

2025-130-001467-3

Bogotá, , 17 de diciembre 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
NOVIEMBRE 2025**

INTRODUCCIÓN

Conforme a las funciones señaladas en la Ley 87 de 1993, Decretos reglamentarios y Plan Avante III 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

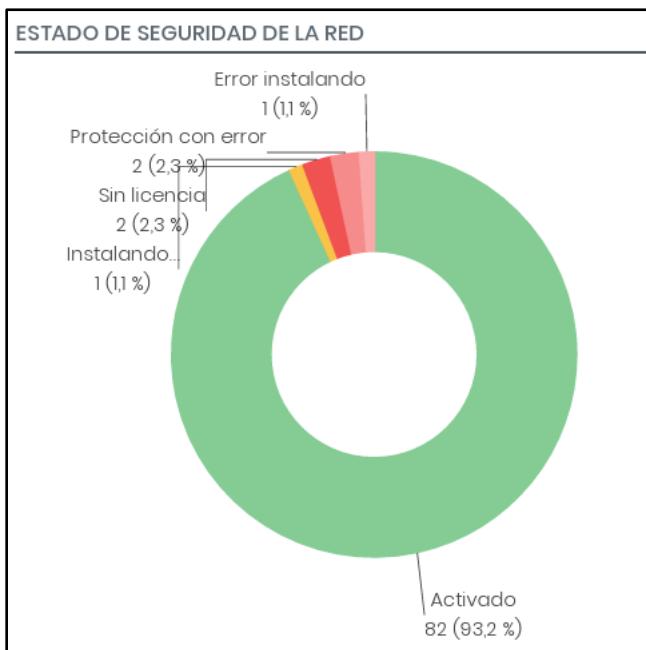
Verificar que las políticas en el manejo de Ciberseguridad en la Sociedad Hotelera Tequendama se socializan en el nivel administrativo. Se realizó el análisis del informe de seguridad del sistema WatchGuard EPDR

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 88 equipos de cómputo identificados de los cuales 82 se encuentran protegidos, 2 equipos con protección con error, 2 equipos sin licencia, 1 equipo que presenta error de instalación y 1 equipo en instalación.



- Amenazas Detectadas por antivirus.

Para el periodo auditado, no se registraron actividades de malware y pups.

- Phishing Detectados.

En el periodo evaluado, se registró un total de 2 detecciones de sitios phishing, sin embargo, no se materializó un riesgo que comprometa la seguridad de la información.

- URLs con malware

En el periodo auditado, se detectaron un total de 132 direcciones de pagina web con algún software malicioso, impidiéndose la materialización de un riesgo a la integridad de la información de la SHT.

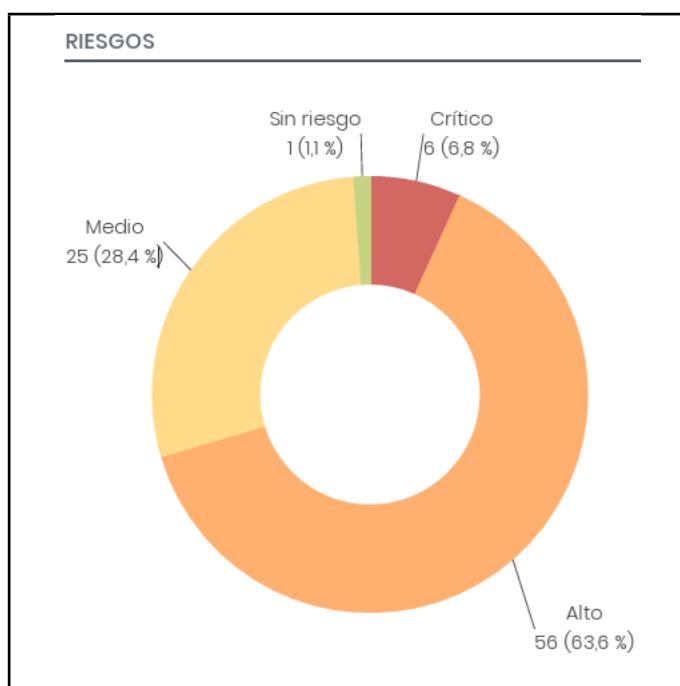


- **Intentos de Intrusión Bloqueados.**

Adicionalmente, se bloquearon un total de 779.133 intentos de intrusión a los equipos de la SHT. Se evidencia que los sistemas de protección de la información dentro del periodo auditado, no permitió el ingreso irregular a la información de la compañía y que por ende se recomienda continuar con las buenas prácticas de bloqueo de páginas web que representen un riesgo en la seguridad de la información, como también correos electrónicos y dispositivos electrónicos.

- **Equipos en Riesgo.**

En el periodo auditado se evidenció que existen 87 equipos con riesgos identificados, equivalente al 98,86% de los equipos en funcionamiento por parte de la SHT. De los cuales 56 equipos tienen riesgo alto, 25 riesgo medio, 6 en riesgo crítico y 1 equipo sin riesgo.





- Top 8 equipos en riesgo.

En atención a la totalidad de los equipos que presentaron riesgo en el periodo auditado, es importante mencionar aquellos equipos los cuales deben realizarse las acciones preventivas y correctivas pertinentes para minimizar la presencia de dichos riesgos para evitar su materialización. A continuación, se mencionan los ocho (8) equipos con mayor calificación de riesgo referentes a ciberseguridad e integridad de la información.

Equipo.	Área SHT.
YPT3	Dirección Financiera.
PVC3	Dirección Financiera.
8SHP	Dirección Financiera.
2RH2	UEN Soluciones Tequendama.
5QHL	Dirección de TIC'S
SLGC	VP. Negocios Turísticos y Gastronómicos
CYPT3	Presidencia SHT.
SHTC	Dirección de Comunicaciones y Marca

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. Asimismo, 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 reitera la recomendación 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 para prevenir y subsanar las posibles brechas en materia de ciberseguridad que pongan en riesgo la integridad de la información corporativa.
4. Se recomienda a la dirección de TIC's revisar con el proveedor Sciotec el componente de Equipos en Riesgo, debido a que no se puede identificar con base en la totalidad de los equipos de la SHT la cantidad exacta de equipos que manifiestan algún tipo de riesgo alto, medio y crítico
5. Se recomienda identificar e implementar acciones para el fomento de la prevención debido al volumen de intentos de intrusión reportados para el mes de noviembre, siendo que es un numero considerable de intentos que pueden comprometer la seguridad cibernetica 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