Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Instructivo No. 1

MINTIC vive digital Colombia TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0	9/06/2017	Versión inicial del documento

TABLA DE CONTENIDO

1. DERECHOS DE AUTOR

2. AUDIENCIA

Este documento está elaborado para las entidades públicas de orden nacional, entidades públicas del orden territorial, que están en proceso de realizar el diligenciamiento de la herramienta de diagnóstico del Modelo de Seguridad de la Información, así como proveedores de servicios de Gobierno en Línea y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la Información en el marco del Programa Gobierno en Línea.

3. INTRODUCCIÓN

El modelo de Seguridad y Privacidad de la Información cuyo propósito es servir como guía para la mejora de los estándares de Seguridad de la Información de las Entidades, cuenta con 5 fases para la gestión de la Seguridad y Privacidad de la información de las Entidades.

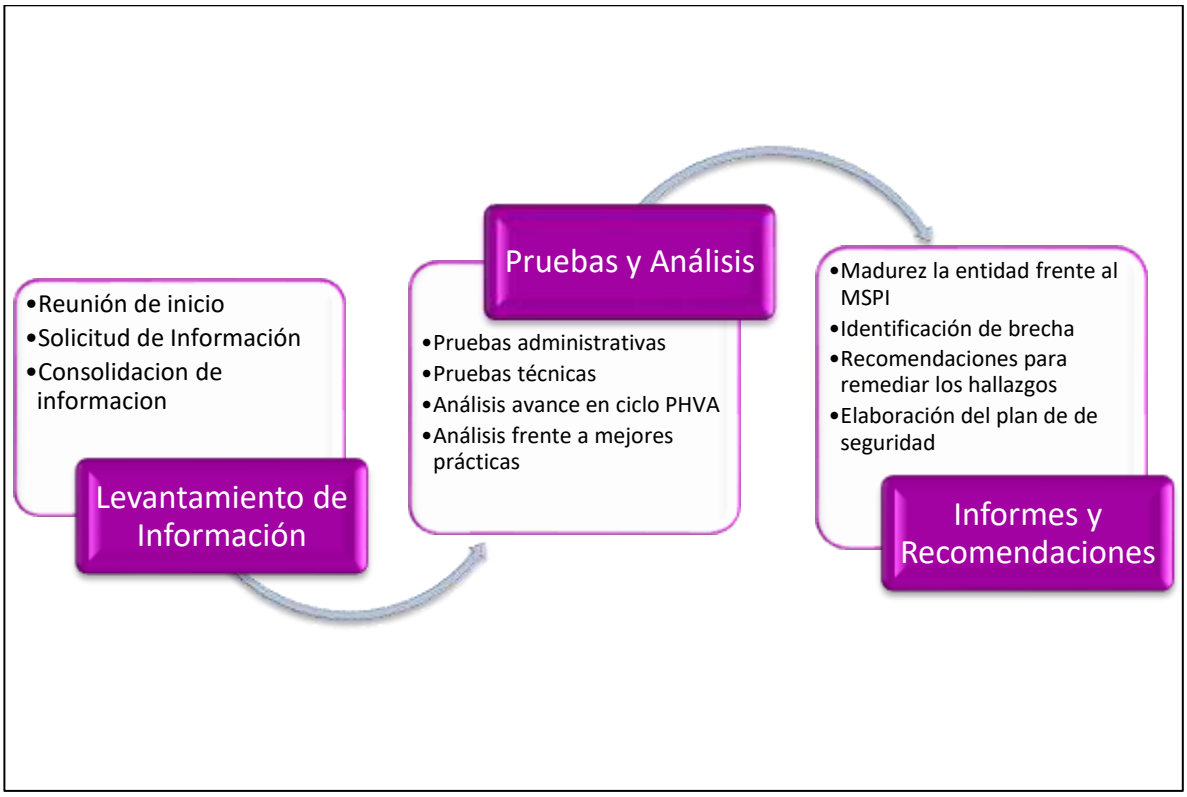
Este documento les permite a las entidades públicas de orden nacional, y entidades públicas del orden territorial, entender de una mejor manera como se debe diligenciar la herramienta de diagnóstico para poder obtener un resultado preciso, el cual le permite a cada entidad generar un plan de seguridad de la información para ser desarrollado al interior de esta, y de esta manera dar cumplimiento con lo estipulado en el manual de gobierno en línea en su cuarto componente.

