integral que cubra todos los aspectos relacionados con la gestión de la seguridad y protección de la privacidad, fortaleciendo la protección de los datos y alineando las políticas institucionales con estándares internacionales reconocidos.

18. Se evidencia la necesidad de incorporar dentro de los objetivos actuales del sistema integrado, aspectos específicos relacionados con el Sistema de Gestión de Seguridad de la Información (SGSI), el Sistema de Gestión de Privacidad de la Información (SGPI) y la ciberseguridad, lo cual permitiría un despliegue específico con actividades, responsables, recursos, tiempos y mediciones específicas.

19. Se evidencia la necesidad de revisar el acceso, la clasificación y etiquetado de la documentación en Kawak con el fin de asegurar que aquellos que contengan información sensible o confidencial cuenten con controles adecuados de acceso y se gestionen conforme a las políticas de seguridad de la Universidad, protegiendo así la integridad y privacidad de la información almacenada.

20. Se evidencia que la UMNG actualmente tiene un inventario de activos donde se han identificado activos de tipo tecnológicos, sin embargo, se sugiere complementar el ejercicio con otro tipo de activos como: procesos o actividades claves, información, personas, etc. lo anterior es fundamental, considerando que los riesgos de seguridad de la información no solo provienen de activos tecnológicos sino también de los procesos misionales, de apoyo, administrativos y operativos. Estos procesos adicionales pueden contener amenazas y vulnerabilidades que, si no se abordan, pueden comprometer la seguridad de toda la organización.

21. Se evidencia la necesidad de clasificar los riesgos institucionales por procesos y áreas específicas (seguridad de la información, ciberseguridad y protección de la privacidad) dado que actualmente se han identificado 87 riesgos a nivel institucional pero no se tienen clasificados por tema de manera específica. Esta segmentación permitirá una gestión más eficiente y focalizada de los riesgos, facilitando la implementación de controles y medidas preventivas que se adapten mejor a las características y particularidades de cada proceso o área y riesgo.

22. Se evidencia la necesidad de revisar la asignación de normas en la matriz de riesgos ya que actualmente, en la matriz de riesgos, cada riesgo está asociado a casi todas las normas, lo que puede generar confusión y falta de enfoque en el tratamiento de los riesgos.

Se recomienda realizar una revisión detallada para asignar normas específicas a cada riesgo, asegurando que estas correspondan de manera precisa a las características y naturaleza del riesgo identificado. Esto permitirá una gestión más eficiente y un cumplimiento normativo más preciso.

23. Se evidencia la necesidad de desarrollar e implementar un formato específico para la aceptación de riesgos que registre tanto el valor actual como el valor residual de los riesgos. Este documento debe evidenciar la aceptación explícita del riesgo por parte de su propietario y detallar los planes de tratamiento y mitigación propuestos, proporcionando así un registro claro y estructurado de las decisiones tomadas.

24. Se evidencia la necesidad de realizar y alinear pruebas de continuidad de las TIC con los objetivos y requisitos de continuidad del negocio. Esto asegurará que las pruebas permitan validar que las estrategias definidas sean pertinentes y que la capacidad de respuesta sea adecuada en situaciones reales de interrupción.

25. Se evidencia la necesidad de identificar y clasificar eventos e incidentes de seguridad de la información, ciberseguridad y protección de la privacidad para el manejo de estas situaciones. Esta diferenciación permitirá a la UMNG priorizar y gestionar de manera efectiva las situaciones críticas.

26. Se evidencia la necesidad de alinear las definiciones de incidentes de seguridad de la información con las categorías de faltas mayores y leves establecidas en el reglamento interno de trabajo y el proceso disciplinario. Esto permitirá una aplicación coherente y formal del proceso disciplinario, asegurando que las medidas tomadas contra el personal u otras partes interesadas que violen las directrices del sistema de gestión sean coherentes y justificadas.

27. Se evidenció la necesidad de definir y formalizar una política que regule las descargas de archivos, tanto en OneDrive como en otros entornos y dispositivos de la organización, para asegurar que solo se realicen descargas autorizadas y que cumplan con las medidas de seguridad establecidas, minimizando así los riesgos de malware y otras amenazas.

28. Se evidenció la necesidad de implementar controles estrictos para proteger el acceso a los routers en las redes públicas de la UMNG. Es fundamental restringir el acceso no autorizado a la configuración del router para evitar vulnerabilidades que podrían ser explotadas por atacantes y comprometer la seguridad de la red.

29. Se evidenció la necesidad de prohibir o controlar de manera estricta la posibilidad de realizar escaneos en las redes públicas de la UMNG. La implementación de políticas y herramientas que monitoricen y limiten este tipo de actividades permitirá reducir riesgos asociados con el mapeo y explotación de vulnerabilidades en la red.

