

Bogotá, , 29 de septiembre de 2026

De: DIANA CAROLINA BARRERO FLOREZ
Jefe de Oficina de Control Interno

Para: COMITÉ DE COORDINACIÓN DE CONTROL INTERNO

Asunto: INFORME DE SEGUIMIENTO CUMPLIMIENTO MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

INTRODUCCIÓN

Conforme a las funciones señaladas en la Ley 87 de 1993, Decretos reglamentarios y Plan Avante de la Sociedad Hotelera Tequendama; esta Oficina en su rol de evaluación y seguimiento al Sistema de Control Interno de la Entidad, acorde al plan de auditoría anual en la vigencia 2026 el cual fue aprobado por el Comité de Coordinación del 29 de enero de 2026 por lo cual es la encargada de la evaluación independiente del Sistema de Control Interno y de proponer las recomendaciones y sugerencias que contribuyan a su mejoramiento y optimización.

A continuación, se presenta el resultado del ejercicio.

METODOLOGÍA

Para llevar a cabo el seguimiento al cumplimiento al “Modelo de Seguridad y Privacidad de la Información” (MSPI) de la Sociedad Hotelera Tequendama, se realizó un análisis documental sobre el grado de implementación del modelo en cabeza de la Dirección de Tecnologías de la Información y Ciberseguridad La anterior actividad está enmarcada dentro de la Dimensión de control Interno del Modelo Integrado de Planeación y Gestión MIPG (3 línea de defensa).

OBJETIVO

Verificar y efectuar seguimiento al cumplimiento del “Modelo de Seguridad y Privacidad de la Información”, así como los procedimientos y controles establecidos, con el fin de mitigar riesgos en materia de ciberseguridad en la Sociedad Hotelera Tequendama S.A.

ALCANCE

Evaluar la efectividad y nivel de madurez del Modelo de Seguridad y Privacidad de la Información en la Sociedad Hotelera Tequendama con el propósito de brindar una adecuada protección de los activos de información como también la mitigación de riesgos relacionados con ciberseguridad y privacidad de la información.

RESULTADOS

De acuerdo con lo anterior, a continuación, se presenta el resultado del seguimiento realizado por la oficina de Control Interno al cumplimiento del Modelo de Seguridad y privacidad de la Información de la Sociedad Hotelera Tequendama. Se tomó como referencia el informe realizado por la Dirección de Tecnologías de la Información y Ciberseguridad:

- GENERALIDADES DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI).

La Oficina de Control Interno evidenció que el MSPI se encuentra publicado en la página web de la SHT, sin embargo, este no está firmado por la persona quien elaboró, revisó y aprobó.

Así mismo, se identificó el modelo se encuentra desactualizado con base en el marco normativo de la vigencia 2022 y en atención a los nuevos lineamientos definidos por el Departamento Administrativo de la Función Pública para la Gestión Integral de Riesgos, así como los lineamientos adoptados por la entidad definidos por el sector defensa y la implementación de sistemas de Inteligencia Artificial, se recomienda a la Dirección de Tecnologías de Información y Ciberseguridad actualizar el MSPI donde se adopten normas actuales que abarquen la realidad de la SHT en materia de seguridad y privacidad de la información, en el cual se defina un objetivo, los roles de los responsables de implementar y desarrollar acciones de detección, de prevención y de corrección.

- CUMPLIMIENTO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

La Oficina de Control Interno identificó con base en el informe de evaluación y seguimiento del modelo de seguridad y privacidad de la información (enero – agosto 2026) emitido por la Dirección de Tecnologías de la Información y Ciberseguridad lo siguiente en cumplimiento al numeral “7. DESCRIPCIÓN GENERAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)” del MSPI.

