2025-130-000654-3

Bogotá, , 8 de julio de 2025

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

Para: **COMITÉ DE COORDINACIÓN DE CONTROL INTERNO**

Asunto: **INFORME DE SEGUIMIENTO CUMPLIMIENTO POLÍTICAS CIBERSEGURIDAD MAYO Y JUNIO 2025**

INTRODUCCIÓN

Conforme a las funciones señaladas en la Ley 87 de 1993, Decretos reglamentarios y Plan Avante II 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 2025 el cual fue aprobado por el Comité de Coordinación de acuerdo a la resolución interna 202306130000075 de 2023 …" A continuación, se presenta el resultado del seguimiento.

METODOLOGÍA

Para llevar a cabo el seguimiento al cumplimiento de políticas de ciberseguridad de las diferentes dependencias de la Sociedad Hotelera Tequendama, se realizó un análisis del informe de seguridad del sistema WatchGuard EPDR realizado por la empresa Sciotec. 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 de las políticas de Ciberseguridad Corporativa, así como los procedimientos y controles establecidos para el funcionamiento, con el fin de mitigar riesgos en materia de ciberseguridad en la Sociedad Hotelera Tequendama S.A.

ALCANCE

Verificar que las políticas en el manejo de Ciberseguridad en la Sociedad Hotelera Tequendama se socializan en el nivel administrativo. Se realizó el análisis del informe de seguridad del sistema WatchGuard EPDR respecto a posibles riesgos que vulneren la integridad de la información en los equipos de cómputo de la SHT.

RESULTADOS

De acuerdo con lo anterior, a continuación, se presenta el resultado del seguimiento realizado por la oficina de Control Interno al cumplimiento de políticas de Ciberseguridad Corporativa de la Sociedad Hotelera Tequendama. Se tomó como referencia el informe de seguridad, arrojando el siguiente resultado:

Para el periodo evaluado, se evidenció que la SHT cuenta con un total de 102 equipos activos, los cuales 98 (96%) se encuentran “Correctamente Protegidos”, 2 (1.96%) se encuentran en “Protección con error” y 2 (1.96%) se encuentran “Sin Licencia”

Se evidenció que los programas ejecutados y analizados son 100% confiables según el informe de seguridad de WatchGuard.

No se evidenció la materialización de la presencia de Malware y PUPS (Aplicaciones con potencial malicioso) en el periodo auditado.

Cra 10 N° 26 -21. Piso 4 / Coworking, Bogotá
sociedadtequendama.com

Se evidenció que el informe de seguridad de WatchGuard, se establecen como criterios de riesgo, la falta de actualización de programas, licencias y sistema operativo en los distintos equipos de la SHT, de este análisis, dio como resultado que de la totalidad de los 102 equipos, 100 se encuentran con riesgo, de los cuales 53 (52%) tienen riesgo alto, 42 (41%) tienen riesgo medio, 5 (5%) tienen riesgo crítico y 2 (2%) no tienen riesgo. Es decir, que el 98% de los equipos de la SHT cuentan con la probabilidad de que se pueda materializar un riesgo referente a descargas de archivos o programas maliciosos que puedan comprometer la integridad de la información de los equipos y en general la información corporativa.

Del análisis general, se evidenciaron los equipos con mayor potencial de descargas de archivos maliciosos, los cuales corresponden a las siguientes dependencias:

- Dirección Financiera - 3 Equipos.
- Ingeniería Subacuatica - 1 Equipo.
- Operación Logística - 1 Equipo.
- Gestión de Negocios (Sociedades) - 1 Equipo.
- Dirección TIC´S - 2 Equipos.
- Gerencia General - 1 Equipo.
- A&B Suites - 1 Equipo.

Con base en lo anterior, se recomienda que las presentes dependencias generen los respectivos avisos al área de TIC´s con la finalidad de realizar las acciones pertinentes a la disminución de riesgos potenciales referentes a instalación de programas y archivos maliciosos que comprometan la información organizacional. Así mismo, en atención al decreto 338 de 2022 del Ministerio de las Tecnologías de la Información, para garantizar los lineamientos generales para fortalecer la seguridad digital, es necesario abarcar al personal administrativo de la Sociedad Hotelera Tequendama quienes deben estar en constante actualización sobre las distintas metodologías para salvaguardar y minimizar los riesgos en materia de ciberseguridad a través de jornadas para actualización de los programas, licencias y demás, fomentando así un ambiente de seguridad y confianza en la información que se comparte por los medios oficiales de la compañía.

Cra 10 N° 26 -21. Piso 4 / Coworking, Bogotá
sociedadtequendama.com

RECOMENDACIONES

La Oficina de Control Interno recomienda a la Administración:

1. Se recomienda realizar jornadas periódicas para la disminución de la presencia de equipos que presentan riesgo de contraer programas y archivos maliciosos.
2. Continuar con la implementación de las mejores prácticas de seguridad y protección de datos de acuerdo a las políticas impartidas desde la Presidencia de la SHT.
3. Se recomienda al equipo de ciberseguridad realizar actividades de inspección aleatoria con la finalidad de evidenciar el origen de aquellos casos de los equipos que presentan riesgo alto y crítico con la finalidad de reforzar y subsanar las posibles brechas en materia de ciberseguridad.

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:

Cra 10 N° 26 -21. Piso 4 / Coworking, Bogotá
sociedadtequendama.com