30. Se evidenció la necesidad de prohibir o regular el uso de ventiladores u otros dispositivos conectados a los puertos USB, ya que estos pueden dañar los equipos y representar un

riesgo para la infraestructura de hardware. Se deben establecer políticas claras para el uso de puertos USB, permitiendo solo dispositivos seguros y necesarios para las funciones laborales.

31. Se evidenció la necesidad de desarrollar un plan estructurado para la migración documental y la adopción de la nueva versión del marco NIST CSF 2.0. Esta planificación debe incluir la evaluación de los cambios introducidos en la nueva versión, la capacitación del personal y la actualización de los procedimientos y controles para asegurar una transición sin interrupciones.

4.3 HALLAZGOS

1. Se evidenció que la UMNG no cuenta con una Declaración de Aplicabilidad formalmente documentada, incumpliendo el requisito 6.1.3 Tratamiento de los riesgos de seguridad de la información literal d) de la norma NTC ISO/IEC 27001:2022.

   La ausencia de este documento impide identificar y justificar claramente los controles de seguridad seleccionados y su aplicabilidad al contexto organizacional en función de los riesgos actuales. Esta situación representa un riesgo potencial para la gestión de la seguridad de la información, ya que no se establece una base sólida para la implementación y monitoreo de los controles necesarios.

2. Se evidenció que la UMNG no dispone de la definición de actividades relacionadas de desarrollo de sistemas subcontratados, incumpliendo el control 8.30 Desarrollo externalizado del Anexo A de la norma NTC ISO/IEC 27001:2022.

   Esta no definición es crítica para asegurar que las actividades de desarrollo de software y sistemas realizadas por terceros cumplan con los estándares de seguridad de la información, ciberseguridad y protección de la privacidad. La falta de estas actividades puede dar lugar a riesgos asociados con la gestión de proveedores, incluyendo la potencial exposición de información sensible y la inadecuada implementación de controles de seguridad. Esto contraviene los principios de gestión de riesgos establecidos en las normas aplicables, lo que podría comprometer la integridad y confidencialidad de los datos.

3. Se evidenció que el análisis DOFA (Debilidades, Oportunidades, Fortalezas y Amenazas) realizado por la UMNG no incluye el tema de privacidad, incumpliendo el requisito 5.2.1 Comprensión de la organización y su contexto de la norma NTC ISO/IEC 27701:2020.

Esta omisión es significativa, ya que la privacidad de los datos es un aspecto fundamental en la gestión de la seguridad de la información y ciberseguridad. La falta de consideración de la privacidad en el análisis DOFA limita la capacidad de la UMNG para identificar y evaluar adecuadamente los riesgos asociados a la protección de datos personales, así como para implementar controles y estrategias efectivas que aseguren el cumplimiento normativo.

4. Se evidenció que la UMNG no cuenta con un listado formal de contacto con las autoridades competentes relacionadas con la seguridad de la información, ciberseguridad y protección de datos, incumpliendo el control 5.5 Contacto con las autoridades del Anexo A de la norma NTC ISO/IEC 27001:2022.

   La ausencia de este listado es una deficiencia importante, ya que limita la capacidad de la UMNG para comunicarse de manera efectiva y oportuna con las autoridades en caso de incidentes de seguridad o violaciones de datos. Esto puede generar retrasos en la notificación de incidentes, lo que puede resultar en sanciones legales y un impacto negativo en la reputación de la organización.

5. Se evidenció que el usuario Liliana Santiago tiene acceso a la herramienta Kawak con los permisos de usuario asignados al usuario Eduardo Martínez, incumpliendo el control 5.17 Información de autenticación del Anexo A de la norma NTC ISO/IEC 27001:2022.

   Esta situación representa un riesgo significativo, ya que la falta de controles adecuados en la gestión de identidades puede conducir a accesos no autorizados y a la manipulación indebida de información sensible. El uso incorrecto de permisos y la falta de responsabilidades del usuario pueden comprometer la confidencialidad, integridad y disponibilidad de los datos gestionados en la herramienta, lo que contraviene los principios de seguridad establecidos en las normativas aplicables.

6. Se evidenció que la UMNG no ha formalizado la identificación de roles, responsabilidades y autoridades de la organización en relación con la seguridad de la información, la ciberseguridad y la privacidad de los datos, incumpliendo el requisito 5.3 Roles, responsabilidades y autoridades de seguridad de la información de la norma NTC ISO/IEC 27001:2022.

   Esta ausencia de claridad puede llevar a la falta de rendición de cuentas y a la confusión sobre las funciones de cada miembro del personal y sus roles en la gestión de la seguridad. Sin una definición precisa de los roles, responsabilidades y autoridades, es probable que no se implementen adecuadamente las políticas y procedimientos necesarios para proteger la información y sus activos relacionados.

7. Se evidenció que la UMNG no ha identificado riesgos y oportunidades relacionados con la seguridad de la información, la ciberseguridad y la privacidad de los datos, incumpliendo el requisito 6.1 Acciones para abordar los riesgos y las oportunidades de la norma NTC ISO/IEC 27001:2022.

