Fecha de solicitud: diciembre de 2025

Solicitado por: Plan anual de auditoría 2026

Fecha de Elaboración Informe: 24 de agosto de 2026

Tema: Auditoría Exprés: “Modelo de Seguridad y Privacidad de la Información. (MSPI). Resolución 02277 de 2025 Mintic”.

Lugar: CAD

Equipo de Trabajo: Gloria Elena López Muñoz, auditora líder
Luis Gabriel Asprilla Martínez, auditor interno

SERVIDORES PARTICIPANTES EN LA AUDITORÍA EXPRÉS:

Funcionario (Dependencia / Cargo):

Sergio Andrés Cadavid Echeverry - Dirección de Tecnología e Información - Profesional universitario

Sara Castaño Agudelo - Dirección de Tecnología e Información - Contratista

Adriana Ximena Flórez Martínez - Dirección de Tecnología e Información - Contratista

ANTECEDENTES Y DESCRIPCIÓN DE LOS HECHOS

La Gerente de Auditoría Interna, en el marco de las funciones otorgadas por la Ley 87 de 1993 “Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones", incluyó en el Plan Anual de Auditoría para la vigencia 2026, la Auditoria exprés “Modelo de Seguridad y Privacidad de la Información. (MSPI). Resolución 02277 de 2025 Mintic”. Esta auditoría Exprés fue formalizada con la Dirección de Tecnología e Información mediante oficio con radicado N° 2026020026341 del 14 de julio de 2026. Se recibió la Carta de Representación mediante oficio con radicados N° 2026020026731 del 16 de julio de 2026. El alcance de la auditoria exprés estuvo enfocado a verificar el avance del modelo a partir del “Informe de diagnóstico al Modelo de Seguridad y Privacidad de la Información. (MSPI), presentado por la universidad de Antioquia en junio de 2025.”

VERIFICACIÓN DE LOS HECHOS

En desarrollo del proceso de la auditoría exprés, se realizó un análisis comparativo entre el diagnóstico efectuado por la universidad de Antioquia durante la vigencia

2025, los resultados de la evaluación de controles efectuada en julio de 2026, las evidencias de implementación suministradas por la Dirección de Tecnología e Información y las respuestas remitidas al cuestionario de validación técnica.

OBSERVACIONES

1. Brechas de implementación en controles tecnológicos del dominio A.8

Condición:
Se evidencia que de los 34 controles tecnológicos del dominio A.8, 13 presentan niveles de implementación cercanos al 60%:

- ✓ Dispositivos de punto final de usuario
- ✓ Acceso al código fuente
- ✓ Gestión de capacidad
- ✓ Gestión de configuración
- ✓ Prevención de fuga de datos (DLP)
- ✓ Copias de seguridad (Backup)
- ✓ Actividades de seguimiento/Monitoreo
- ✓ Uso de programas de utilidad privilegiados
- ✓ Ciclo de vida de desarrollo seguro
- ✓ Requisitos de seguridad de aplicaciones
- ✓ Arquitectura segura
- ✓ Codificación segura
- ✓ Pruebas de seguridad en desarrollo y aceptación

Criterio:

NTC-ISO/IEC 27001:2022 y Modelo de Seguridad y Privacidad de la Información, en los numerales del Anexo A.8 de la NTC-ISO/IEC 27001:2022 relacionados:

- ✓ Gestión de capacidad (A.8.6).
- ✓ Gestión de configuración (A.8.9).
- ✓ Prevención de fuga de datos (A.8.12).
- ✓ Copias de seguridad (A.8.13).
- ✓ Actividades de monitoreo (A.8.16).
- ✓ Uso de programas utilitarios privilegiados (A.8.18).
- ✓ Desarrollo seguro (A.8.25).
- ✓ Arquitectura segura (A.8.27).
- ✓ Codificación segura (A.8.28).

- ✓ Pruebas de seguridad (A.8.29).

Explicación de la Métrica:

El MSPI de MinTIC utiliza el Instrumento de Identificación de la Línea Base de Seguridad:

- ✓ Las hojas de Cláusulas evalúan los requisitos obligatorios de ISO 27001:2022.
- ✓ Las hojas de Organizacionales (A.5), Personas (A.6), Físicos (A.7) y Tecnológicos (A.8) evalúan los controles del Anexo A.
- ✓ El resultado se expresa como un porcentaje de implementación y efectividad por dominio.

