

UNIVERSIDAD MILITAR NUEVA GRANADA



INFORME DE AUDITORIA CONTROL INTERNO	Fecha Emisión: 2024/04/10	GI-MA-F-17
	Revisión No.: 2	Página 1 de 26

FECHA DE EMISIÓN DEL INFORME PRELIMINAR	Día:	01	Mes:	10	Año:	2026
--	------	----	------	----	------	------

FECHA DE EMISIÓN DEL INFORME FINAL	Día:	15	Mes:	10	Año:	2026
---------------------------------------	------	----	------	----	------	------

1. INFORMACIÓN GENERAL

Macroproceso:	Planeación Estratégica
Proceso:	Gestión Estratégica TIC
Líder de Proceso / Jefe(s) Dependencia(s):	CN (R) Ricardo Ariza Urango Ph.D. Jefe de la Oficina Asesora de las Tecnologías de la Información y las Comunicaciones.
Representante Alta Dirección	BG (R) Arnulfo Traslaviña Sáchica Rector (E)
Objetivo General de la Auditoría:	Evaluar el grado de cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), actualizado mediante la Resolución MinTIC 02277 del 3 de junio de 2025, que modifica el Anexo 1 de la Resolución 500 de 2021 y adopta lineamientos alineados con la Norma ISO/IEC 27001:2022, verificando la existencia, pertinencia y efectividad de los componentes, políticas, procedimientos y controles definidos por la UMNG.
Objetivos Específicos de la Auditoría:	<ol style="list-style-type: none">1. Determinar la capacidad del Modelo de Seguridad y Privacidad de la Información (MSPI) en UMNG, para cumplir los requisitos legales, reglamentarios, normativos, contractuales y establecidos por la entidad.2. Determinar la eficacia del Modelo de Seguridad y Privacidad de la Información (MSPI) en UMNG frente al cumplimiento de los objetivos establecidos.3. Identificar áreas de mejora potencial del Modelo de Seguridad y Privacidad de la Información (MSPI) en UMNG.

UNIVERSIDAD MILITAR NUEVA GRANADA



Alcance de la Auditoría:	<p>Gestión Estratégica de TIC y procesos relacionados al Modelo de Seguridad y Privacidad de la Información (MSPI) en UMNG de acuerdo con el GI-PR-F-14 Mapa de Macroprocesos revisión No.17.I.</p> <p>El periodo objeto de evaluación comprenderá la información, actividades, operaciones, registros y demás evidencias generadas entre el 1 de septiembre de 2025 y el 31 de agosto de 2026, sin perjuicio de la revisión de antecedentes o evidencias de periodos anteriores cuando resulte necesario para verificar la implementación, continuidad, trazabilidad y eficacia de los controles evaluados.</p> <p><u>Sedes:</u></p> <p>Sedes Bogotá</p> <ul style="list-style-type: none"> - Carrera 11 No 101-80 (Bogotá, Colombia) - Facultad de Medicina y Ciencias de la Salud Transversal 3 No 49-00 - Edificio La Equidad: Calle 100 9ª-45 <p>Sede Campus Nueva Granada</p> <ul style="list-style-type: none"> - Kilómetro 2, vía Cajicá-Zipacquirá
Criterios de la Auditoría:	<p>Resolución MinTIC 500 de 2021 y su Anexo 1, actualizado mediante la Resolución 02277 de 2025; Modelo de Seguridad y Privacidad de la Información (MSPI) vigente; Decreto 1078 de 2015, modificado por el Decreto 767 de 2022, en lo relacionado con la Política de Gobierno Digital y el habilitador de Seguridad y Privacidad de la Información; requisitos de ISO/IEC 27001:2022 incorporados por el MSPI; legislación colombiana aplicable en materia de seguridad de la información, privacidad, protección de datos personales, transparencia, gestión documental y seguridad digital; políticas, manuales, procedimientos, metodologías, planes, contratos y demás disposiciones internas adoptadas por la Universidad Militar Nueva Granada dentro del alcance de la auditoría.</p>
Auditor Líder	Germán Andrés Sánchez Ortégón
Auditor acompañante	Miguel Ángel Suárez Benítez – Experto Técnico

Reunión de Apertura						Ejecución de la Auditoría				Cierre Proceso de Auditoría					
Día	08	Mes	09	Año	2026	Desde	08/09/2026	Hasta	24/09/2026	Día	01	Mes	10	Año	2026
							D / M / A		D / M / A						

UNIVERSIDAD MILITAR NUEVA GRANADA



4. RESULTADOS DE LA AUDITORÍA

ASPECTOS RELEVANTES (Fortalezas identificadas que aportan valor al proceso y al MSPI)

Aspecto conforme No. 1

7.1 — Recursos. Se evidencia la asignación de recursos presupuestales específicos para actividades relacionadas con protección de datos, infraestructura de seguridad, mantenimiento de sistemas, respaldo y recuperación, así como la consideración del MSPI dentro de la planificación presupuestal institucional. Esta situación constituye una fortaleza al demostrar disponibilidad de recursos para soportar la implementación, operación y sostenibilidad de los controles de seguridad y privacidad, favoreciendo el cumplimiento de los objetivos del Modelo.

Aspecto conforme No. 2

7.5.1 — Información documentada – Generalidades. Se evidencia la existencia de una estructura institucional para la gestión documental que incluye Tablas de Retención Documental, intervención y organización progresiva del archivo físico, gestión de archivos de gestión, central e histórico y utilización del sistema de gestión documental CADET para comunicaciones y documentos institucionales. Esta situación constituye una fortaleza al proporcionar mecanismos institucionales para organizar, conservar, recuperar y gestionar la información documentada requerida para la operación y trazabilidad de los procesos.

Aspecto conforme No. 3

10.1 — Seguimiento de hallazgos. Se evidencia la existencia de un mecanismo de seguimiento por parte de Control Interno que consolida el estado de los hallazgos y las actividades de mejoramiento, permitiendo identificar avances y cierres con corte periódico. Esta situación constituye una fortaleza al proporcionar información centralizada para el seguimiento institucional y facilitar la identificación de retrasos que requieren intervención de los responsables y la Alta Dirección.

Aspecto conforme No. 4

A.5.19 — Seguridad de la información en la relación con proveedores. Se evidencia la utilización de mecanismos institucionales para identificar y visualizar información asociada a proveedores y sus riesgos, incluyendo registros en SECOP y herramientas de seguimiento como Power BI. Esta situación constituye una fortaleza al facilitar la consolidación, consulta y supervisión de información relacionada con terceros, proporcionando una base para fortalecer posteriormente la evaluación específica de sus riesgos de seguridad y privacidad.

Aspecto conforme No. 5

A.7.2 — Entrada física. Se evidencia que en la biblioteca de la sede Facultad de Medicina y Ciencias de la Salud se encuentra implementado un mecanismo robusto para el control de salida de material bibliográfico, mediante dispositivos magnéticos asociados a los libros y sensores ubicados en el punto de salida. Esta situación constituye una fortaleza al reducir el riesgo de retiro no autorizado, pérdida o sustracción de activos bibliográficos, fortalecer la trazabilidad sobre su salida y aportar positivamente a

UNIVERSIDAD MILITAR NUEVA GRANADA



la protección de los recursos de información administrados por la Universidad.

Aspecto conforme No. 6

A.8.22 — Segregación de redes. Se evidencia la implementación de mecanismos de seguridad perimetral que restringen desde redes externas el acceso directo a servicios administrativos y de backend del portal institucional, incluyendo servicios como SSH, RDP y servicios de aplicación, mientras se mantiene una arquitectura diferenciada para el acceso interno y externo. Esta situación constituye una fortaleza al reducir la superficie de exposición y el riesgo de accesos no autorizados a servicios sensibles, aportando positivamente a la protección y segregación de las redes institucionales.