4. PROPÓSITO

El propósito de este documento es ofrecer un instructivo de orientación para el diligenciamiento de la herramienta de diagnóstico.

5. DESARROLLO DE LA METODOLOGÍA DE AUTODIAGNOSTICO

En la siguiente gráfica se muestran las fases para la ejecución de la evaluación en cada una de las entidades:



Gráfica 1 - Fases de Desarrollo

A continuación de detalla cada una de las hojas que contiene la herramienta de diagnóstico:

5.1. HOJA 1 -> PORTADA:

A continuación, se muestran y explican los componentes de la hoja portada:

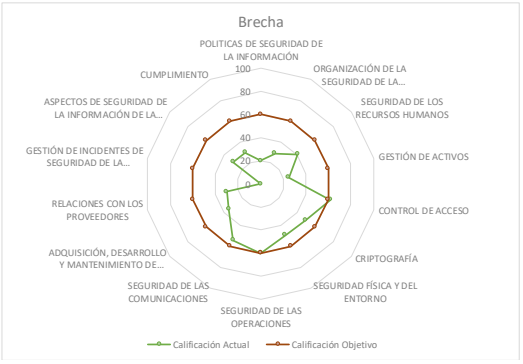
Gráfica 2 - Encabezado, hoja Portada

Encabezado: En el encabezado se debe diligenciar:

- **Entidad evaluada:** Aquí se diligencia el nombre de la entidad a revisar el cual se replicará en los encabezados de las demás hojas del instrumento automáticamente.
- **Fechas de Evaluación:** En este campo se coloca el rango de fechas en el que inicia y finaliza la evaluación en formato dd/mm/aaaa – dd/mm/aaaa.
- **Contacto:** Datos del contacto que nos atiende en la entidad evaluada, como el nombre, cargo, teléfono y correo electrónico.
- **Elaborado por:** Nombre de la persona que ejecuta la evaluación.

BRECHA ANEXO A ISO 27001:2013

No.	PUNTAJE - DOMINIO		
	DOMINIO	Calificación Actual	Calificación Objetivo
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	60
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	29	60
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	41	60
A.8	GESTIÓN DE ACTIVOS	25	60
A.9	CONTROL DE ACCESO	62	60
A.10	CRIPTOGRAFÍA	50	60
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	49	60
A.12	SEGURIDAD DE LAS OPERACIONES	60	60
A.13	SEGURIDAD DE LAS COMUNICACIONES	54	60
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	35	60
A.15	RELACIONES CON LOS PROVEEDORES	30	60
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	60
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	30	60
A.18	CUMPLIMIENTO	30	60
PROMEDIO		***36,79***	***60***



Gráfica 3 - Análisis de brecha frente a la guía de controles MSPI e ISO 27002

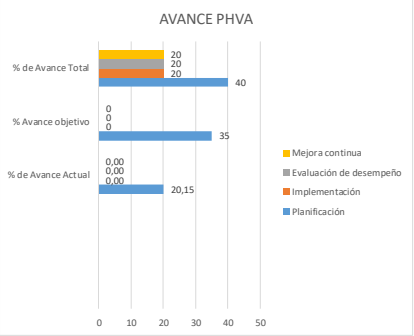
Brecha Anexo A ISO 27001:2013: En este componente se muestra el resultado del análisis de brecha frente a los controles del Anexo A, del estándar ISO 27001:2013, y la guía de controles (Guía #8) del Modelo de Seguridad de Privacidad de la Información el cuadro de resumen y la gráfica se construyen automáticamente en la medida que se diligencia el Instrumento. Aquí se puede evidenciar la calificación de cada dominio frente a la escala de evaluación definida y también en comparación con la calificación objetivo correspondiente a cada año estipulada en el Manual de Gobierno en Línea así:

TIPO DE ENTIDAD	2015	2016	2017	2018	2019	2020
De Orden Nacional	40%	60%	80%	100%	Mantener 100%	Mantener 100%
De Orden Territorial A	35%	50%	80%	100%	Mantener 100%	Mantener 100%
De Orden Territorial B y C	10%	30%	50%	65%	80%	100%

Gráfica 4 - Avance PHVA

AVANCE PHVA

No.	AVANCE PHVA			
	COMPONENTE	% de Avance Actual	% Avance objetivo	% de Avance Total
1	Planificación	20,15	35	40
2	Implementación	0,00	0	20
3	Evaluación de desempeño	0,00	0	20
4	Mejora continua	0,00	0	20
TOTAL			100	



Gráfica 5 - Avance PHVA

Avance PHVA: Este componente de la hoja consta de una tabla y una gráfica, permite evidenciar el avance en el ciclo del modelo de seguridad definido en el documento MSPI, el cual está alineado con los plazos para la implementación de las actividades que se establecieron para el Manual de Gobierno en Línea, y a través del Decreto 1078 de 2015, en el Titulo 9, Capitulo 1, Sección 3.

La tabla muestra el estado de avance (columna % de avance actual) frente a cada una de las etapas del ciclo (columna componente), es importante tener en cuenta que de acuerdo al tipo de entidad hay diferentes objetivos (columna % avance objetivo) de avance, así:

TIPO DE ENTIDAD	2015	2016	2017	2018	2019	2020
De Orden Nacional	40%	60%	80%	100%	Mantener 100%	Mantener 100%
De Orden Territorial A	35%	50%	80%	100%	Mantener 100%	Mantener 100%
De Orden Territorial B y C	10%	30%	50%	65%	80%	100%

Gráfica 6 - Plazos para alcanzar avances en el PHVA[1]

La columna avance total es el máximo avance posible a lograr.

El tipo de entidad se diligencia en la hoja levantamiento de información, este dato permite que se calcule de manera automática el avance objetivo de acuerdo a lo presentado en la gráfica 6.

La gráfica presenta una comparación entre el avance logrado por la entidad, el avance objetivo y el avance total posible.

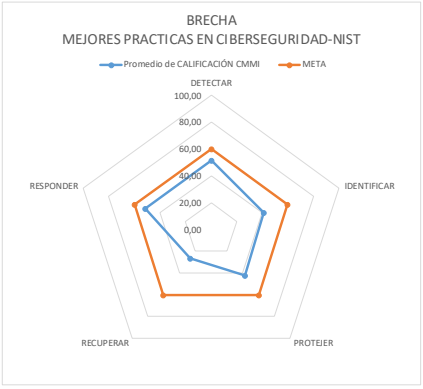
[1] Tomado de las páginas 26-29 del documento Modelo de Seguridad y Privacidad de la Información MSPI, de Mintic.

Gráfica 7 - Nivel de madurez

Nivel de Madurez: Este componente indica el nivel de madurez en el que se encuentra la entidad evaluada con respecto al Modelo de Seguridad y Privacidad de la Información.

CALIFICACIÓN FRENTE A MEJORES PRÁCTICAS EN CIBERSEGURIDAD (NIST)

FUNCION CIBERSEGURIDAD	edio de CALIFICACIÓN	META
DETECTAR	51,25	60
IDENTIFICAR	41,00	60
PROTEJER	42,54	60
RECUPERAR	26,67	60
RESPONDER	51,11	60
Total general	**43,60**	



Gráfica 8 - Calificación frente a mejores prácticas

Calificación Frente a Mejores Prácticas: En este componente se muestra una tabla con los resultados de comparar la calificación de acuerdo a la escala de evaluación de los controles existentes en la entidad frente a la mejor práctica en Ciberseguridad definida por NIST[2]. La grafica muestra la brecha entre la calificación alcanzada y la calificación objetivo, correspondiente a estipulado en la gráfica No.5 y 6.

[2] National Institute of Standards and Technology

5.2. HOJA 2 -> ESCALA DE EVALUACIÓN:

Esta hoja no se diligencia y es el punto de referencia para calificar los controles de las hojas administrativas, técnicas, PHVA, ciberseguridad.