Aunque existe un documento de trabajo que aborda estos riesgos, este no cuenta con la formalidad necesaria para ser considerado un registro oficial. La ausencia de un proceso formalizado de identificación de riesgos limita la capacidad de la organización para evaluar y gestionar adecuadamente las amenazas potenciales que pueden comprometer la confidencialidad, integridad y disponibilidad de la información.

8. Se evidenció que la UMNG no cuenta con evidencia suficiente que demuestre la planificación adecuada para alcanzar los objetivos de seguridad de la información, ciberseguridad y privacidad de los datos establecidos incumpliendo los requisitos 6.2 Objetivos de seguridad de la información y planificación para alcanzarlos de la norma NTC ISO/IEC 27001:2022 y requisito 5.4.2 Objetivos de seguridad de la información y planificación para alcanzarlos de la norma NTC ISO/IEC 27701:2020.

   Se han definido objetivos, sin embargo, no se han documentado los planes específicos, recursos asignados, ni las responsabilidades necesarias para su *cumplimiento*. Esta falta de planificación puede comprometer la efectividad de la gestión de la seguridad de la información y limitar la capacidad de la UMNG para evaluar su progreso hacia estos objetivos.

9. Se evidenció durante la auditoría que la UMNG no dispone de un documento formal que respalde la planificación de cambios del sistema de gestión de seguridad, ciberseguridad y protección de la privacidad, incumpliendo el requisito 6.3 Planificación de cambios de la norma NTC ISO/IEC 27001:2022.

   Esta ausencia limita la capacidad de la organización para gestionar de manera efectiva los cambios que puedan impactar en la seguridad de la información, la ciberseguridad y la protección de la privacidad. La falta de una planificación adecuada puede resultar en implementaciones desorganizadas, confusiones *sobre roles y responsabilidades, y una evaluación inadecuada de los riesgos asociados con los cambios propuestos. Es crucial desarrollar un documento de planificación de cambios que contemple los procesos de evaluación de riesgos, aprobación, implementación y revisión post-cambio, garantizando así una gestión controlada y efectiva de las modificaciones en el sistema de gestión de seguridad de la información.*

10. Se evidenció que la UMNG no ha definido la competencia requerida para los cargos relacionados con la seguridad de la información, la ciberseguridad y la protección de la privacidad, incumpliendo el requisito 7.2 Competencia de la norma NT ISO/IEC 27001:2022 y 5.5.2 Competencia de la norma NTC ISO/IEC 27701:2020.

    En particular, no se han establecido criterios claros en cuanto a la educación, formación y experiencia necesarias para desempeñar los cargos que afectan el desempeño de la seguridad de la información, ciberseguridad y protección de la privacidad.

11. Se evidenció que la UMNG no cuenta con una matriz formal que defina y estructure las comunicaciones internas y externas relacionadas con la seguridad de la información, ciberseguridad y protección de la privacidad, incumpliendo el requisito 7.4 Comunicación de la norma NTC ISO/IEC 27001:2022.

    Esta ausencia impide establecer canales de comunicación claros y efectivos, así como garantizar que la información relevante sobre seguridad de la información, ciberseguridad y protección de la privacidad llegue a las partes interesadas adecuadas. Sin una matriz de comunicación interna y externa, se corre el riesgo de que se pierda información crítica, se generen malentendidos y no se logre un adecuado nivel de concienciación y formación en materia de seguridad.

12. Se identificó que la UMNG no implementa ningún tipo de restricción para la descarga de información, más allá de los controles existentes en OneDrive. No se cuenta con políticas o lineamientos que regulen la descarga, transferencia o almacenamiento de datos sensibles o críticos incumpliendo el control 8.12 Prevención de fuga de datos del Anexo A de la norma NTC ISO/IEC 27001:2022.

    Se recomienda establecer políticas claras y procedimientos para la gestión de la información, que incluyan restricciones específicas sobre la descarga de datos, así como una capacitación adecuada para el personal sobre estas políticas.

13. Se evidenció que no se encuentran definidos mecanismos de clasificación formal de la información incumpliendo el control 5.12 Clasificación de la información del Anexo A de la norma NTC ISO/IEC 27001:2022.

    Se recomienda definir los criterios de clasificación de información que permita implementar la identificación y etiquetado de la misma, asegurando que todos los empleados en la UMNG tengan un entendimiento común de qué información es General, Restringida y cuál es Confidencial, y las medidas de seguridad asociadas a cada nivel.

14. Se evidenció que la UMNG no cuenta con mecanismos formales definidos de etiquetado de la información, ni se han establecido procesos de clasificación de datos incumpliendo el control 5.13 Etiquetado de la información del Anexo A de la norma NTC ISO/IEC 27001:2022.

    La ausencia de un sistema de etiquetado y clasificación impide identificar adecuadamente el nivel de sensibilidad de la información y las medidas de protección necesarias para cada tipo de dato.