RECOMENDACIONES

(Situaciones que conviene fortalecer y beneficio esperado)

Recomendación No. 1

4.1 — Comprensión de la organización y de su contexto. Se evidencia la necesidad de fortalecer el análisis del contexto institucional incorporando de manera diferenciada los asuntos internos y externos relacionados con seguridad de la información, privacidad y ciberseguridad, considerando que actualmente estos aspectos se encuentran integrados principalmente dentro de categorías administrativas y tecnológicas generales. Esta situación podría limitar la identificación y seguimiento de cambios del entorno que afecten específicamente el logro de los resultados previstos del MSPI. **R1**

Recomendación No. 2

4.2 — Necesidades y expectativas de las partes interesadas. Se evidencia la necesidad de fortalecer la identificación y documentación de las necesidades y expectativas de las partes interesadas pertinentes al MSPI, considerando que la matriz GI-GI-F-6 V4 identifica los grupos de interés, pero no incorpora de manera completa sus necesidades y expectativas relacionadas con seguridad y privacidad, encontrándose esta información aún en elaboración. Esta situación podría dificultar la determinación de los requisitos que deben ser abordados por el sistema y su posterior trazabilidad hacia riesgos, controles y obligaciones aplicables. **R2**

Recomendación No. 3

5.3 — Formalización de la tercerización de funciones CISO. Se evidencia la necesidad de formalizar institucionalmente la decisión de tercerizar funciones asociadas al rol de CISO y de definir de manera expresa su autoridad, alcance, responsabilidades, mecanismos de reporte y articulación con los demás roles del MSPI. La ausencia de esta formalización podría generar ambigüedad respecto de la autoridad efectiva para dirigir, coordinar y escalar asuntos de seguridad de la información. **R3**

Recomendación No. 4

6.1.1 — Acciones para abordar riesgos y oportunidades. Se evidencia la necesidad de fortalecer la aplicación transversal de la gestión de riesgos de privacidad dentro del MSPI. Si bien el “Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025”, versión 1.0, incorpora expresamente la privacidad dentro de su alcance y metodología, en las matrices y procesos revisados

UNIVERSIDAD MILITAR NUEVA GRANADA



durante la auditoría no se evidenció de manera homogénea la identificación, valoración y tratamiento de riesgos derivados del tratamiento de datos personales. Esta situación podría ocasionar que eventos con impacto sobre los titulares o la IIP sean gestionados de forma desigual o queden fuera del ciclo institucional de riesgos y oportunidades. **R4**

Recomendación No. 5

7.1 — Trazabilidad presupuestal. Se evidencia la necesidad de fortalecer la trazabilidad presupuestal de los recursos destinados al MSPI, diferenciando claramente los componentes de gasto e inversión y relacionando cada asignación con los planes, proyectos, riesgos y controles que soporta. La necesidad de mejora se sustenta en el PETI 2024-2028 y el PESI 2025-2026, que contienen proyectos y estimaciones o análisis presupuestales, así como en la evidencia de planeación presupuestal revisada durante la auditoría; sin embargo, no se observó una relación completa entre las partidas ejecutadas, los riesgos, los controles y los resultados del MSPI. Esta situación podría dificultar la evaluación de la suficiencia de los recursos y la medición del costo real de implementación y mantenimiento del Modelo.

R5

Recomendación No. 6

7.5.3 — Control de la información documentada. Se evidencia la necesidad de fortalecer la trazabilidad sobre la aplicación de las Tablas de Retención Documental, particularmente mediante la conservación y disponibilidad de evidencias de las transferencias realizadas conforme a los tiempos y disposiciones establecidos en las TRD. La ausencia o dificultad para demostrar estas transferencias podría afectar la adecuada conservación, recuperación y disposición de la información documentada institucional. **R6**

Recomendación No. 7

9.1 — Relación objetivo–indicadores. Se evidencia la necesidad de fortalecer la relación entre los indicadores definidos y el objetivo institucional de mitigación de riesgos, considerando que el indicador No. 36 “Valoración de activos de información”, asociado al objetivo institucional No. 15, refleja el avance en la valoración de activos, pero no permite determinar directamente el nivel de mitigación alcanzado ni la eficacia de los controles aplicados. La permanencia de una métrica que no mida directamente el resultado esperado podría generar resultados favorables del indicador sin demostrar efectivamente que los riesgos de seguridad y privacidad han disminuido. **R7**

Recomendación No. 8

9.1 — Cobertura del sistema de seguimiento y medición. Se evidencia la necesidad de fortalecer y actualizar el seguimiento, medición, análisis y evaluación del MSPI, articulándolo con los mecanismos institucionales existentes del Sistema Integrado de Gestión (SIG). El proceso de Gestión Estratégica TIC deberá determinar y documentar los mecanismos pertinentes para evaluar el desempeño y la eficacia del Modelo, incluyendo qué debe ser objeto de seguimiento y medición, los métodos aplicables, la periodicidad, los responsables y el análisis de los resultados. Esta articulación deberá aprovechar los instrumentos institucionales ya definidos, evitando la generación de mecanismos paralelos o duplicados, y asegurando que la Alta Dirección disponga de información suficiente para

UNIVERSIDAD MILITAR NUEVA GRANADA



evaluar integralmente el desempeño del MSPI. **R8**

Recomendación No. 9

9.2 — Auditoría interna. Se evidencia la necesidad de fortalecer la consideración explícita de los requisitos aplicables al MSPI dentro de la planificación, ejecución y seguimiento del Programa Anual de Auditoría de la Universidad, manteniendo el enfoque integral del Sistema Integrado de Gestión (SIG). La recomendación no implica establecer un programa de auditoría independiente para el MSPI, sino asegurar que sus criterios, riesgos y requisitos sean incorporados, cuando corresponda, en los ejercicios de auditoría institucionales, de manera que se garantice una cobertura suficiente del Modelo, se optimicen los recursos y se evite la duplicidad de evaluaciones. **R9**

Recomendación No. 10

9.3 — Integración de la Revisión por la Dirección. Se evidencia la necesidad de fortalecer la integración del MSPI dentro de la Revisión por la Dirección del Sistema Integrado de Gestión (SIG), sin que ello implique realizar un ejercicio independiente o paralelo. Para este propósito, el proceso de Gestión Estratégica TIC deberá suministrar oportunamente la información correspondiente al desempeño del Modelo y asegurar que las entradas y salidas aplicables al MSPI sean incluidas, analizadas y trazables dentro del ejercicio institucional de revisión, de manera que la Alta Dirección pueda adoptar decisiones sobre su conveniencia, adecuación, eficacia, recursos y oportunidades de mejora. **R10**

Recomendación No. 11

A.5.1 — Políticas de seguridad de la información. Se evidencia la necesidad de actualizar, armonizar y mejorar la trazabilidad del Manual Integral de Políticas de Seguridad de la Información con el MSPI V5, incluyendo su referencia explícita dentro de la Declaración de Aplicabilidad y revisando la denominación y estructura del documento para diferenciar adecuadamente políticas y directrices temáticas. Mantener referencias desactualizadas o desconectadas de la Declaración de Aplicabilidad podría generar inconsistencias entre los controles declarados y las directrices institucionales que los soportan. **R11**

Recomendación No. 12

A.5.7 — Inteligencia sobre amenazas. Se evidencia la necesidad de fortalecer el proceso de inteligencia de amenazas, asegurando que la información recopilada desde diferentes fuentes y servicios de seguridad se analice de manera estructurada y se traduzca de forma trazable en acciones sobre riesgos, controles y mecanismos de protección de la Universidad. La evidencia revisada incluye la alerta de CrowdStrike del 14 de agosto de 2026 sobre actividad maliciosa de severidad alta, el informe de supervisión del servicio EDR/MDR y registros de fuentes de monitoreo; no obstante, no se aportó un procedimiento o registro consolidado que demuestre el ciclo completo de obtención, análisis, contextualización, decisión y retroalimentación de la inteligencia de amenazas hacia los riesgos y controles del MSPI. Esta situación podría limitar la capacidad institucional para anticipar, prevenir y responder oportunamente a amenazas emergentes. **R12**

