CUESTIONES INTERNAS Y EXTERNAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA ETITC (DOFA)

INTRODUCCION

La Escuela Tecnológica Instituto Técnico Central, mediante el presente documento, pretende comunicar el resultado del ejercicio de identificación de las cuestiones internas y externas que son pertinentes al Modelo de Seguridad y Privacidad de la Información de Gobierno Digital y al Sistema de Gestión de Seguridad de la Información, favoreciendo con esto, las tareas relacionadas con idear estrategias que permitan eliminar cualquier aspecto que ponga en riesgo la capacidad de lograr los resultados previstos, dando cumplimiento a los requisitos normativos al numeral 4.1 Conocimiento de la Organización y de su Contexto, de la norma NTC ISO/IEC 27001:2022.

CUESTIONES INTERNAS (Factores Internos)	
8 Fortalezas	**18 Debilidades**
F1 - Implementación al 100% del Modelo de Seguridad y Privacidad de la Información de Gobierno Digital.	D2 - Falta de gestión de cambios a la infraestructura tecnológica
F2 - Infraestructura tecnológica sólida y de alto nivel.	D3 - Falta de software especializado que permitan hacer seguimiento de análisis de vulnerabilidades, realizar pruebas de penetración, auditoría de redes y a sistemas de información.
F3 - La ETITC cuenta con un proceso de Gestión de Seguridad de la Información a cargo de Rectoría y Subordinado a la Oficina Asesora de Planeación.	D4 - Falta de mantenimiento a la Infraestructura Crítica y Física: Cableado Estructurado, Racks, Aires Acondicionados, Sistemas de Extinción de Incendios, Sistema de Alerta Sísmica, UPS y Plantas eléctricas y Sistema de Protección contra descargas Eléctricas Atmosféricas
F4 - El proceso Gestión de Seguridad de la Información se encuentra constituido, en el Sistema de Aseguramiento de Calidad.	D5 - Falta de conocimientos del personal de Gestión de Informática y Comunicaciones que aporta a la implementación de controles técnicos de Seguridad de la Información.
F5 - Alto nivel cultural en temas de seguridad de la información en el recurso humano de la ETITC, gracias a la implementación del Plan de Sensibilización y Entrenamiento del SGSI para la vigencia 2024.	D6 - Existencia de infraestructura tecnológica sin apoyo y/o custodia del proceso de informática y comunicaciones.
F6 - Manual de Políticas de Seguridad y Privacidad de la Información, adoptado mediante Resolución No. 449 del 24 de octubre de 2017.	D8 - Desconocimiento por parte de los servidores públicos y contratistas en las técnicas de Ingeniería social (spam, phishing, fakemailing, entre otros.)
F7 - Procedimientos de seguridad de la información, controlados en el	D10 - Falta de lineamientos para la asignación de roles y

Sistema de Aseguramiento de Calidad y socializados al interior de la Escuela.	responsabilidades para gestión de usuarios en los sistemas de información
F8 - Ingreso de las Bases de Datos al RNBD, de la Superintendencia de Industria y Comercio, para cumplir con lo establecido en la Ley 1581 de 2012.	D11 - Falta de apropiación de los procesos, procedimientos y uso de los sistemas de información de la Escuela por parte de los servidores públicos y contratistas.
	D12 - Falta de respaldo de personas para el desarrollo de actividades críticas en los casos que se presente incapacidades, vacaciones, muerte, licencias, entre otros.
	D13 - Notificación inoportuna de novedades de usuario de servidores públicos y contratistas (Retiro, vacaciones, muerte, licencias, terminación de contrato, cesión de contrato, rotación de dependencias) al área de Informática y Comunicaciones.
	D14 - Ausencia y/o desactualización del Plan de Contingencia, Planes de Recuperación de Desastres (DRP), Objetivo de punto de recuperación (RPO) y de objetivo de tiempo de recuperación (RTO) y Retorno a la normalidad.
	D15 - Manejo inadecuado de contraseñas.
	D16 - Falta de presupuesto para la renovación de la infraestructura tecnológica, lo que genera contar con infraestructura obsoleta e incompatibilidad con nuevas tecnologías.
	D17 - Incumplimiento de políticas de seguridad de la información por autorización de uso de whatsaap web a funcionarios.
	D18 - Falta de familiaridad normativa de ISO 27001:2022 de la

	comunidad educativa con los nuevos requisitos y cambios en la estructura de la norma.
	D19 - Falta de adaptación de procesos y gestión de cambios para cumplir con los nuevos requisitos y enfoques de la norma.
	D20 - Falta de documentación relacionada con el sistema de gestión de seguridad de la información, ciberseguridad y protección de la privacidad de datos personales y continuidad del servicio para reflejar los cambios introducidos por la nueva versión.
	D21 - Falta de coordinación con las partes interesadas para asegurar la alineación durante el proceso de transición de ISO 27001:2022.

CUESTIONES ENTERNAS (Factores Externos)	
10 Amenazas	**4 Oportunidades**
A1 - Cambios frecuentes en la estructura del Modelo de Seguridad y Privacidad de la Información de Gobierno Digital.	O1 - Reconocimiento, por parte de los entes de control, a la ETITC, por los resultados satisfactorios obtenidos, en el cumplimiento de los requisitos de seguridad de la información de Gobierno Digital.
A2 - Aumento de los niveles del crimen organizado a través de internet.	O2 - Creciente necesidad de implementar el Modelos de Seguridad y Privacidad de la Información de Gobierno Digital; y el Sistema de Gestión de Seguridad de la Información, en las Instituciones de Educación Superior, a nivel Nacional.
A3 - Incremento en la presencia de ataques de ramsonware de alto perfil en Colombia.	O3 - Asesoría y entrenamiento al personal que custodia la Seguridad de la Información en temas especializados de ciberseguridad y actualización de nuevos controles del anexo A de la norma ISO 27001.
A4 - Incremento en la fabricación y diseminación de virus en el internet.	O4 - Adquisición de herramientas especializadas para la investigación técnica, análisis de vulnerabilidades, gestión de incidentes, gestión integral del riesgo de ciberseguridad y riesgo operacional y simulacros ante un ataque cibernético.
A5 - Falta de asesoría, por parte de los entes de control, para la implementación de los lineamientos de seguridad de la información, en temas relacionados a Gobierno Digital.	
A6 - Desastre natural como inundación, incendio, terremoto, sismos, falla eléctrica interna y	

externa, así como manifestaciones e incluso ataques terroristas.	
A7 - Los proveedores de los sistemas operativos, canal de internet, no son compatibles con la infraestructura tecnológica de la Escuela.	
A8 - Ataques informáticos a infraestructura tecnológica debido a puertos de comunicación TCP/UDP no autorizados en estado abierto (sin filtrar).	
A9 - Falta de respuesta ante una interrupción en la prestación del servicio de proveedores hacia la ETITC.	
A10 - Incumplimiento legal a los requisitos y normatividad de ISO 27001:2022 por cambios de la estructura de la norma.	

Cordialmente,

Esp. Sandra J. Guerrero G.
Líder del Sistema de Gestión de Seguridad de la Información