15. Se evidenció que en los contratos de los proveedores UNION TEMPORAL SEPECANDIS 2.0, ESRI COLOMBIA SAS, INFRAESTRUCTURA TECNOLOGICA S.A.S, IT DISCOVERY SOLUTIONS SAS, IT DISCOVERY SOLUTIONS SAS, SOPORTE INTEGRAL DE INGENIERIA Y AUTOMATIZACION SAS, DIGITAL NEW ERA SAS de la UMNG no se ha definido requisitos de seguridad de la información

contractualmente, incumpliendo el control 5.20 Abordar la seguridad de la información en los acuerdos con los proveedores del Anexo A de la norma NTC ISO/IEC 27001:2022.

La falta de requisitos específicos sobre la seguridad de la información puede exponer a la UMNG a riesgos significativos relacionados con el manejo y procesamiento de información y activos relacionados por parte de terceros. Sin una clara definición de las responsabilidades y expectativas en materia de seguridad, se dificulta la gestión del riesgo asociado con la cadena de suministro y se incrementa la probabilidad de incidentes de seguridad.

16. Se evidenció que la UMNG no cuenta con un procedimiento formal que regule el proceso de copias de respaldo. Aunque se realizan copias de respaldo de manera planificada, estas se ejecutan intuitivamente, basándose en la experiencia del personal del área, incumpliendo el control 8.13 Copia de seguridad de la información del Anexo A de la norma NTC ISO/IEC 27001:2022.

    La falta de un procedimiento documentado puede resultar en la pérdida de datos críticos y en la incapacidad de restaurar información en caso de incidentes, lo que representa un riesgo significativo para la continuidad del negocio. Se recomienda desarrollar e implementar un procedimiento formal para la gestión de copias de respaldo, que incluya aspectos como la frecuencia de las copias, la seguridad de los datos respaldados y la capacitación del personal involucrado.

17. Se evidenció que la UMNG no tiene publicada en su página de internet la política de uso de datos personales incumpliendo la ley 1581 de 2012 artículo 12, el decreto 1377 de 2013 artículo 13, 16 y 17 y el control 5.34 del Anexo A de la norma NTC ISO/IEC 27001:2022.

    Esta ley exige a los responsables del tratamiento de datos deben tener una política de tratamiento accesible que informe a los titulares sobre sus derechos y el manejo que se dará a sus datos. Es importante cumplir con esta normatividad para hacer un uso adecuado de la información personal.

18. Se evidenció que la UMNG no ha realizado los registros de las bases de datos ante el Registro Nacional de Bases de Datos (RNBD), incumpliendo la ley 1581 de 2012 artículo 25 y el control 5.34 del Anexo A de la norma NTC ISO/IEC 27001:2022.

    Para realizar el registro de bases de datos, la UMNG deberá aportar a la Superintendencia de Industria y Comercio las políticas de tratamiento de la información, las cuales obligarán a los responsables y encargados del mismo, y cuyo incumplimiento acarreará las sanciones correspondientes.

19. Se evidenció que en el contrato del Oficial de Seguridad de la Información de la UMNG no se encontraba firmado al momento de la auditoría, incumpliendo el control 6.6

Acuerdos de confidencialidad o no divulgación del Anexo A de la norma NTC ISO/IEC 27001:2022.

La falta de un acuerdo de confidencialidad o de su firma expresa, puede resultar en la divulgación no autorizada de información crítica.

20. Se evidenció que la UMNG no cuenta con un análisis de impacto sobre el negocio (por sus siglas en inglés BIA), ni tampoco la definición de estrategias de continuidad de las TIC y planes de continuidad de las TIC, incumpliendo el control 5.30 Preparación de las TIC para la continuidad de la actividad del Anexo A de la norma NTC ISO/IEC 27001:2022.

    El proceso BIA debería utilizar tipos y criterios de impacto para evaluar los impactos a lo largo del tiempo resultantes de la interrupción de las actividades comerciales que ofrecen productos y servicios. La magnitud y la duración del impacto resultante deberían utilizarse para identificar las actividades prioritarias a las que se debe asignar un objetivo de tiempo de recuperación (RTO). LA BIA debería entonces determinar qué recursos se necesitan para apoyar las actividades prioritarias. También debería especificarse un RTO para estos recursos. Un subconjunto de estos recursos debería incluir los servicios de TIC.

21. Se evidenció que en los computadores de la sala de reuniones del primer piso de la sede principal donde se llevó a cabo la auditoría el día 24 de septiembre de 2024, el computador del usuario Secretaría de cursos Luisa Fernanda, del edificio de posgrados y los computadores de los usuarios de la Oficina TIC de la sede del Campus Nueva Granada tenían archivos con información, almacenados directamente en el escritorio, incumpliendo el control 7.7 Escritorio limpio y pantalla limpia del Anexo A de la norma NTC ISO/IEC 27001:2022.