Tabla de Escala Nivel de Cumplimiento ISO 27001 ANEXO A		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Definido	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Gráfica 9 – Hoja escala de evaluación

5.3. HOJA 3 -> LEVANTAMIENTO DE INFORMACIÓN:

A continuación, se muestran y explican los componentes de la hoja de Levantamiento de Información:

DATOS BASICOS	
Tipo Entidad	De orden territorial B o C
Mision	
Analisis de Contexto	<PEGAR DOCUMENTO COMO ARCHIVO EMBEBIDO>
Mapa de Procesos	<PEGAR DOCUMENTO COMO ARCHIVO EMBEBIDO>
Organigrama	<PEGAR DOCUMENTO COMO ARCHIVO EMBEBIDO>

Gráfica 10 - Datos Básicos

Datos básicos: En este componente se deben diligenciar o adjuntar los datos básicos de conocimiento de la entidad, como:

- **El tipo de entidad,** es decir si es de orden nacional, territorial A,B o C, este campo es de tipo selección y debe ser diligenciado para determinar el porcentaje de avance objetivo en el ciclo PHVA
- **El análisis de contexto**[3] que es un documento exigido por la ISO 27001 y hace referencia a determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el SGSI.
- **Mapa de procesos de la entidad**
- **Organigrama de la entidad**

PREGUNTAS	
Que le preocupa a la Entidad en temas de seguridad de la información?	
En que nivel de madurez considera que está?	
En que componente del ciclo considera que va?	

Gráfica 11 - Preguntas de levantamiento de información

Preguntas: Este componente se debe diligenciar para conocer mejor de la entidad y permitirá orientar las recomendaciones hacia sus necesidades.

3 La ISO 27001 hace referencia a la norma ISO 31000:2009 en el apartado 5.3.

NO.	DATOS E INFORMACIÓN A RECOLECTAR PARA LA EVALUACIÓN **Lista de información BASICA a solicitar**	NOMBRE DEL DOCUMENTO	OBSERVACIONES
1	Tipo de entidad (Nacional, Territorial A, Territorial B o C)	Doc-01	
2	Misión	Doc-02	
3	Análisis de contexto: La entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad	Doc-03	
4	Mapa de Procesos		
5	Procesos seleccionados para el análisis indicando cual es crítico	Doc-05	
6	Inventario de dispositivos para las pruebas técnicas que contenga nombre, descripción, proceso(s) al que pertenece, ip, si es ip externa o interna	Doc-06	
7	Organigrama de la entidad, detallando el área de seguridad de la información o quien haga sus veces	Doc-07	
8	Políticas de seguridad de la información formalizada y firmada	Doc-08	
9	Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades.		

Gráfica 12 - Lista de Información a solicitar

Lista de información a solicitar: Esta es la misma información que fue solicitada a las entidades a través del Anexo 2, aquí se transfiere la información diligenciada por la entidad en el nombre del documento entregado y las observaciones si aplica.

5.4. HOJA 4 -> AREAS INVOLUCRADAS:

Esta hoja pretende involucrar en el proceso de autoevaluación el área o responsable, el tema a tratar y el funcionario que debe apoyar en el desarrollo del tema.

RESPONSABLE / AREA	TEMA	FUNCIONARIO
Control interno	Revisiones de seguridad de la información	
	Revisión independiente de la seguridad de la información	
	Cumplimiento con las políticas y normas de seguridad.	
	CUMPLIMIENTO	
	Auditoria Interna Plan	
	Auditoria Interna Ejecución y Subsanación de hallazgos y brechas	
Gestión humana	Selección e investigación de antecedentes	
	Términos y condiciones del empleo	
Líder de Proceso 1	**PROCESO**	
	DESCRIPCIÓN DEL PROCESO	
Líder de Proceso 2	**PROCESO**	
	DESCRIPCIÓN DEL PROCESO	
Líder de Proceso 3	**PROCESO**	
	DESCRIPCIÓN DEL PROCESO	
Responsable de compras y adquisiciones	RELACIONES CON LOS PROVEEDORES	
	Seguridad de la información en las relaciones con los proveedores	
	Gestión de la prestación de servicios de proveedores	