UNIVERSIDAD MILITAR NUEVA GRANADA



Recomendación No. 13

A.5.8 — Seguridad de la información en la gestión de proyectos. Se evidencia la necesidad de definir y documentar claramente qué actividades institucionales se consideran proyectos y establecer la articulación entre los procesos de Planeación, Contratación y Gestión Estratégica TIC para incorporar requisitos y análisis de seguridad de la información durante su ciclo de vida. La ausencia de criterios homogéneos podría ocasionar que determinados proyectos no sean sometidos a evaluación de riesgos ni incorporen oportunamente requisitos de seguridad y privacidad. **R13**

Recomendación No. 14

A.5.10 — Uso aceptable de activos de información y otros activos asociados a la misma. Se evidencia la necesidad de consolidar y fortalecer los lineamientos de uso aceptable de la información y otros activos asociados, considerando que actualmente se encuentran distribuidos en diferentes apartados del Manual Integral de Políticas de Seguridad de la Información y que la Declaración de Aplicabilidad los relaciona principalmente con compromisos de confidencialidad. Esta dispersión puede dificultar su comprensión, aplicación uniforme y trazabilidad, aumentando el riesgo de interpretaciones inconsistentes sobre el uso autorizado de los activos institucionales. **R14**

Recomendación No. 15

A.5.10 — Uso aceptable de activos de información y otros activos asociados a la misma. Se evidencia la necesidad de definir y formalizar reglas institucionales para el uso de WhatsApp y otras aplicaciones de mensajería instantánea en actividades laborales, estableciendo criterios sobre información que puede compartirse, uso de cuentas personales o institucionales, grupos autorizados, tratamiento de datos personales, conservación de evidencias, transferencia de archivos y reporte de incidentes. La ausencia de lineamientos específicos puede generar divulgación no autorizada de información, pérdida de trazabilidad, exposición de datos personales y uso inadecuado de canales no controlados por la Universidad. **R15**

Recomendación No. 16

A.5.16 — Gestión de la identidad. Se evidencia la necesidad de fortalecer el esquema de acceso a las redes inalámbricas institucionales mediante mecanismos de autenticación individual, autorización temporal y trazabilidad de usuarios, especialmente para visitantes y terceros. La implementación de esquemas de acceso temporal con identificación del usuario, aprobación cuando corresponda y vencimiento automático permitiría reducir la dependencia de claves compartidas, mejorar la identificación de las conexiones y facilitar su revocación. La ausencia de estos mecanismos podría incrementar el riesgo de conexiones no autorizadas y limitar la trazabilidad sobre el uso de la red institucional. **R16**

Recomendación No. 17

A.5.22 — Seguimiento, revisión y gestión de cambios de servicios de proveedores. Se evidencia la necesidad de fortalecer el seguimiento a los proveedores durante la ejecución contractual, considerando que la supervisión documentada se concentra principalmente al cierre y no se realiza sistemáticamente durante periodos intermedios de prestación del servicio. Esta situación podría

UNIVERSIDAD MILITAR NUEVA GRANADA



impedir la identificación oportuna de desviaciones en el cumplimiento de requisitos de seguridad, niveles de servicio y cambios que incrementen los riesgos asociados al proveedor. **R17**

Recomendación No. 18

A.5.25 — Evaluación y decisión sobre los eventos de seguridad de la información. Se evidencia la necesidad de fortalecer y documentar los criterios utilizados para evaluar los eventos de seguridad y determinar cuándo deben ser clasificados y gestionados como incidentes. La ausencia de criterios homogéneos de evaluación, severidad y priorización podría generar tratamientos diferentes ante eventos similares y retrasar la activación de los mecanismos de respuesta. **R18**

Recomendación No. 19

A.5.29 — Seguridad de la información durante interrupciones. Se evidencia la necesidad de revisar y fortalecer el documento actualmente denominado Plan de Recuperación de Desastres, asegurando que su alcance contemple integralmente la continuidad de la seguridad de la información durante situaciones de interrupción y que su denominación y estructura reflejen adecuadamente dicho propósito. Mantener un enfoque limitado exclusivamente a recuperación tecnológica podría dejar sin tratamiento otros controles de seguridad necesarios durante escenarios de contingencia. **R19**

Recomendación No. 20

A.5.33 — Protección de registros. Se evidencia la necesidad de fortalecer el mecanismo alternativo utilizado para el registro de ingresos cuando el sistema principal de control de acceso no se encuentra disponible, considerando que durante la auditoría estos registros estaban siendo gestionados manualmente mediante un archivo Excel almacenado localmente en el computador del punto de entrada. Esta situación podría afectar la disponibilidad, integridad y trazabilidad de los registros y generar riesgo de pérdida de información ante falla, daño o indisponibilidad del equipo, especialmente si no se cuenta con mecanismos de respaldo y recuperación definidos para este tipo de contingencias. Se recomienda establecer un procedimiento alternativo formal, con almacenamiento seguro, respaldo periódico y posterior conciliación con el sistema principal de control de acceso. **R20**

Recomendación No. 21

A.6.2 — Términos y condiciones de empleo. Se evidencia la necesidad de fortalecer los actos administrativos y demás instrumentos que formalizan la vinculación de personal, incorporando de manera explícita responsabilidades relacionadas con seguridad y privacidad de la información, complementando los compromisos de confidencialidad actualmente existentes. La ausencia de requisitos suficientemente detallados podría generar desconocimiento o interpretaciones diferentes respecto de las obligaciones que deben observar las personas durante su vinculación. **R21**

Recomendación No. 22

A.7.11 — Servicios de apoyo. Se evidencia la necesidad de fortalecer los lineamientos para el uso de la red eléctrica regulada, considerando que durante el recorrido se identificaron equipos de consumo general, como hornos microondas, conectados a circuitos destinados al soporte de infraestructura tecnológica. Esta situación podría generar consumo innecesario de la capacidad disponible,

UNIVERSIDAD MILITAR NUEVA GRANADA



sobrecargas o perturbaciones eléctricas que afecten la estabilidad y disponibilidad de los equipos y servicios tecnológicos. Se recomienda definir, comunicar y controlar los tipos de equipos autorizados para conexión a la red regulada. **R22**



Evidencia fotográfica 1. Equipos de consumo general conectados a circuitos destinados al soporte de infraestructura tecnológica.

Recomendación No. 23

A.7.14 — Eliminación segura o reutilización de equipos. Se evidencia la necesidad de fortalecer la gestión del ciclo de vida de los equipos tecnológicos que han sido retirados de operación por daño, obsolescencia o sustitución, considerando que durante los recorridos se identificaron en diferentes áreas equipos pendientes de reintegro, baja o disposición final que permanecen almacenados por periodos prolongados. Esta situación podría dificultar la trazabilidad de los activos y prolongar innecesariamente su custodia, además de incrementar el riesgo de pérdida, acceso no autorizado o recuperación de información almacenada en los dispositivos cuando no se aplican oportunamente procedimientos de borrado seguro y disposición. Adicionalmente, la permanencia innecesaria de estos activos puede generar costos administrativos asociados a almacenamiento, aseguramiento y gestión patrimonial. Se recomienda establecer y controlar tiempos para el reintegro, evaluación, borrado seguro, baja, reutilización o disposición final de los equipos. **R23**

Recomendación No. 24

A.8.15 — Registro de eventos. Se evidencia la necesidad de fortalecer la trazabilidad de las conexiones a las redes inalámbricas institucionales, considerando que la asignación dinámica de direcciones IP y el uso de credenciales compartidas pueden dificultar la asociación inequívoca entre una dirección IP, un dispositivo y un usuario determinado. Esta situación podría limitar la capacidad de investigación y atribución ante incidentes de seguridad, por lo que resulta conveniente asegurar la correlación de registros de DHCP, controlador inalámbrico, mecanismos de autenticación y firewall.