    Esta práctica no cumple con las mejores prácticas de seguridad de la información y la gestión de datos, ya que puede dar lugar a la pérdida de información sensible y a un acceso no autorizado a datos importantes además incumple con las directrices de escritorio limpio planteadas en la política de seguridad de información establecida en la organización.

22. Se evidenció que la UMNG no cuenta con un proceso formal de gestión de la capacidad para sus sistemas y recursos de TI, incumpliendo el control 8.6 Gestión de capacidad del Anexo A de la norma NTC ISO/IEC 27001:2022.

    Esta carencia impide evaluar y garantizar que la infraestructura tecnológica esté alineada con las demandas actuales y futuras de la UMNG. Se requiere establecer un proceso que permita la planificación y gestión de la capacidad de los sistemas para asegurar que se satisfacen los requisitos de rendimiento y disponibilidad. La falta de gestión de la capacidad puede llevar a un rendimiento deficiente de los sistemas, tiempos de inactividad no planificados y una mala experiencia para los

usuarios. Se recomienda que la organización desarrolle un marco de gestión de la capacidad que incluya la monitorización, análisis y planificación adecuada de los recursos tecnológicos.

23. Se evidenció que desde la red pública de la sede de posgrados, la red pública de la sede del Campus Nueva Granada y los computadores de la biblioteca y el computador externo del corredor de la Facultad de Medicina y Ciencias de la Salud se pudo acceder a páginas de contenido web no autorizado, incumpliendo el control 8.23 Filtrado web Gestión de capacidad del Anexo A de la norma NTC ISO/IEC 27001:2022.

    Este hecho incumple requisitos de seguridad de la información y de ciberseguridad asociados con la necesidad de implementar controles de filtrado web para prevenir el acceso a contenido inapropiado o no autorizado, lo cual es fundamental para mantener la seguridad de la información. El acceso a páginas no permitidas puede comprometer la integridad de los sistemas de información y exponer a la UMNG a riesgos de seguridad, como malware o phishing. Se recomienda que la UMNG revise y refuerce sus controles de filtrado web, asegurando que se apliquen políticas adecuadas y se realicen auditorías regulares para garantizar el cumplimiento de las restricciones de acceso.

24. Se evidenció que la UMNG no cuenta con medidas implementadas para proteger los sistemas de información durante las pruebas de auditoría, incumpliendo el control 8.34 Protección de los sistemas de información durante las pruebas de auditoría del Anexo A de la norma NTC ISO/IEC 27001:2022.

    La ausencia de medidas de protección adecuadas durante las auditorías pone en riesgo la confidencialidad, integridad y disponibilidad de la información. Esto podría resultar en filtraciones de datos, modificaciones no autorizadas en los sistemas, interrupciones operativas, y comprometer la seguridad de la información de la UMNG.

25. Se identificó que para los sistemas de control de aire acondicionado del data center y el sistema de CCTV de la sede de posgrados, en el software de control de acceso al data center principal del Campus Nueva Granada, en el software de control de acceso al data center principal y en el software de seguridad electrónica Lenel Onguard del sistema de CCTV de la sede principal, se tienen configuraciones de horas diferentes, incumpliendo el control 8.17 Sincronización de reloj del Anexo A de la norma NTC ISO/IEC 27001:2022.

    Este control es fundamental para garantizar la precisión y la coherencia en los registros de eventos y las transacciones dentro de los sistemas de información. Adicionalmente brinda confianza como muestra probatoria ante una investigación ante un incidente de seguridad.

26. Se evidenció que en el área de carnetización de la sede principal se encuentra un equipo de cómputo ubicado de manera insegura, el computador está amarrado a una mesa de forma colgante, incumpliendo el control 7.8 Ubicación y protección de los equipos del Anexo A de la norma NTC ISO/IEC 27001:2022.

    Esta situación representa un riesgo para la seguridad de la información y la protección física de los activos tecnológicos.

27. No se evidencia seguimiento a los objetivos de seguridad de la información, ciberseguridad y privacidad, incumpliendo el requisito 6.2 Objetivos de seguridad de la información y planificación para alcanzarlos literal d) de la norma NTC ISO/IEC 27001:2022.

    La ausencia de seguimiento a los objetivos puede llevar a una falta de control y ajuste oportuno de las políticas y medidas de seguridad, generando brechas de seguridad y riesgos no identificados en el sistema de gestión. Esto compromete la eficacia de las estrategias de seguridad de la información, ciberseguridad y protección de la privacidad.

28. No se evidencia en la verificación de la revisión por la dirección la entrada de los cambios de las necesidades y expectativas de las partes interesadas que sean pertinentes con la seguridad de la información, ciberseguridad y privacidad incumpliendo el requisito 9.3.2 Entradas de la revisión por la dirección literal c) de la norma NTC ISO/IEC 27001:2022.

