INFORME DE AUDITORÍA TÉCNICA INTERNA A IMPLEMENTACIÓN DE CONTROLES ASOCIADOS A LA NORMA ISO 27001:2013

1. OBJETIVO

El Instrumento de Evaluación del MSPI busca identificar el nivel de madurez en que se encuentra la entidad frente a la implementación del Modelo de Seguridad y Privacidad de la Información, de igual manera permite establecer el estado de gestión y de adopción de los controles técnicos y administrativos al interior de la Alcaldía de Bucaramanga.

2. ALCANCE

El autodiagnóstico del MSPI es aplicable a los activos de información pertenecientes a los diferentes procesos y los recursos tecnológicos de la entidad.

3. METODOLOGÍA

Levantamiento de Información

- Solicitud de Información
- Consolidación de Información

Validación de Evidencias

- Revisión de la Documentación
- Entrevistas con las partes interesadas
- Análisis frente a mejores prácticas

Informes y Recomendaciones

- Identificación de la brecha en seguridad
- Recomendaciones frente a las debilidades encontradas
- Definición del Plan de Seguridad

4. DESARROLLO Y RESULTADOS

Dentro de la herramienta de autodiagnóstico se desarrollaron los siguientes componentes con el fin de identificar la brecha en seguridad frente a los requisitos definidos en el Modelo de Seguridad y Privacidad de la Información:

- **ISO 27001:2013 Anexo A** En este componente se mide el grado de implementación y adopción de cada uno de los dominios y sus objetivos de control definidos en el mencionado anexo. Dentro de este escenario se busca medir la efectividad de los controles, establecer las responsabilidades para ejecutarlos y gestionar la implementación de acciones correctivas.

- **Avance de Implementación del ciclo PHVA** Este componente busca identificar el nivel de formalización y de Gestión del Modelo de Seguridad y Privacidad de la Información, el cual considera su operación basada en un ciclo PHVA (Planear, Hacer, Verificar y Actuar) así como lo requisitos reglamentarios y de funcionamiento buscando gestionar adecuadamente los activos de información de la entidad.

- **Nivel de Madurez** En este componente se indica el nivel de implementación del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.

- **CIBER** Dentro de este componente se pretende determinar la calificación frente a las mejores prácticas en Ciberseguridad basadas en el marco de trabajo del NIST, las cuales apoyan la gestión del riesgo de ciberseguridad a través de 5 funciones simultaneas y continuas con el propósito de Identificar, Proteger, Detectar, Responder y Recuperar, proporcionando una visión de alto nivel del ciclo de vida de la administración de los riesgos de ciberseguridad dentro de la entidad.

5. EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO

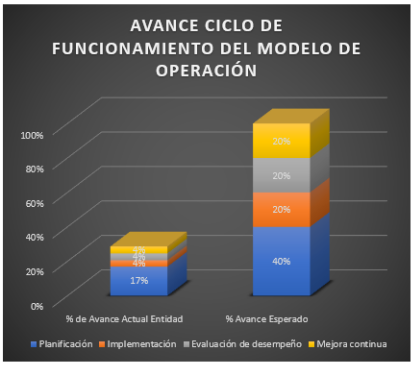
Evaluación de Efectividad de controles

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	32	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	34	100	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	20	100	INICIAL
A.9	CONTROL DE ACCESO	38	100	REPETIBLE
A.10	CRIPTOGRAFÍA	10	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	33	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	29	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	42	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	40	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	20	100	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	30	100	REPETIBLE
A.18	CUMPLIMIENTO	46,5	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		34	100	REPETIBLE

Brecha Anexo A ISO 27001:2013

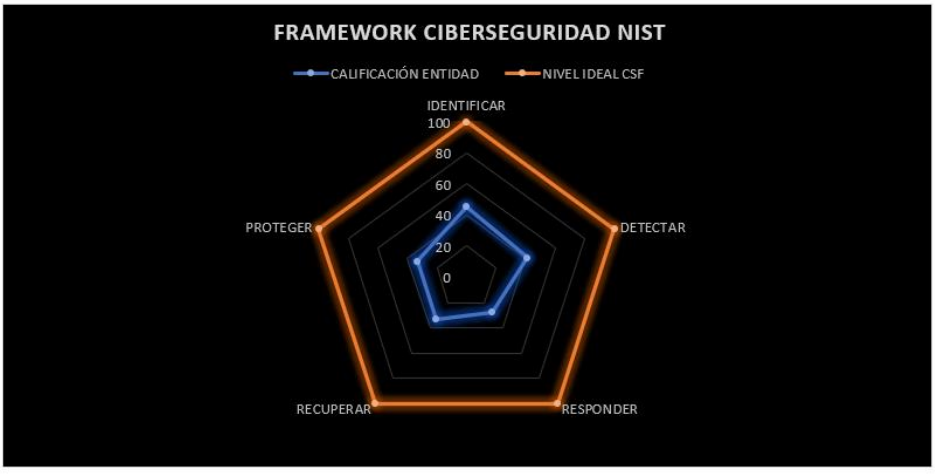
6. AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2022	Planificación	17%	40%
	Implementación	4%	20%
	Evaluación de desempeño	4%	20%
	Mejora continua	4%	20%
TOTAL	TOTAL	29%	100%



7. CALIFICACIÓN FRENTE A MEJORES PRÁCTICAS EN CIBERSEGURIDAD (NIST)

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	45	100
DETECTAR	41	100
RESPONDER	28	100
RECUPERAR	33	100
PROTEGER	33	100



8. CONCLUSIONES

- Según los resultados obtenidos se evidencia que la entidad cuenta con un nivel de calificación Bajo, lo que en la escala de evaluación equivale a un nivel repetible, el cual establece que frente a la implementación de los controles asociados al anexo A de la Norma ISO 27001:2013, los controles se han desarrollado en diferentes procesos y son seguidos por deferentes actores pero no existe una formalización ni comunicación adecuada sobre los estándares y procedimientos de seguridad de la información.

- Los dominios que registran un menor nivel de implementación son los relacionados con la Gestión de activos, Criptografía, Seguridad de las Operaciones, Relación con Proveedores y Gestión de Incidentes de Seguridad de la Información, los cuales registran un nivel de calificación por debajo del 30% y se deberían priorizar con el fin de disminuir la brecha de seguridad frente a estos requisitos.

- Frente a las fases de operación del ciclo PHVA, se puede evidenciar que todas las fases contemplan un nivel inicial de avance en su implementación al no contar con los requerimientos técnicos, normativos, reglamentarios y de funcionamiento que son necesarios para cumplir con los objetivos estratégicos del Modelo de Seguridad y Privacidad de la Información.

GABRIEL FERNANDO ANAYA BLANCO
CPS – Proceso de Gestión de las TIC.

Apoyo técnico :
Elkin Alfredo Albarracin Navas – CPS Proceso de Gestión de las TIC