R24

UNIVERSIDAD MILITAR NUEVA GRANADA



Recomendación No. 25

A.8.20 — Seguridad en redes. Se evidencia la necesidad de revisar y fortalecer el esquema de exposición y acceso remoto al Sistema de Gestión Documental CADET, considerando que actualmente se encuentra accesible directamente desde Internet. Resulta conveniente evaluar si la publicación pública es estrictamente necesaria para el modelo de operación y, de acuerdo con el riesgo, implementar mecanismos adicionales de protección como acceso restringido, VPN, ZTNA, autenticación reforzada, filtrado de aplicaciones o controles equivalentes. Mantener una superficie de exposición mayor a la necesaria podría incrementar la probabilidad de intentos de acceso no autorizado, explotación de vulnerabilidades y afectación de la información institucional. **R25**

Recomendación No. 26

A.8.20 — Seguridad en redes. Se evidencia la necesidad de fortalecer el control sobre los puntos físicos de red dispuestos en diferentes áreas de las sedes de la Universidad, considerando que algunos se encuentran accesibles para conexión directa de dispositivos y no se evidenció, durante el recorrido, un mecanismo visible que permita determinar si los puertos se encuentran deshabilitados, restringidos o sujetos a autenticación antes de otorgar conectividad. Esta situación podría facilitar la conexión de dispositivos no autorizados a segmentos de red institucionales, limitar la trazabilidad de los accesos e incrementar el riesgo de acceso indebido a recursos internos. **R26**

Recomendación No. 27

A.8.26 — Requisitos de seguridad de las aplicaciones. Se evidencia la necesidad de fortalecer la definición, implementación y verificación de requisitos de seguridad para las aplicaciones y servicios web institucionales. El “Informe Ethical Hacking/Vulnerabilidades” de enero de 2026, cuyo alcance comprendió UNIVEX y la página web institucional, reportó 12 vulnerabilidades —1 crítica, 2 altas, 6 medias y 3 bajas—, entre ellas uso de componentes obsoletos, protocolos criptográficos inseguros, certificado SSL/TLS vencido, ausencia de cabeceras de seguridad HTTP y métodos HTTP innecesarios habilitados. De manera complementaria, la evaluación técnica realizada durante la auditoría al portal institucional identificó ausencia de controles y encabezados como Content Security Policy, protección contra framing, X-Content-Type-Options y Subresource Integrity. Estas evidencias muestran la conveniencia de fortalecer los criterios de seguridad, endurecimiento, validación y seguimiento de las aplicaciones expuestas, con el fin de reducir la probabilidad de explotación de configuraciones o componentes vulnerables. **R27**

HALLAZGOS

(Descripción del Problema + Evidencia Objetiva + Requisito Incumplido)

Hallazgo No. 1

D.1 — Diagnóstico MSPI. Se evidenció que el diagnóstico utilizado por la Universidad corresponde al ejercicio de Autodiagnóstico de Gobierno Digital 2025 para MIPG, sin evidenciarse la aplicación del instrumento de diagnóstico del MSPI ni una equivalencia documentada que demuestre la cobertura

UNIVERSIDAD MILITAR NUEVA GRANADA



integral de sus fases, requisitos y controles. Esta situación limita la identificación objetiva de las brechas específicas del Modelo y puede afectar la priorización de las acciones necesarias para su implementación y mejora. Se incumple el requisito D.1 “Diagnóstico MSPI” del MSPI V5. **H1**

Hallazgo No. 2

4.3 — Determinación del alcance del MSPI. Se evidenció que la Universidad dispone del documento “Alcance Versión 2026 VF”, elaborado el 21 de julio de 2026, el cual desarrolla el contexto, las partes interesadas, las interfaces, los procesos incluidos y los límites organizacionales, físicos y tecnológicos del SGSI/MSPI. No obstante, durante la auditoría no se aportó evidencia que permita demostrar su aprobación y formalización institucional como información documentada vigente dentro del sistema de gestión. Esta situación limita la capacidad de demostrar que los límites y la aplicabilidad del MSPI han sido formalmente determinados, comunicados y controlados por la instancia competente. Se incumple el requisito 4.3 “Determinación del alcance del MSPI” del MSPI V5. **H2**

Hallazgo No. 3

5.2 — Política. Se evidenció que la Universidad cuenta con antecedentes institucionales de política y con el Manual Integral de Políticas de Seguridad de la Información, revisión 1, aprobado por Rectoría y creado en 2019; adicionalmente, el PESI 2025-2026 contempla dentro de sus actividades la formalización y aprobación de una política de seguridad de la información. No obstante, durante la auditoría no se aportó una Política de Seguridad y Privacidad de la Información vigente, formalmente aprobada y armonizada con el MSPI V5, que actualice integralmente los instrumentos históricos y establezca los compromisos actuales de la Alta Dirección. Esta situación limita la existencia de una directriz vigente y verificable para orientar los objetivos, responsabilidades, cumplimiento y mejora del Modelo. Se incumple el requisito 5.2 “Política” del MSPI V5. **H3**

Hallazgo No. 4

5.3 — Roles, responsabilidades y autoridades. Se evidenció que los roles, responsabilidades y autoridades necesarios para la operación del MSPI no se encuentran completamente definidos, formalizados e integrados en los instrumentos institucionales, identificándose ausencia o insuficiente definición de funciones relacionadas con seguridad y privacidad, propietarios y custodios de activos, dueños de riesgos, proveedores y otras responsabilidades pertinentes; adicionalmente, no se evidenció la designación formal del responsable de protección de datos personales. Esta situación puede generar vacíos de autoridad, duplicidad de funciones y falta de responsabilidad sobre decisiones y controles del sistema. Se incumple el requisito 5.3 “Roles, responsabilidades y autoridades” del MSPI V5. **H4**

Hallazgo No. 5

6.1.2 — Evaluación de riesgos de seguridad de la información. Se evidenció que la identificación y evaluación de riesgos de seguridad y privacidad se encuentra concentrada principalmente en el proceso de Gestión Estratégica TIC, sin evidenciarse una identificación sistemática de estos riesgos en los demás procesos institucionales que crean, procesan, almacenan o transmiten información. Esta situación limita la cobertura de la gestión de riesgos y puede ocasionar que amenazas y vulnerabilidades presentes en procesos académicos, administrativos y de apoyo no sean evaluadas ni tratadas oportunamente. Se incumple el requisito 6.1.2 “Evaluación de riesgos de seguridad de la

UNIVERSIDAD MILITAR NUEVA GRANADA



información" del MSPI V5. **H5**

Hallazgo No. 6

6.1.3 — Tratamiento de riesgos de seguridad de la información. Se evidenció que la Universidad cuenta con una Declaración de Aplicabilidad versión 2, creada el 25 de junio de 2025 y aprobada el 8 de septiembre de 2025, así como con un Plan de Tratamiento de Riesgos y documentos técnicos complementarios de SoA. No obstante, en los soportes revisados no se evidenció una trazabilidad suficiente y bidireccional que permita relacionar cada escenario de riesgo con la decisión de tratamiento adoptada, los controles seleccionados, su justificación, responsables, evidencia de implementación y criterios de eficacia. La matriz SoA consolidada V1 declara la aplicabilidad de los controles y sus responsables, pero no identifica de forma explícita los riesgos concretos que originan cada selección de control. Esta situación limita la capacidad de demostrar que el tratamiento responde de manera sistemática a los riesgos evaluados y que los controles seleccionados son suficientes y eficaces. Se incumple el requisito 6.1.3 "Tratamiento de riesgos de seguridad de la información" del MSPI V5. **H6**