Gráfica 13 – Áreas Involucradas

5.5. HOJA 5 -> PRUEBAS ADMINISTRATIVAS:

A continuación, se muestran y explican los componentes de la hoja de pruebas administrativas:

Estas pruebas están orientadas a los temas de seguridad de la información que no están directamente relacionadas con las áreas tecnológicas de la entidad, y contemplan entre otras cosas la evaluación, implementación, revisión y mejoras de la Política de Seguridad de la Información, la evaluación de la definición de las responsabilidades para la gestión de la seguridad de la información y si están acordes con las necesidades la entidad, la evaluación de la organización de la seguridad de la información, la revisión y evaluación de los acuerdos de confidencialidad, la evaluación de la cooperación con autoridades y grupos de interés y la revisión de la documentación y formalización de procedimientos de la entidad. Estas pruebas incluyen los controles dados en la Norma ISO 27001:2013 de los dominios A5, A6, A7, A8, A17 y A18.

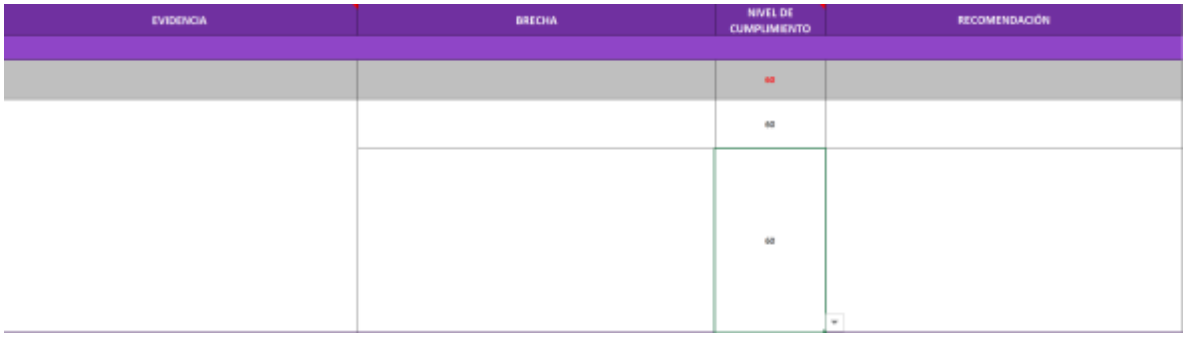
ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MIPI	CIBERSEGURIDAD	PRUEBA
POLITICA DE SEGURIDAD DE LA INFORMACIÓN							
A5.1	Responsable de TI	POLITICAS DE SEGURIDAD DE LA INFORMACION	Dimensión de la dirección para gestión de la seguridad de la información	6.1	Componente planificación y modelo de madurez nivel gestionado		
A5.1.1	Responsable de TI	Documento de la política de seguridad y privacidad de la información	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y a la partes externas pertinentes	A.5.1.1	Componente planificación y modelo de madurez nivel	02.09 b	
A5.1.2	Responsable de TI	Revisión y evaluación	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	A.5.1.2	componente planificación		

Gráfica 14 - Hoja Administrativas, columna 1 a 8

En esta hoja deben diligenciarse las pruebas administrativas a continuación se explican los primeros 8 campos, correspondientes a la gráfica anterior:

- **ID. ítem:** Este campo ya está diligenciado y no debe modificarse, corresponde al identificador del ítem evaluado, para las pruebas administrativas todos los ítems empiezan con la letra A y un consecutivo numérico.
- **Cargo:** Responsable o área que deberá facilitar el acceso a la información y evidencias sobre la definición e implementación del control o requisito a evaluar.
- **Ítem:** Nombre del control o requisito a evaluar.