De acuerdo con el instrumento aplicado el modelo calcula:
Nivel de implementación = Controles implementados y efectivos ×100 / Controles evaluados

La evidencia institucional muestra que el instrumento clasifica los resultados dentro de niveles de madurez o implementación. Por ejemplo:

- ✓ A.5 = 74 → Gestionado
- ✓ A.6 = 80 → Gestionado
- ✓ A.7 = 74 → Gestionado
- ✓ A.8 = 52 → se identificó como dominio con mayor brecha de fortalecimiento.

En consecuencia, cuando TI responde: "13 controles tecnológicos presentan un nivel de implementación del 60%", está indicando que esos controles, según el instrumento MSPI, han sido evaluados como **parcialmente implementados y eficaces**, pero todavía no alcanzan el estado objetivo definido por la entidad.

Proceso: Gestión de Tecnologías e Información.

OPORTUNIDADES DE MEJORA

1. La entidad dispone de métricas relacionadas con MFA, usuarios con contraseñas débiles, correos sospechosos reportados, incidentes por factor humano y participación en campañas.
2. Sería importante definir un indicador que permita demostrar objetivamente la efectividad de las campañas y su contribución a la disminución del riesgo.

3. En la entidad aún existen dependencias pendientes de incorporación al esquema institucional de autenticación reforzada. Se hace necesario que toda la organización cumpla con el nivel de seguridad establecida, para que de dicha manera se reduzcan los riesgos de: compromiso de credenciales, suplantación de identidad, accesos no autorizados.

4. La entidad realiza seguimiento a incidentes y eventos de seguridad; sin embargo, se requiere fortalecer mecanismos para explotar la información asociada a tendencias, recurrencia, causa raíz e indicadores predictivos que permitan orientar estratégicamente la toma de decisiones en la gestión y atención de eventos.

CONCLUSIONES DE LA AUDITORÍA

1. El análisis realizado permite concluir que la entidad ha experimentado un avance significativo en la consolidación de su Sistema de Gestión de Seguridad de la Información (SGSI), evidenciando mejoras en aspectos relacionados con gobernanza, formalización documental, cultura organizacional, gestión de incidentes, gestión de riesgos, sensibilización institucional y fortalecimiento progresivo de capacidades de ciberseguridad.

2. Se destaca la estructuración de un equipo especializado de Seguridad de la Información, la implementación del RoadMap de Seguridad, la ejecución del Plan Estratégico de Seguridad de la Información (PESI), el fortalecimiento de mecanismos de autenticación, la implementación progresiva de MFA, la adopción de herramientas de autogestión de credenciales, la gestión de vulnerabilidades y la consolidación de una estrategia institucional de cultura de seguridad.

3. Se han desarrollado actividades de sensibilización y se fortaleció la incorporación de contenidos de seguridad dentro de los procesos institucionales de formación, inducción y reinducción.

4. Se han implementado progresivamente mecanismos de fortalecimiento de autenticación mediante MFA y herramientas de autogestión de contraseñas (GINA), así como la ejecución de ejercicios técnicos orientados a identificar credenciales débiles dentro del Directorio Activo.

5. La entidad ha incorporado iniciativas orientadas al fortalecimiento de la postura de seguridad tales como: vigilancia tecnológica, monitoreo de Deep Web y Dark Web, gestión de vulnerabilidades, gestión de accesos privilegiados, protección de servicios en nube.

FIRMA RESPONSABLES DE LA AUDITORÍA EXPRÉS

ORIGINAL FIRMADO
Gloria Elena López Muñoz - Gerencia de Auditoría Interna – Profesional Universitaria

ORIGINAL FIRMADO
Luis Gabriel Asprilla Martínez - Gerencia de Auditoría Interna - Técnico Operativo

La mejor defensa para una cultura del control es la prevención y la mejora continua. Desde la Gerencia de Auditoría Interna trabajamos para promover el logro de los objetivos de Gobierno.