Hallazgo No. 7

7.4 — Comunicación. Se evidenció que el Plan Estratégico de Comunicaciones institucional revisado no incorpora de manera explícita las necesidades de comunicación asociadas al MSPI, sin evidenciarse la determinación integral de qué comunicar, cuándo, a quién, cómo y quién es responsable de las comunicaciones relacionadas con seguridad y privacidad de la información. Esta situación puede generar comunicaciones fragmentadas o no oportunas y limitar la apropiación del Modelo por las partes interesadas. Se incumple el requisito 7.4 "Comunicación" del MSPI V5. **H7**

Hallazgo No. 8

7.5.1 — Información documentada – Generalidades. Se evidenció que la Universidad dispone de diversos documentos del MSPI, entre ellos planes de seguridad y riesgos, una Declaración de Aplicabilidad y un Procedimiento de Gestión del Cambio del SGSI formalmente aprobado. Sin embargo, durante la auditoría se identificaron documentos clave que aún no evidencian formalización o aprobación institucional, entre ellos la matriz de roles y los perfiles propuestos de CISO y Oficial de Protección de Datos, además de la necesidad de actualizar la política general de seguridad. Esta situación impide asegurar que toda la información documentada necesaria para la operación consistente del MSPI se encuentre vigente, aprobada, controlada y disponible para los responsables. Se incumple el requisito 7.5.1 "Información documentada – Generalidades" del MSPI V5. **H8**

Hallazgo No. 9

9.1 — Seguimiento, medición, análisis y evaluación. Se evidenció que el esquema de seguimiento y medición del MSPI presenta debilidades en su ejecución, identificándose indicadores del año 2025 sin resultados de medición y ausencia de análisis durante 2026 conforme a la periodicidad definida para el seguimiento. Esta situación limita la capacidad de la Universidad para determinar tendencias, desviaciones y eficacia de los controles, así como para adoptar oportunamente decisiones de mejora. Se incumple el requisito 9.1 "Seguimiento, medición, análisis y evaluación" del MSPI V5. **H9**

UNIVERSIDAD MILITAR NUEVA GRANADA



Hallazgo No. 10

9.3 — Revisión por la Dirección. Se evidenció que, en la Revisión por la Dirección realizada el 16 de septiembre de 2026, no se aportó evidencia suficiente que permita demostrar que las entradas y salidas aplicables al MSPI hubieran sido presentadas y analizadas integralmente dentro del ejercicio efectuado por la Alta Dirección. Si bien la Revisión por la Dirección puede desarrollarse de manera integrada con los demás componentes del Sistema Integrado de Gestión (SIG), debe asegurarse la inclusión y trazabilidad de la información correspondiente al desempeño del MSPI, incluyendo, según corresponda, resultados de seguimiento y medición, cumplimiento de objetivos, resultados de auditorías, estado de acciones, cambios, riesgos, necesidades de recursos y oportunidades de mejora. La evidencia revisada no permitió demostrar de manera suficiente dicho análisis integral. Se incumple el requisito 9.3 "Revisión por la Dirección" del MSPI V5. **H10**

Hallazgo No. 11

10.1 — Eficacia del mejoramiento. Se evidenció que el tratamiento de los hallazgos derivados de la auditoría 2024 presenta un nivel insuficiente de cumplimiento. El Informe de Seguimiento GI-MA-F-39 del 10 de agosto de 2026, aprobado por la Oficina de Control Interno de Gestión, establece que el plan actualizado comprende 33 hallazgos y 98 actividades y que, con corte al 31 de julio de 2026, 35 actividades (35 %) cumplen con la evidencia requerida mientras 63 (65 %) no cumplen. Esta proporción demuestra que una parte significativa de las acciones continúa pendiente o no cuenta con evidencia suficiente, prolongando la exposición a las causas y riesgos que originaron los hallazgos. Se incumple el requisito 10.1 "Mejora continua" del MSPI V5. **H11**

Hallazgo No. 12

10.2 — No conformidad y acción correctiva. Se evidenció que el tratamiento de las no conformidades y acciones correctivas derivadas de auditorías anteriores no se ejecuta de manera consistente con análisis de causa y verificación documentada de eficacia. El Informe de Seguimiento GI-MA-F-39 del 10 de agosto de 2026 reporta que, de 98 actividades del plan actualizado, 63 (65 %) no cumplen con la evidencia requerida; adicionalmente, en la matriz de seguimiento y en la muestra revisada durante la auditoría se identificaron acciones sin demostración consistente de análisis de causa raíz o de evaluación de eficacia, así como casos en los que se retiraron indicadores que presentaban desviaciones sin evidenciar un tratamiento formal de las causas que originaron su incumplimiento. Esta situación puede ocasionar la recurrencia de las no conformidades y limita la capacidad de demostrar que las acciones adoptadas eliminan efectivamente sus causas. Se incumple el requisito 10.2 "No conformidad y acción correctiva" del MSPI V5. **H12**

Hallazgo No. 13

A.5.5 — Contacto con las autoridades. Se evidenció que el mecanismo institucional para mantener los contactos pertinentes con autoridades relacionadas con seguridad de la información se encuentra aún en proceso de construcción. Si bien el Manual Integral de Políticas de Seguridad de la Información define el responsable autorizado para realizar reportes ante autoridades, no se evidencia un esquema formalizado y plenamente implementado que identifique las autoridades aplicables, mecanismos de contacto, responsables, criterios de contacto y escalamiento, ni su mantenimiento actualizado. Esta

UNIVERSIDAD MILITAR NUEVA GRANADA



situación podría retrasar la coordinación, escalamiento, notificación y respuesta oportuna ante incidentes o situaciones que requieran intervención de autoridades externas. Se incumple el control A.5.5 “Contacto con las autoridades” del MSPI V5. **H13**

Hallazgo No. 14

A.5.6 — Contacto con grupos de interés especiales. Se evidenció que la Universidad no cuenta con mecanismos formalmente establecidos y mantenidos para el contacto con grupos de interés especializados, foros, asociaciones profesionales, CSIRT/CERT u otras comunidades relevantes de seguridad de la información. Esta situación limita el intercambio oportuno de conocimiento, alertas, experiencias, buenas prácticas y mecanismos de cooperación frente a amenazas emergentes, afectando la capacidad de actualización y fortalecimiento del MSPI. Se incumple el control A.5.6 “Contacto con grupos de interés especiales” del MSPI V5. **H14**

Hallazgo No. 15

A.5.9 — Inventario de información y otros activos asociados. Se evidenció que la Universidad no cuenta actualmente con un inventario de información y otros activos asociados plenamente implementado y vigente, encontrándose este en proceso de construcción y sin aprobación definitiva en KAWAK. Esta situación limita la identificación, trazabilidad, valoración y asignación de responsabilidades sobre los activos que soportan la información institucional, afectando la adecuada gestión de riesgos y la definición de controles de protección. Se incumple el control A.5.9 “Inventario de información y otros activos asociados” del MSPI V5. **H15**

Hallazgo No. 16

A.5.12 — Clasificación de la información. Se evidenció que, aunque el Manual Integral de Políticas de Seguridad de la Información establece lineamientos para la clasificación de la información, estos no se encuentran implementados de manera efectiva sobre los activos de información institucionales. Esta situación impide determinar y aplicar consistentemente niveles de protección acordes con la confidencialidad, integridad, disponibilidad y requisitos aplicables a la información, aumentando el riesgo de tratamientos inadecuados. Se incumple el control A.5.12 “Clasificación de la información” del MSPI V5. **H16**

Hallazgo No. 17

A.5.13 — Etiquetado de la información. Se evidenció que no se encuentra implementado un esquema institucional de etiquetado de la información acorde con los niveles de clasificación definidos, identificándose además que en la gestión documental no se reconoce actualmente documentación clasificada como confidencial y se gestiona de manera general como no confidencial. Esta situación dificulta que usuarios y custodios identifiquen el nivel de protección requerido y puede ocasionar tratamientos, accesos, transferencias o disposiciones inadecuadas de información sensible. Se incumple el control A.5.13 “Etiquetado de la información” del MSPI V5. **H17**

