

SHT. 202402000006563

COMUNICACION INTERNA

FECHA: 31 mayo 2024

PARA: COMITÉ DE COORDINACIÓN DE CONTROL INTERNO

DE: HENRY MOLANO VIVAS
JEFE OFICINA DE CONTROL INTERNO

ASUNTO: INFORME DE SEGUIMIENTO CUMPLIMIENTO POLITICAS CIBERSEGURIDAD MAYO 2024

INTRODUCCIÓN

Conforme a las funciones señaladas en la Ley 87 de 1993, Decretos reglamentarios y Plan Avante II de la Sociedad Tequendama; esta Oficina en su rol de evaluación y seguimiento al Sistema de Control Interno de la Entidad, acorde al plan de auditoria anual en la vigencia 2024 el cual fue aprobado por el Comité de Coordinación de acuerdo a la resolución interna 20230613000075 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 Tequendama, se realizó visita presencial a la UEN Operación Logística. La anterior actividad está enmarcada dentro de la Dimensión de control Interno del Modelo Integrado de Planeación y Gestión MIPG (3 línea de defensa).

Posteriormente se realizó una encuesta referente al conocimiento sobre "Ciberseguridad Corporativa" a los funcionarios de la ST.

4



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 Tequendama S.A.

ALCANCE

Verificar que las políticas en el manejo de Ciberseguridad en la Sociedad Tequendama. Se utilizaron métodos de entrevista y diligenciamiento de encuesta.

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 Tequendama. Se tomo una muestra aleatoria de 6 funcionarios del Departamento desarrollo Humano y Contratación y compras evidenciando que poseen conocimiento básico y desconocen algunos términos frente al tema en referencia.

CUESTIONARIO DE AUTOCONTROL DE SEGUIMIENTO DE RIESGOS DE CIBERSEGURIDAD					
ITEM	RESPONSABILIDAD CIBERSEGURIDAD CON LA SOCIEDAD	SI	NO	ALGUNAS VECES	RESPUESTA
1	¿Tiene o ha tenido acceso a software de la Sociedad sin autorización?		6		
2	¿Presta o ha prestado las claves o usa las claves de los demás?	1	5		
3	¿Utiliza correo personal en los equipos de la Sociedad?	1	5		
4	¿Baja información con remitente desconocidos en lo equipos de la sociedad?	1	5		
5	¿Utiliza los puesto USB? En caso de que sea usada que medidas de mitigación realiza	1	5		SE PASA POR ANTIVIRUS
6	¿Conoce de temas de ciberseguridad y como aporta para blindar la Sociedad de ataques?	5	1		
7	¿Que conoce de Ataques de phishing?	4	2		
8	¿Que conoce de Ataques de Ransomware?	2	4		
9	¿Que conoce de Malware?	1	5		
10	¿Que conoce de Spam o correo no deseado?	6			
11	¿Que conoce de ATAQUES A LA NUBE?	4	2		
12	¿Diligencio el acta de compromiso de ciberseguridad? (evidencia de envió)	5	1		
13	¿Qué tipo de páginas WEB consulta en los equipos de la Sociedad?				Referentes al cargo

14	¿Cuándo llega un correo sospechoso sabe qué hacer?	6			Eliminarlo y avisar a tics
15	Donde almacena la información que produce (nube, drive, correo, etc) y que backup efectúa				PC, Drive, correo Nube, backup

De acuerdo a la muestra tomada de los funcionarios que realizaron la encuesta, el auditor denoto que aún existen desafíos significativos para actuar con prontitud para fortalecer la mitigación de riesgos, y desde el autocontrol tener conciencia a este tema en los equipos de alto rendimiento de la ST.

Estos desafíos comprometen la seguridad de los sistemas y datos de las empresas. Para abordarlos, es esencial trabajen de la mano en campañas de sensibilización, formación en ciberseguridad, investigación, desarrollo de tecnologías, y regulaciones más robustas son algunas de las medidas necesarias.

RECOMENDACIONES

La Oficina de Control Interno recomienda a la Administración:

1. Capacitar al personal en concientización en seguridad de información.
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 ST.
3. Se recomienda al equipo de ciberseguridad la creación de matrices de riesgos y los respectivos planes de contingencia. †

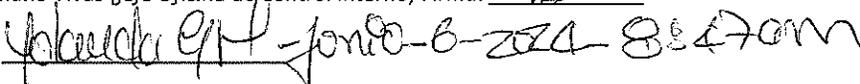
Cordialmente,



HENRY MOLANO VIVAS
Jefe Oficina de Control Interno

Elaboró: Andrea del Pilar Cogua Páez (Auditor) Firma: 

Revisó y aprobó. Henry Molano Vivas (jefe Oficina de Control Interno) Firma: 

Recibió: Gerencia General  - junio - 6 - 2021 8:54 AM