FASE	DESCRIPCIÓN	CUMPLIMIENTO
<u>DIAGNOSTICO</u>	Identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.	Se evidenció diagnóstico realizado por la dirección de tecnologías de la información y ciberseguridad con corte al año 2026 como: “Parcialmente Implementada” . <i>Cumple con la fase de diagnóstico</i>
<u>PLANIFICACIÓN</u>	Elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo	No se evidenció el plan de seguridad y privacidad de la información. <i>No cumple con el desarrollo de la fase de planificación.</i>

<u>IMPLEMENTACIÓN</u>	Implementación de la planificación realizada en la fase anterior del MSPI	<i>No cumple con la fase de implementación por falta del plan de seguridad y privacidad de la información.</i>
<u>EVALUACIÓN Y DESEMPEÑO</u>	Proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.	<i>No cumple con la fase de evaluación y desempeño por la ausencia del plan de seguridad y privacidad de la información.</i>
<u>MEJORA CONTINUA</u>	Consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.	<i>No cumple con la fase de mejora continua, debido a que no existe un plan de seguridad y privacidad de la información.</i>
<u>MODELO DE MADUREZ</u>	Este esquema permite identificar el nivel de madurez del MSPI en el que se encuentran las entidades, midiendo la brecha entre el nivel actual de la entidad y el nivel optimizado.	<i>No cumple con la fase de modelo de madurez por la ausencia del plan de seguridad y privacidad de la información.</i>

Con relación a las actividades enmarcadas en el MSPI planteado en la vigencia 2022 solo se evidenció el desarrollo de la fase de “Diagnostico” para la posterior implementación del plan de seguridad y privacidad de la información, sin embargo, dicho plan no se encuentra planteado para su ejecución, configurándose una debilidad que genera un posible riesgo de seguridad digital por la inexistencia de un plan de seguridad que defina los criterios de evaluación para la definición de las actividades que se deben desarrollar en la entidad en materia de seguridad y privacidad de la información, como también la definición de roles, responsabilidades, evidencias y seguimientos que garanticen la mejora continua del modelo así como su medición con relación a otras entidades y establecer su nivel de madurez

- ACTIVIDADES DE DETECCIÓN Y CORRECCIÓN TIC.

En entrevista con la Dirección de Tecnologías de la Información y Ciberseguridad, se establecieron unas actividades que permiten la detección y corrección de posibles amenazas que afecten a la seguridad y privacidad de la información de la SHT a través del sistema SecOps que permite a la entidad la detección de distintos dispositivos electrónicos que se encuentran conectados a la red como también a los correos electrónicos corporativos; dicho sistema se encarga de realizar el análisis de posibles amenazas y las corrige de forma automática. Sin embargo, no se evidenció que el sistema abarque las demás plataformas digitales que cuenta la SHT como lo son: ERP Dynamics 365, página web, IntegraTEQ, etc, que manejan flujos de información constante y son susceptibles a posibles amenazas.

La OCI recomienda que se articulen los controles sobre seguridad y protección de la información, con base en los riesgos planteados por la dirección de tecnologías de la información en la vigencia 2026 a través de la implementación de un MSPI acorde a las dinámicas actuales de la

entidad, como también, abarcar dentro del modelo, aspectos relacionados con el uso de la Inteligencia Artificial (IA) para la prevención de amenazas que afecten la integridad de la información digital, fomentando la mejora continua de los procesos.

RECOMENDACIONES

La Oficina de Control Interno recomienda a la Administración:

- 1) Se recomienda a la Dirección de Tecnologías de la Información y Ciberseguridad actualizar el MSPI que responda a los nuevos lineamientos de la gestión integral de riesgos, como también los lineamientos del sector defensa y normatividad vigente. Esta actualización debe definir los objetivos, roles, responsabilidades, tareas, entregables y vigencia del modelo.
- 2) Se recomienda a la Dirección de Tecnologías de la Información y Ciberseguridad estructurar, formalizar y ejecutar el Plan de Seguridad y Privacidad de la Información con base en los sistemas digitales y dinámicas actuales de la entidad.
- 3) Se recomienda ampliar el alcance del sistema SecOPS y los controles de ciberseguridad para que cobijen las plataformas digitales de la SHT como lo son el ERP Dynamics 365, página web, IA, etc. para la prevención de amenazas que comprometan la integridad de la información de la SHT

Cordialmente;



DIANA CAROLINA BARRERO FLOREZ
Jefe De Oficina De Control Interno
Oficina Control Interno

Anexos:

Elaboró: KIYOSHI JULIÁN MIYAUCHI CORTES / OCI

Aprobó: DIANA CAROLINA BARRERO FLOREZ OCI

Copia: JORGE RÍOS