Hallazgo No. 18

A.5.15 — Control de acceso. Se evidenció que la red inalámbrica destinada a invitados en la sede

UNIVERSIDAD MILITAR NUEVA GRANADA



Facultad de Medicina y Ciencias de la Salud presenta cobertura que se extiende hasta zonas exteriores de la Universidad y permite la conexión sin mecanismos de autenticación, credenciales de acceso o autorización previa. Esta situación posibilita que personas ubicadas fuera del perímetro institucional puedan utilizar la conectividad provista por la Universidad sin identificación ni control, incrementando el riesgo de uso no autorizado de los recursos de red, consumo indebido del servicio, realización de actividades maliciosas desde la infraestructura institucional y limitaciones para la trazabilidad de los usuarios conectados. Se incumple el control A.5.15 “Control de acceso” del MSPI V5. **H18**

Hallazgo No. 19

A.5.16 — Gestión de identidades. Se evidenció que el acceso a las redes inalámbricas POS_PRIV y POS_PUB se realiza mediante una credencial compartida conocida por múltiples usuarios, sin un mecanismo de autenticación individual que permita identificar, autorizar y revocar de manera diferenciada los accesos a la red institucional. Esta situación reduce la trazabilidad de las conexiones, dificulta la atribución de acciones y aumenta el riesgo de acceso no autorizado a los recursos tecnológicos de la Universidad. Se incumple el control A.5.16 “Gestión de identidades” del MSPI V5. **H19**

Hallazgo No. 20

A.5.20 — Abordar la seguridad de la información en los acuerdos con proveedores. Se evidenció que la Universidad dispone del formato institucional GA-GH-F-40 “Acuerdo Específico de Confidencialidad para Contratistas”, revisión 1 de 2026, el cual incorpora obligaciones relacionadas con medidas de seguridad, notificación de incidentes, auditoría, confidencialidad, devolución o destrucción de información y responsabilidades posteriores a la terminación. No obstante, en los contratos con proveedores revisados durante la auditoría no se evidenció de manera suficiente y homogénea la incorporación o aplicación de requisitos de seguridad y privacidad acordes con los riesgos específicos del producto o servicio suministrado. Esta situación puede generar diferencias en la exigibilidad de obligaciones sobre acceso, tratamiento de información, reporte de incidentes, continuidad y devolución o eliminación de activos durante la relación contractual. Se incumple el control A.5.20 “Abordar la seguridad de la información en los acuerdos con proveedores” del MSPI V5. **H20**

Hallazgo No. 21

A.5.21 — Gestión de la seguridad de la información en la cadena de suministro TIC. Se evidenció que no se encuentran incorporados de manera suficiente requisitos específicos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios TIC, incluidos los derivados de terceros, componentes, soporte y dependencias tecnológicas. Esta situación puede extender riesgos hacia la infraestructura y servicios institucionales sin que existan obligaciones y controles contractuales adecuados sobre los diferentes participantes de la cadena de suministro. Se incumple el control A.5.21 “Gestión de la seguridad de la información en la cadena de suministro TIC” del MSPI V5. **H21**

UNIVERSIDAD MILITAR NUEVA GRANADA



Hallazgo No. 22

A.5.24 — Planificación y preparación de la gestión de incidentes. Se evidenció que la Universidad cuenta con lineamientos generales para la gestión de incidentes en el Manual Integral de Políticas de Seguridad de la Información y con capacidades tecnológicas de detección y respuesta soportadas, entre otros mecanismos, por el servicio EDR/MDR y CrowdStrike. No obstante, en la evidencia suministrada durante la auditoría no se aportó un procedimiento vigente y plenamente implementado que defina de manera integral funciones y responsabilidades, criterios de clasificación y severidad, mecanismos de escalamiento, registros de incidentes, informes de cierre y lecciones aprendidas que permitan demostrar la preparación y trazabilidad del proceso. Esta situación puede generar tratamientos no homogéneos, dificultades de escalamiento y pérdida de evidencia para la mejora posterior a los incidentes. Se incumple el control A.5.24 “Planificación y preparación de la gestión de incidentes” del MSPI V5. **H22**

Hallazgo No. 23

A.5.30 — Preparación de las TIC para la continuidad de la actividad. Se evidenció que no se han realizado pruebas de los mecanismos definidos para la recuperación y continuidad de las tecnologías de información y comunicaciones. Esta situación impide demostrar que las capacidades de recuperación funcionen dentro de los tiempos y condiciones requeridos ante una interrupción real, aumentando el riesgo de indisponibilidad prolongada y afectación de los servicios institucionales. Se incumple el control A.5.30 “Preparación de las TIC para la continuidad de la actividad” del MSPI V5. **H23**

Hallazgo No. 24

A.5.34 — Privacidad y protección de la IIP. Se evidenció que en diferentes puntos de atención de la Universidad se utilizan códigos QR que direccionan a formularios para el registro y recolección de datos personales con distintos fines, sin que en el momento de la recolección se informe de manera suficiente al titular sobre las finalidades del tratamiento, el responsable del tratamiento, los derechos que le asisten ni el acceso a la Política de Tratamiento de Datos Personales de la UMNG. Esta situación afecta la transparencia del tratamiento y limita la capacidad de la Universidad para demostrar que los titulares han sido debidamente informados sobre el uso de sus datos personales antes o durante su recolección. Se incumple el control A.5.34 “Privacidad y protección de la IIP” del MSPI V5. **H24**

UNIVERSIDAD MILITAR NUEVA GRANADA



Evidencia fotográfica 2. Qr Colocado en la entrada de la sede Facultad de Medicina y Ciencias de la Salud | Qr Colocado en la entrada de la sede Sede principal: Carrera 11 n.º 101-80

Hallazgo No. 25

A.5.34 — Privacidad y protección de la IIP. Se evidenció que en los puntos de acceso al edificio de la Facultad de Medicina y Ciencias de la Salud no se encuentra dispuesto de manera visible y oportuna el aviso de privacidad informando que está siendo grabado. Esta situación limita la transparencia del tratamiento de imágenes y la posibilidad de informar adecuadamente a los titulares sobre la recolección y tratamiento de sus datos personales mediante CCTV. Se incumple el control A.5.34 “Privacidad y protección de la IIP” del MSPI V5. **H25**

Hallazgo No. 26

A.5.34 — Privacidad y protección de la IIP. Se evidenció que, durante el ingreso de visitantes de la sede principal de la UMNG – Calle 100, las autorizaciones relacionadas con el tratamiento de datos personales de niños del Colegio Skills Garden a la actividad de la huerta de Patroclo, no contenían información suficientemente completa sobre las finalidades específicas del tratamiento ni permitían demostrar de manera adecuada la autorización otorgada por su representante legal. En algunos registros se observaron únicamente nombres digitados en el campo de autorización y no se especificaba, entre otros aspectos, si la imagen o voz de los menores podía ser captada, grabada, utilizada o divulgada durante la actividad. De igual manera ningún formato tenía diligenciado los datos de fecha y lugar. Esta situación limita la capacidad de la Universidad para demostrar que el tratamiento de datos personales de menores se realiza de manera previa, expresa, informada y verificable, incrementando el riesgo de utilización de imágenes u otros datos para finalidades no suficientemente informadas al representante legal. Se incumple el control A.5.34 “Privacidad y protección de la IIP” del MSPI V5. **H26**

