Sociedad Tequendama

2025-130-000964-3

Bogotá, , 27 de agosto de 2025

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

Para: **Funcionarios**

Asunto: **INFORME DE SEGUIMIENTO CUMPLIMIENTO POLÍTICAS CIBERSEGURIDAD JULIO 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

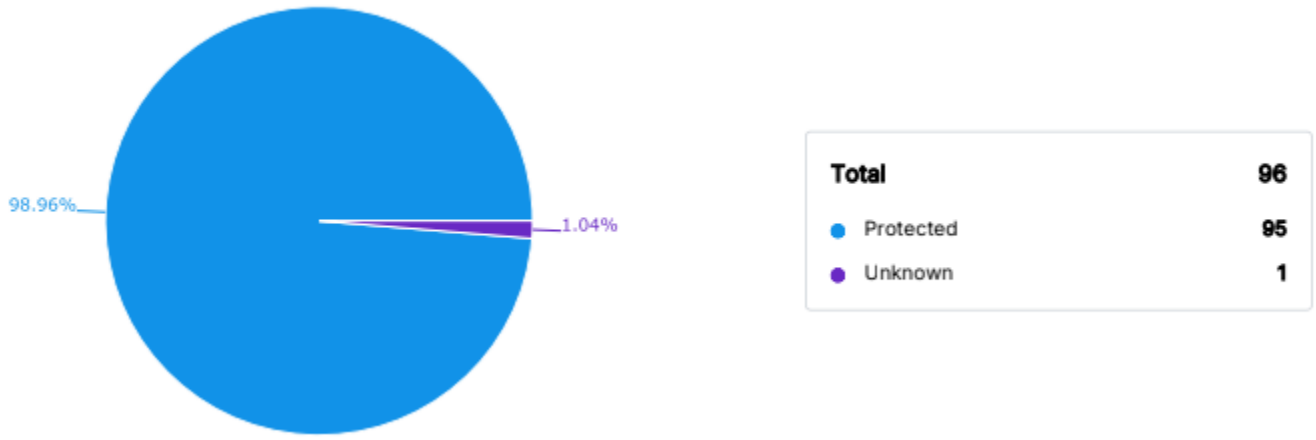
Verificar que las políticas en el manejo de Ciberseguridad en la Sociedad Hotelera Tequendama se socializan en el nivel administrativo, se realizó el análisis del informe de seguridad del sistema WatchGuard EPDR respecto a posibles riesgos que vulneren la integridad de la información en los equipos de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

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

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, para lo cual 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 95 equipos de cómputo identificados con protección activa y 1 equipo desconocido también protegido.



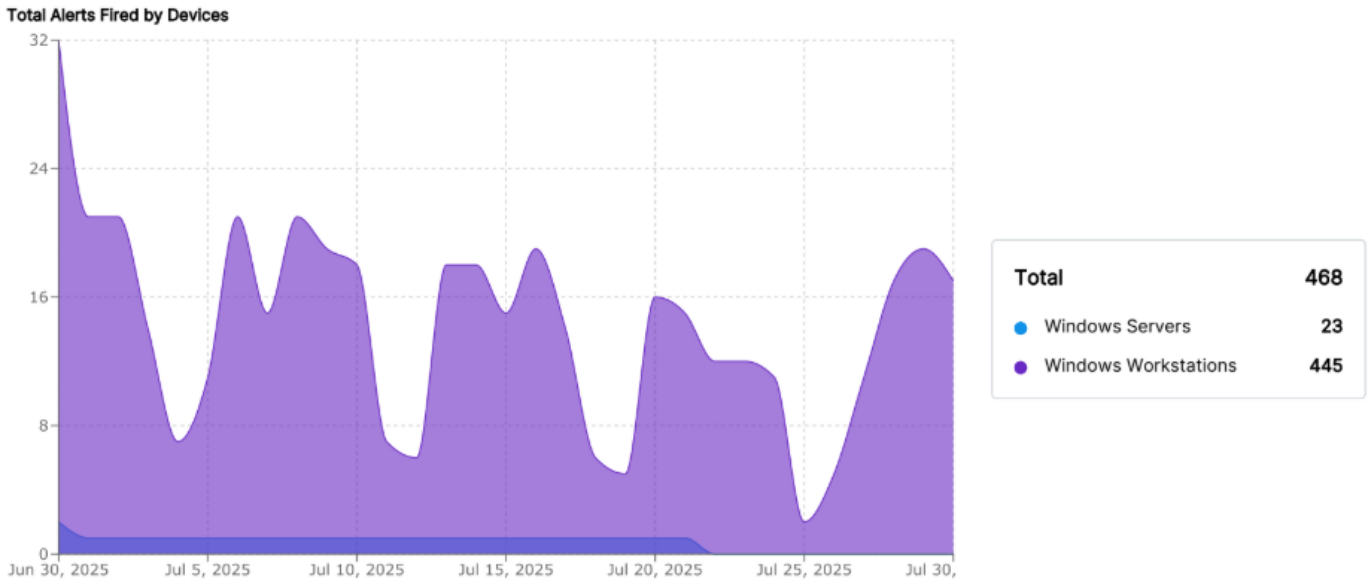
Sin embargo, dentro del periodo auditado se evidencio que se presentaron alertas de posibles ataques a la información de la SHT, así mismo, se resaltan en el informe, cuales son aquellos dispositivos que presentan mayor cantidad de alertas que pueden afectar a la ciberseguridad de la SHT.

No.	DISPOSITIVO	CANTIDAD DE ALERTAS.	ÁREA.
1	YPT3	32	DIRECCIÓN FINANCIERA
2	8SJ1	27	SOLUCIONES TEQUENDAMA
3	M5M3	23	ING. SUBACUÁTICA
4	UNIDAD TIC´S	23	DIRECCIÓN TIC´S
5	8ZPB	22	SOLUCIONES TEQUENDAMA

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

6	SCP2	22	DIRECCIÓN FINANCIERA
7	SK1C	20	OFI. PLANEACIÓN ESTRATÉGICA
8	YPT3	18	DIRECCIÓN FINANCIERA - ACTIVOS FIJOS
9	SM2C	18	SECRETARÍA GENERAL
10	YPT3	17	DIRECCIÓN FINANCIERA.

Respecto al total de alertas registradas en el periodo del 30 de junio al 30 de julio, se presentó un total de 468 alertas correspondientes a 23 alertas generadas desde el servidor y 445 desde los equipos de cómputo de los distintas áreas de la SHT, contando con el pico más altos el 30 de junio con 32 alertas y manteniendo un comportamiento y el más bajo el 25 de julio de 2025.



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.

RECOMENDACIONES

La Oficina de Control Interno recomienda a la Administración:

1. Se recomienda realizar jornadas periódicas de depuración y actualización del software en los equipos de cómputo de la SHT 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 de equipos de cómputo de la SHT 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: MONICA TORRES

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