- **Descripción:** Explicación de lo que se espera del control o requisito, este campo es una orientación para el evaluador y está alineado con lo solicitado en Gobierno en Línea, el MSPI, las mejores prácticas (ISO 27002, NIST).
- **ISO:** Indica el nombre del control del anexo A de la Norma ISO 27001:2013, que se corresponde con el control o con el requisito.
- **MSPI:** Indica que requisito del Modelo de Seguridad definido por el ministerio de las TIC, corresponde con el control o requisito evaluado. Que puede estar relacionado con el ciclo PHVA o el modelo de madurez definido.
- **Ciberseguridad:** Indica que requisito de Ciberseguridad definido por NIST corresponde con el control o requisito evaluado.
- **Prueba:** Este campo es la guía para que el evaluador desarrolle las pruebas y revise el nivel de cumplimiento frente a la Norma ISO 27001:2013 (se han incluido mejores prácticas sugeridas por la ISO 27002:2013), también se incluyen los requisitos de Gobierno en Línea y el MSPI.



Gráfica 15 - Hoja Administrativas columna 9 a 12

A continuación, se explican los campos restantes:

- **Evidencia:** Este campo debe diligenciarse por el evaluador, documentando el resultado de las entrevistas, la fecha de la entrevista y el cargo del entrevistado, y adjuntando cuando aplique (como documento embebido) la evidencia de una prueba o hallazgo. El diligenciamiento debe hacerse a nivel dos (2) de cada Identificador de Ítem, por ejemplo A.1.1, A.2.1, etc. Por lo que se deben combinar las celdas.
- **Brecha:** Este campo debe diligenciarse por el evaluador, indicando que le hace falta al control o requisito para cumplir frente a la Norma ISO 27001:2013, también se incluyen los requisitos de Gobierno en Línea y el MSPI.

- **Nivel de cumplimiento:** Este campo debe diligenciarse por el evaluador, y solo acepta los valores 0, 20, 40, 60, 80 y 100, de acuerdo a la Hoja Escala de Evaluación, que ya fue explicada en el numeral 4.1.1, de este documento. Recomendación: Este campo debe diligenciarse por el evaluador, y debe indicar las actividades o acciones requeridas para solucionar las debilidades, incumplimientos evidenciados durante las pruebas.

5.6. HOJA 6 -> PRUEBAS TÉCNICAS:

A continuación, se muestran y explican los componentes de la hoja de pruebas técnicas:

Evaluación de controles y requisitos: Los controles y requisitos evaluados están asociados los dominios A9, A10, A11, A12, A13, A14 y A16, a los requisitos del MSIP, Gobierno en Línea y mejores prácticas en ciberseguridad.