    La revisión por la dirección es fundamental para asegurar que la organización responda de manera adecuada a los cambios en las necesidades y expectativas de las partes interesadas. Al no analizar estos cambios durante las revisiones, se pierde la oportunidad de ajustar estrategias y controles de forma proactiva, lo cual es esencial para mantener un sistema de gestión relevante y eficaz. El impacto negativo de no hacerlo incluye el riesgo de que las medidas de seguridad y políticas de ciberseguridad queden obsoletas o mal alineadas con los requerimientos actuales, lo que puede resultar en brechas de seguridad y pérdida de confianza de las partes interesadas.

29. Se evidenció que no se han identificado los requisitos para asegurar la seguridad de la información en la gestión de proyectos, incumpliendo el control A.5.8 Seguridad de la información en la gestión de proyectos del anexo A de la norma la ISO IEC 27001:2022.

    La falta de identificación de requisitos de seguridad en la gestión de proyectos expone a la organización a riesgos significativos de pérdida, fuga o manipulación no autorizada de información durante el desarrollo y ejecución de los proyectos. Esto puede resultar en incumplimientos de seguridad, fallos en la gestión de riesgos y posibles impactos negativos en los resultados de los proyectos, afectando la

confianza de los clientes y partes interesadas y comprometiendo la conformidad normativa y la reputación de la organización.

30. Se evidenció durante las visitas realizadas a las sedes Facultad de Medicina y Ciencias de la Salud ubicada en la Transversal 3 n.° 49-00 (50 cámaras dañadas), Sede Posgrados calle 94 A # 13 – 54 (1 cámara dañada) y el Campus Nueva Granada (100 cámaras dañadas aproximadamente). Adicionalmente en el Campus Nueva Granada el sistema CCTV no se encontraban funcionando en el momento de la auditoría, incumpliendo el control Monitoreo de la seguridad física del anexo A de la norma la ISO IEC 27001:2022.

    Esta situación indica que la organización no está garantizando un monitoreo efectivo de la seguridad física. Esto puede tener un impacto negativo al aumentar la vulnerabilidad de las instalaciones frente a accesos no autorizados y otras amenazas físicas, poniendo en riesgo la seguridad de los activos y la información que se encuentran en esas ubicaciones.

31. Se evidenció que no se han identificado los requisitos para asegurar la seguridad de la información en la gestión de proyectos, incumpliendo el control A.5.8 Seguridad de la información en la gestión de proyectos del anexo A de la norma la ISO IEC 27001:2022.

    La falta de identificación de requisitos de seguridad en la gestión de proyectos expone a la organización a riesgos significativos de pérdida, fuga o manipulación no autorizada de información durante el desarrollo y ejecución de los proyectos. Esto puede resultar en incumplimientos de seguridad, fallos en la gestión de riesgos y posibles impactos negativos en los resultados de los proyectos, afectando la confianza de los clientes y partes interesadas y comprometiendo la conformidad normativa y la reputación de la organización.

32. Se evidenció que el sistema de Seguridad Electrónica Lenel Onguard, finalizó el último contrato de mantenimiento en octubre de 2021 y hasta la fecha no cuenta con mantenimiento preventivo ni correctivo, incumpliendo el control A.7.13 Mantenimiento de equipos, del anexo A de la norma la ISO IEC 27001:2022.

    La ausencia de estas acciones de mantenimiento puede resultar en fallos operativos que afecten la continuidad de los servicios y comprometan la seguridad física y lógica de los sistemas. Además, aumenta el riesgo de interrupciones no planificadas y brechas de seguridad.

33. Se evidenció durante la visita realizada a la Sede Posgrados calle 94 A # 13 – 54 que no se cuenta con el aviso de privacidad del sistema CCTV, incumpliendo la ley 1581 de 2012 artículo 12, el decreto 1377 de 2013 artículo 13, 16 y 17 y el control 5.34 del Anexo A de la norma NTC ISO/IEC 27001:2022.

Las señales o avisos implementados deben ser visibles y legibles teniendo en cuenta el lugar en el que opere el sistema de vigilancia y contar como mínimo con el contenido de un aviso de privacidad, a saber:
- Incluir información sobre quién es el responsable del tratamiento y sus datos de contacto.
- Indicar el tratamiento que se dará a los datos y la finalidad del mismo.
-Incluir los derechos de los titulares.
-Indicar dónde está publicada la política de tratamiento de la información.

34. Se evidenció durante la auditoría de los controles físicos en la sede de la Facultad de Medicina de la UMNG, específicamente en el cuarto técnico principal ubicado en el último piso, la presencia de desorden, elementos de construcción de proveedores de mantenimiento, equipos de tecnología con polvo, acceso físico sin control, incumpliendo el control A.7.8 Ubicación y protección de los equipos, del anexo A de la norma NTC ISO IEC 27001 2022.