UNIVERSIDAD MILITAR NUEVA GRANADA



Hallazgo No. 27

A.5.36 — Cumplimiento de las políticas, reglas y normas de seguridad de la información. Se evidenció que no se dispone de registros suficientes que demuestren la realización sistemática de revisiones sobre el cumplimiento de las políticas, reglas y normas de seguridad de la información y que, ante las desviaciones identificadas, no se evidenció la generación consistente de acciones correctivas. Esta situación limita la capacidad de la Universidad para detectar incumplimientos, corregir sus causas y demostrar la eficacia de sus mecanismos de supervisión. Se incumple el control A.5.36 “Cumplimiento de las políticas, reglas y normas de seguridad de la información” del MSPI V5. **H27**

Hallazgo No. 28

A.6.2 — Condiciones del empleo – obligaciones contractuales. Se evidenció que los contratos revisados no incorporan de manera suficiente las responsabilidades específicas de seguridad y privacidad de la información aplicables al personal, más allá de los compromisos generales de confidencialidad identificados. Esta situación limita la exigibilidad contractual de obligaciones relacionadas con uso de activos, controles de acceso, manejo de información, reporte de incidentes y cumplimiento de las políticas institucionales. Se incumple el control A.6.2 “Condiciones del empleo – obligaciones contractuales” del MSPI V5. **H28**

Hallazgo No. 29

A.6.7 — Trabajo remoto. Se evidenció que la Universidad ha establecido lineamientos y requerimientos de seguridad para las personas formalmente vinculadas bajo la modalidad de teletrabajo, sin evidenciarse controles equivalentes para las demás actividades de trabajo remoto mediante las cuales funcionarios, contratistas, docentes u otros usuarios pueden acceder, procesar o gestionar información institucional fuera de las instalaciones. Esta situación puede generar condiciones de seguridad heterogéneas y aumentar la exposición de la información frente a accesos no autorizados, uso de redes o dispositivos no controlados, pérdida de información y dificultades para la gestión de incidentes. Se incumple el control A.6.7 “Trabajo remoto” del MSPI V5. **H29**

Hallazgo No. 30

A.7.2 — Controles de entrada física. Se evidenció que el cuarto de rack ubicado en la biblioteca de la sede Facultad de Medicina y Ciencias de la Salud no cuenta con mecanismos efectivos para restringir y registrar el acceso, al encontrarse sin control mediante llave o mecanismo equivalente y no disponer de una bitácora de ingreso. Esta situación permite el acceso no controlado a infraestructura de comunicaciones y limita la trazabilidad sobre las personas que ingresan al área, incrementando el riesgo de manipulación, desconexión, alteración, daño o acceso no autorizado a los equipos allí instalados. Se incumple el control A.7.2 “Controles de entrada física” del MSPI V5. **H30**

Hallazgo No. 31

A.7.2 — Controles de entrada física. Se evidenció que en la sede principal de la UMNG, Carrera 11 y la sede Facultad de Medicina y Ciencias de la Salud, los torniquetes de acceso permiten registrar ingresos consecutivos utilizando la misma credencial, sin que el sistema exija o valide previamente un evento de salida asociado. Esta situación debilita la efectividad del control de acceso físico, puede

UNIVERSIDAD MILITAR NUEVA GRANADA



permitir el uso repetido o compartido de una misma credencial y limita la trazabilidad sobre las personas que efectivamente ingresan a las instalaciones. Se incumple el control A.7.2 "Controles de entrada física" del MSPI V5. **H31**

Hallazgo No. 32

A.7.3 y A.7.5 — Seguridad de oficinas, salas e instalaciones y protección contra amenazas físicas y ambientales

Se evidenciaron deficiencias en las condiciones de seguridad y protección física y ambiental de cuatro áreas técnicas que alojan infraestructura tecnológica de la UMNG, documentadas mediante registros fotográficos individuales:

1. **Centro de datos de la Sede Campus Nueva Granada:** se almacenan materiales y equipos ajenos a la operación de la infraestructura que soporta servicios de red y videovigilancia, dejados temporalmente por personal de mantenimiento (ver evidencia fotográfica 3).
2. **Cuarto técnico de Ingeniería, bloque D, primer piso, sede principal, Carrera 11:** no dispone de bitácora para registrar los ingresos ni de un mecanismo de cierre mediante llave de seguridad. Se almacenan alimentos, bebidas y utensilios, y se mantiene un hervidor eléctrico conectado y utilizado dentro del recinto donde se encuentra el rack de red (ver evidencia fotográfica 4).
3. **Cuarto técnico de Ingeniería Mecatrónica, sede principal, Carrera 11:** se almacenan mobiliario, equipos, estructuras, cajas y otros elementos ajenos a su función técnica, que obstruyen el acceso y dificultan la inspección visual del rack de comunicaciones (ver evidencia fotográfica 5).
4. **Cuarto técnico de la Sede Campus Nueva Granada:** presenta suciedad, equipos con componentes internos expuestos por ausencia de cubiertas de protección, humedad significativa, deterioro de paredes y evidencias de filtraciones y goteras (ver evidencia fotográfica 6).
5. **Cuarto técnico de la Facultad de Humanidades, sede principal, Carrera 11:** presenta acumulación de polvo y suciedad sobre los dispositivos de comunicaciones, almacenamiento de elementos ajenos a la operación tecnológica y uso compartido del espacio con funciones diferentes a las propias de un cuarto técnico, incluidas condiciones asociadas a un área de baño (ver evidencia fotográfica 7)

Estas condiciones afectan el orden, el control de acceso y la protección de áreas técnicas; dificultan la inspección, el mantenimiento y la respuesta ante incidentes, e incrementan la exposición de la infraestructura a manipulación accidental o no autorizada, obstrucciones, derrames, corrosión, cortocircuitos, incendio, daño físico e indisponibilidad de los servicios soportados. Incumpliendo los controles A.7.3, «Seguridad de oficinas, salas e instalaciones», y A.7.5, «Protección contra amenazas físicas y ambientales», del MSPI V5. **H32**

Soporte: cuatro conjuntos de registros fotográficos, uno por cada área técnica descrita.

UNIVERSIDAD MILITAR NUEVA GRANADA



Evidencia fotográfica 3. Cilindro almacenado directamente sobre el piso en el cuarto técnico Sede Campus Nueva Granada.

Cuarto técnico Ingeniería bloque D – primer piso



Imagen A



Imagen B



Imagen C

Evidencias fotográficas del área inspeccionada

Evidencia fotográfica 4. Cuarto técnico de Ingeniería, bloque D, primer piso

UNIVERSIDAD MILITAR NUEVA GRANADA



Registro fotográfico – Cuarto técnico Ingeniería Mecatrónica



A. Cuarto técnico – Ingeniería Mecatrónica



B. Condiciones generales del cuarto técnico



C. Detalle de espacio reducido



D. Equipos y cableado en el cuarto técnico



E. Detalle de silla y elementos en el cuarto técnico

Evidencia fotográfica 5. Cuarto técnico de Ingeniería Mecatrónica



Evidencia fotográfica 6. Imágenes del cuarto técnico de la Sede Campus Nueva Granada evidenciando humedad, filtraciones y exposición de componentes técnicos a suciedad, corrosión, cortocircuitos, y daño físico.