    Esta situación aumenta significativamente los riesgos derivados de amenazas físicas y ambientales, así como del acceso y los daños no autorizados afectando la disponibilidad y continuidad de los equipos.

8. CONCLUSIONES DE AUDITORÍA

1. Una vez realizado el ejercicio de auditoría interna para determinar el nivel de madurez de seguridad de la información, ciberseguridad y privacidad de datos en la UNIVERSIDAD MILITAR NUEVA GRANADA, de acuerdo con los principales marcos establecidos, normatividad y legislación relacionada, se observa un **grado medio de madurez** (**L2)** donde se evidencian **elementos reproducibles, pero intuitivos y se realizan prácticas de acuerdo a la experiencia del personal aunque sin comunicación formal y se depende del conocimiento individual** para el cumplimiento de gran parte de los requisitos establecidos en las normas técnicas internacionales NTC ISO IEC 27001:2022, ISO IEC 27701:2020 y NIST CSF.
2. Se sugiere, culminar y **dar prioridad al ejercicio de identificación de activos de información**, **incluyendo otros tipos de activos** a los actualmente identificados (ej: procesos y actividades claves, información, personas, etc.) en todos los procesos, **e identificar los riesgos de seguridad, ciberseguridad y privacidad de datos**, asociados con la pérdida de confidencialidad, de integridad y disponibilidad de información dentro del alcance del sistema de gestión de la organización.
3. Se han identificado **no conformidades y áreas en las que se puede mejorar el cumplimiento** de los requisitos de seguridad, ciberseguridad y privacidad de datos, las cuales se deben trabajar en su totalidad para asegurar un desempeño óptimo del sistema.

4. Se han identificado **oportunidades de mejora** que facilitarán que la UMNG aumente la capacidad para cumplir con los requisitos establecidos.
5. Las fortalezas identificadas confirman el **compromiso de los funcionarios de la UMNG** frente a la mejora continua y el logro de los propósitos organizaciones en el contexto de la seguridad de la información, la ciberseguridad y privacidad de los datos.
6. Se evidencia la necesidad de continuar trabajando hacia la **documentación y formalización del SGS,** situación que permitiría una gestión más eficaz y coherente, evitando duplicidades y utilizando los recursos de manera mas eficiente.
7. Se evidencia la necesidad de establecer de manera clara y detallada el **despliegue de los objetivos relacionados con la seguridad de la información, la ciberseguridad y la privacidad de datos,** situación que permite definir de manera clara y estructurada las acciones necesarias, responsables, recursos y plazos para alcanzar esos objetivos, además facilita el seguimiento y control del progreso, y facilita que las metas definidas se cumplan de manera eficaz, promoviendo la mejora continua.
8. Se evidencia la necesidad de fortalecer la **gestión integral de riesgos y oportunidades,** situación que permitiría establecer las acciones necesarias que facilite anticiparse a la ocurrencia de eventos potenciales no deseados y sus impactos, así como aprovechar las capacidades de la entidad para mejorar la reputación y la confianza de las diferentes partes interesadas y tomar decisiones estratégicas y operativas más informadas, alineadas con los objetivos de la entidad.

CONCLUSIONES ESPECÍFICAS DE LA AUDITORÍA INTERNA - SEGURIDAD DE LA INFORMACIÓN –

1. Se identifica la necesidad de **complementar el ejercicio de análisis del contexto de la organización y la identificación de las partes interesadas**, asegurando que se aborden de manera integral y actualizada las necesidades y expectativas de todos los actores relevantes. Es recomendable revisar y ajustar regularmente el análisis para considerar cualquier cambio en el entorno interno o externo, así como integrar de manera efectiva a las partes interesadas en los procesos de seguridad.
2. Se ha evidenciado la necesidad de **ampliar y actualizar continuamente la identificación de riesgos**, asegurando que el análisis cubra todas las áreas y procesos críticos de la organización mediante la participación activa de distintos procesos y el uso de herramientas tecnológicas. Además, se recomienda **optimizar los planes de tratamiento de riesgos**, haciéndolos más específicos y con un monitoreo continuo para evaluar la eficacia de las medidas, complementando con programas de capacitación para mejorar las habilidades del personal en la gestión y

mitigación de riesgos, y así adaptarse de manera efectiva a las amenazas emergentes.

3. Se ha evidenciado que el **filtrado web** no está funcionando correctamente en algunas redes, ya que se permitió el acceso a sitios no autorizados, lo cual representa un incumplimiento de la política actual de la UMNG sobre el acceso y filtrado de contenido.
4. Se ha evidenciado que las **directivas sobre escritorio limpio y pantalla despejada** de la política de la UMNG, se incumple en varios casos donde en el escritorio de computadores constatados se almacenan archivos que contienen información sensible.
5. Se recomienda **establecer un proceso formal para confirmar que los ensayos de auditoría** y otras actividades de garantía relacionadas con la evaluación de los sistemas operativos estén debidamente planificados y acordados entre el equipo de auditoría y la dirección correspondiente. Implementar esta práctica garantizará una mayor transparencia y alineación en los objetivos de la auditoría, además de fomentar una colaboración efectiva entre las partes involucradas.
6. Se identifica la necesidad de **implementar un proceso riguroso para verificar que todos los cambios en las instalaciones de tratamiento de la información y en los sistemas de información** se realicen conforme a procedimientos de gestión de cambios definidos en la organización. Esta práctica garantizará que cada modificación sea evaluada adecuadamente en términos de impacto, riesgos y beneficios, minimizando la posibilidad de errores y vulnerabilidades.
7. Se ha observado que el **etiquetado de la información** no se realiza. Fortalecer este proceso mediante la implementación de un etiquetado claro y consistente a nivel de archivo permitiría una identificación más precisa y un mejor manejo de la información y otros activos.
8. Se identifica la necesidad de **fortalecer la gestión de la seguridad en la relación con proveedores**, asegurando que los acuerdos incluyan cláusulas específicas sobre la protección de la información y los requisitos de ciberseguridad. Es recomendable establecer procedimientos claros para evaluar y monitorear regularmente el cumplimiento de estos requisitos por parte de los proveedores, así como integrar controles adicionales que aseguren que cualquier riesgo relacionado con terceros sea gestionado de manera proactiva y alineado con las políticas de seguridad de la organización.

CONCLUSIONES ESPECÍFICAS DE LA AUDITORÍA INTERNA - CIBERSEGURIDAD–

1. El **análisis de riesgos cibernéticos** debe considerar cómo los riesgos identificados podrían impactar la capacidad de la organización para cumplir con su misión. Los

activos clave, servicios críticos y datos deben priorizarse en función de su importancia para la misión organizacional.

2. Se identifica la necesidad de comprender a los interesados internos y externos, y asegurar que sus necesidades y expectativas en cuanto a la gestión de riesgos de ciberseguridad sean comprendidas y consideradas. Este control involucra tanto a los actores internos (empleados, directivos, socios) como a los externos (clientes, proveedores, reguladores) en la gestión de riesgos, asegurando que sus intereses estén reflejados en las estrategias de ciberseguridad.
3. Se identifica la necesidad de complementar políticas internas que reflejen los requisitos legales y contractuales relacionados con ciberseguridad y privacidad. Esto puede incluir políticas sobre el tratamiento de datos personales, gestión de incidentes de seguridad, y la transferencia transfronteriza de datos.
4. Se requiere establecer objetivos claros que alineen los servicios críticos y las capacidades internas con las expectativas de los interesados. Estos objetivos deben reflejar la resiliencia ante incidentes de ciberseguridad, la continuidad operativa y el cumplimiento de estándares de calidad.
5. Se requiere identificar cómo la interrupción de los servicios críticos impactaría en la organización, y utilizar esta información para priorizar las medidas de mitigación de riesgos. Los servicios y capacidades más críticos requieren mayores niveles de protección y continuidad.
6. La UMNG debe definir claramente su apetito por el riesgo en el contexto de la ciberseguridad, es decir, el nivel de riesgo que está dispuesta a aceptar en sus operaciones. Esto puede variar según los procesos o activos involucrados.

CONCLUSIONES ESPECÍFICAS DE LA AUDITORÍA INTERNA - PRIVACIDAD DE DATOS –

1. Este es el sistema de gestión que tiene el nivel de madurez más bajo de los 3 evaluados. No se evidencia una definición clara de estrategias de implementación, así como la asignación de responsables y recursos específicos. Es importante no perder el horizonte de ir más allá de los requisitos mínimos que establece la legislación colombiana frente a este tema (política de tratamiento de datos personales, acuerdos de confidencialidad, entre otros).
2. Se requiere definir claramente los roles de controladores y procesadores de información en el sistema de gestión de privacidad, especificando las actividades en las que cada uno de ellos interviene. Esto permitirá asegurar que las responsabilidades y obligaciones de cada parte estén bien delimitadas, facilitando el cumplimiento normativo y fortaleciendo la protección de los datos personales.

Además, se recomienda documentar estas definiciones y actividades asociadas para garantizar una mayor transparencia y trazabilidad en el tratamiento de la información.

3. Se observa la necesidad de considerar la alineación de los principios de privacidad (licitud, equidad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; integridad y confidencialidad; y responsabilidad proactiva) con los controles y actividades definidos para los roles de controladores y procesadores de información. Esto permitirá asegurar que los controles implementados no solo cumplan con las normativas, sino que también se adhieran a los principios fundamentales de privacidad, garantizando así una gestión integral y coherente de los datos personales a lo largo de todo su ciclo de vida.

Elaborado por:	Aprobado por:
Germán Andrés Sánchez Ortegón **Auditor Líder**	**Claudia Johanna Crane Santander** **Jefe Oficina Control Interno de Gestión**