UNIVERSIDAD MILITAR NUEVA GRANADA



Registro fotográfico – Cuarto técnico Facultad de Humanidades



Imagen A



Imagen B



Imagen C



Imagen D

Evidencia fotográfica 7. cuarto técnico de la Facultad de Humanidades

Hallazgo No. 33

A.7.7 — Escritorio limpio y pantalla limpia. Se evidenció que en la oficina de registro de entrada de la sede principal de la UMNG, Carrera 11, el equipo asignado al supervisor permanecía encendido y desatendido, con el bloqueo automático de sesión deshabilitado, manteniendo además abiertas aplicaciones como correo electrónico y WhatsApp con información visible y accesible desde el puesto de trabajo. Esta situación incrementa el riesgo de acceso no autorizado, consulta, modificación, envío o divulgación indebida de información institucional y limita la protección de las sesiones activas cuando el usuario se ausenta del equipo. Se incumple el control A.7.7 “Escritorio limpio y pantalla limpia” del MSPI V5. **H33**

Hallazgo No. 34

A.7.7 — Escritorio limpio y pantalla limpia. Se evidenció que la Universidad no cuenta con directrices institucionales formalmente definidas para la aplicación de prácticas de escritorio limpio y pantalla limpia, que establezcan criterios sobre protección de documentos, medios removibles, información visible, bloqueo de sesiones, manejo de impresiones y aseguramiento de los puestos de trabajo durante ausencias temporales o al finalizar la jornada. Esta situación puede generar exposición, pérdida, consulta o utilización no autorizada de información institucional y dificulta la aplicación homogénea de controles por parte de funcionarios, docentes, contratistas y demás usuarios. Se incumple el control A.7.7 “Escritorio limpio y pantalla limpia” del MSPI V5. **H34**

UNIVERSIDAD MILITAR NUEVA GRANADA



Hallazgo No. 35

A.7.8 — Ubicación y protección de equipos. Se evidenció que en el cuarto técnico TI, sede Calle 100, se mantienen equipos y componentes tecnológicos en condiciones inadecuadas de almacenamiento y protección, observándose equipos de comunicaciones apilados sobre mobiliario, monitores y otros dispositivos dispuestos directamente sobre el piso, cableado almacenado sin organización y elementos tecnológicos fuera de gabinetes o racks destinados para su protección. Esta situación incrementa el riesgo de daño físico, golpes, caídas, manipulación accidental, deterioro de los equipos y afectación de su disponibilidad, además de dificultar la adecuada administración y mantenimiento del área técnica. Se incumple el control A.7.8 “Ubicación y protección de equipos” del MSPI V5. **H35**

Cuarto técnico – Ingeniería Bloque D, primer piso – Sede Calle 100



Evidencia fotográfica 8. cuarto técnico TI, sede Calle 100

Hallazgo No. 36

A.7.13 — Mantenimiento de equipos. Se evidenció que en el cuarto técnico de la sede Facultad de Medicina y Ciencias de la Salud las UPS que soportan la infraestructura tecnológica se encuentran operando en modo bypass, condición que coincide con la ausencia de un plan formal de mantenimiento preventivo y correctivo para estos equipos. Esta situación puede reducir o anular la capacidad efectiva de respaldo y acondicionamiento eléctrico ante fallas del suministro de energía,

UNIVERSIDAD MILITAR NUEVA GRANADA



incrementando el riesgo de indisponibilidad, apagado inesperado, afectación de equipos y pérdida o corrupción de información. Se incumple el control A.7.13 “Mantenimiento de equipos” del MSPI V5.

H36



Evidencia fotográfica 9. Ups del cuarto técnico de la sede Facultad de Medicina y Ciencias de la Salud operando en modo bypass

Hallazgo No. 37

A.8.1 — Dispositivos terminales de usuario. Se evidenció que en el pasillo del segundo piso de la sede Facultad de Medicina y Ciencias de la Salud se encuentra instalado un televisor con pantalla táctil destinado a la divulgación de información pública, el cual permite al usuario interactuar con el sistema y realizar navegación más allá de la función prevista de visualización, encontrándose además conectado a una red privada institucional. Esta situación posibilita el uso no autorizado del dispositivo y puede facilitar el acceso indebido a recursos tecnológicos, la ejecución de acciones no previstas, la exposición de información o el aprovechamiento del equipo como punto de entrada hacia la red interna, incrementando el riesgo de afectación de la confidencialidad, integridad y disponibilidad de los activos de información. Se incumple el control A.8.1 “Dispositivos terminales de usuario” del MSPI V5.

H37

Hallazgo No. 38

A.8.17 — Sincronización de relojes. Se evidencia que en el centro de datos principal de la sede Calle 100, así como en computadores, cámaras y otros dispositivos tecnológicos de la sede, se presentan diferencias en la fecha y hora configuradas, sin evidenciarse una sincronización homogénea de los relojes de los sistemas y equipos. Esta situación puede afectar la correlación y trazabilidad de los registros de eventos, incidentes, accesos y actividades realizadas sobre la infraestructura tecnológica, dificultando el análisis forense, la reconstrucción de eventos y la determinación precisa de su secuencia temporal. Se incumple el control A.8.17 “Sincronización de relojes” del MSPI V5. **H38**

UNIVERSIDAD MILITAR NUEVA GRANADA



Hallazgo No. 39

A.8.17 — Sincronización de relojes. Se evidencia que en el sistema de CCTV de la Sede Campus Nueva Granada se presentan diferencias en la fecha y hora mostradas por distintas cámaras y dispositivos asociados al sistema de videovigilancia, sin evidenciarse una sincronización homogénea de los relojes. Esta situación puede afectar la correlación y trazabilidad de los registros de video, dificultar la reconstrucción cronológica de eventos y limitar la confiabilidad de la evidencia utilizada para investigaciones de incidentes de seguridad. Se incumple el control A.8.17 “Sincronización de relojes” del MSPI V5. **H39**

Hallazgo No. 40

A.8.23 — Filtrado web. Se evidencia que los mecanismos de filtrado web de las redes inalámbricas POS_PUB y POS_PRIV permiten el acceso a categorías y servicios que pueden incrementar la exposición a riesgos de seguridad, incluyendo servicios de proxy capaces de facilitar la evasión de controles de navegación. Esta situación puede aumentar la exposición de usuarios y activos institucionales a malware, phishing, contenido no autorizado y mecanismos de elusión de las medidas de seguridad. Se incumple el control A.8.23 “Filtrado web” del MSPI V5. **H40**

Hallazgo No. 41

A.8.26 — Requisitos de seguridad de las aplicaciones. Se evidencia que el Sistema de Gestión Documental CADET, accesible públicamente desde Internet mediante cadet.umng.edu.co, presenta debilidades en la configuración de seguridad de la aplicación web, identificándose ausencia de Content Security Policy (CSP), Strict-Transport-Security (HSTS), X-Content-Type-Options, protección contra framing y Subresource Integrity, así como una condición reportada sobre la cookie de sesión sin el atributo Secure o establecida mediante HTTP. Esta situación incrementa la exposición de un sistema autenticado que gestiona información institucional frente a riesgos relacionados con la protección de sesiones, contenido web y comunicaciones. Se incumple el control A.8.26 “Requisitos de seguridad de las aplicaciones” del MSPI V5. **H41**

CONCLUSIONES DE LA AUDITORÍA

La auditoría evidencia avances relevantes en la formalización del MSPI, entre ellos la existencia de una Declaración de Aplicabilidad aprobada, mecanismos institucionales de gestión documental, asignación de recursos y seguimiento a acciones de mejoramiento. Sin embargo, persisten brechas de carácter transversal en gobierno del MSPI, gestión de riesgos, medición, revisión por la dirección, proveedores, continuidad, privacidad, controles de acceso, gestión de activos y condiciones físicas y tecnológicas de varias sedes.

Una proporción de las condiciones observadas guarda relación con asuntos identificados en evaluaciones anteriores, particularmente en roles y responsabilidades, clasificación y etiquetado, proveedores, comunicaciones, continuidad, filtrado web, seguridad en proyectos y revisión del

UNIVERSIDAD MILITAR NUEVA GRANADA



desempeño. Esta recurrencia evidencia la necesidad de fortalecer el análisis de causa, la priorización, el cierre oportuno y la verificación de eficacia de las acciones correctivas.

A partir de la consolidación final, los responsables deberán formular o actualizar los planes de mejoramiento necesarios, priorizando las no conformidades que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional.

Elaborado por:	Aprobado por:
 GERMÁN ANDRÉS SÁNCHEZ ORTEGÓN Auditor Líder	 CLAUDIA JOHANNA CRANE SANTANDER Jefe Oficina de Control Interno de Gestión

Informe de Auditoría al Modelo de Seguridad y Privacidad de la Información - MSPI