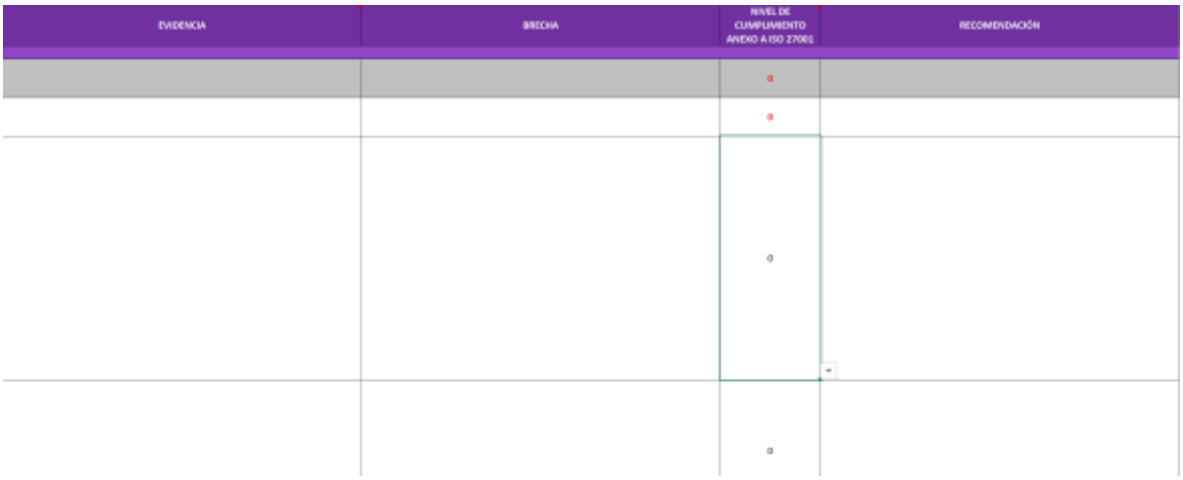
ÍTEM	CARGO	ÍTEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA
CONTROL DE ACCESO							
T.1	Responsable de SI/Responsable de TICs	CONTROL DE ACCESO		A.9	Componente planificación y modelo de madurez nivel gestionado		
T.1.1	Responsable de SI	REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO	Se debe limitar el acceso a información y a instalaciones de procesamiento de información.	A.9.1	Modelo de madurez definido		
T.1.1.1	Responsable de SI	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	A.9.1.1		PR.DS-5	Revisar que la política contenga lo siguiente: a) los requisitos de seguridad para las aplicaciones del negocio; b) las políticas para la divulgación y autorización de la información, y los niveles de seguridad de la información y de clasificación de la información; c) la coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes; d) la legislación pertinente y cualquier obligación contractual concerniente a la limitación del acceso a datos o servicios; e) la gestión de los derechos de acceso en un entorno distribuido y en red, que reconoce todos los tipos de conexiones disponibles; f) la separación de los roles de control de acceso, (solicitud de acceso, autorización de acceso, administración del acceso); g) los requisitos para la autorización formal de las solicitudes de acceso; h) los requisitos para la revisión periódica de los derechos de acceso; i) el retiro de los derechos de acceso; j) el registro de los registros de todos los eventos significativos concernientes al uso y gestión de identificación de los usuarios, e información de autenticación secreta, en el archivo permanente; k) los roles de acceso privilegiado.
T.1.1.2	Responsable de TICs	Acceso a redes y a servicios en red	Se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	A.9.1.2		PR.AC-4 PR.DS-5 PR.PT-3	Revisar la política relacionada con el uso de redes y de servicios de red y verificar que incluya: a) las redes y servicios de red a los que se permite el acceso; b) los procedimientos de autorización para determinar a quién se permite el acceso a cuál redes y servicios de red; c) los controles y procedimientos de gestión para proteger el acceso a las conexiones de red y a los servicios de red;

Gráfica 46 - Hoja Técnicas, columna 1 a 8

En esta hoja deben diligenciarse las pruebas técnicas a continuación se explican los primeros 8 campos, correspondientes a la gráfica anterior:

- **ID. ítem:** Este campo ya está diligenciado y no debe modificarse, corresponde al identificador del ítem evaluado, para las pruebas técnicas todos los ítems empiezan con la letra T y un consecutivo numérico.
- **Cargo:** Responsable o área que deberá facilitar el acceso a la información y evidencias sobre la definición e implementación del control o requisito a evaluar.
- **Ítem:** Nombre del control o requisito a evaluar.
- **Descripción:** Explicación de lo que se espera del control o requisito, este campo es una orientación para el evaluador y está alineado con lo solicitado en Gobierno en Línea, el MSPI, las mejores prácticas (ISO 27002, NIST).
- **ISO:** Indica el nombre del control del anexo A de la Norma ISO 27001:2013, que se corresponde con el control o con el requisito.

- **MSPI:** Indica que requisito del Modelo de Seguridad definido por el ministerio de las TIC, corresponde con el control o requisito evaluado. Que puede corresponder al ciclo PHVA o el modelo de madurez definido.
- **Ciberseguridad:** Indica que requisito de Ciberseguridad definido por NIST corresponde con el control o requisito evaluado.
- **Prueba:** Este campo es la guía para que el evaluador desarrolle las pruebas y revise el nivel de cumplimiento frente a la Norma ISO 27001:2013 (se han incluido mejores prácticas sugeridas por la ISO 27002:2013), también se incluyen los requisitos de Gobierno en Línea y el MSPI.



Gráfica 17 - Hoja Técnicas, columna 9 a 12

A continuación, se explican los campos restantes:

- **Evidencia:** Este campo debe diligenciarse por el evaluador, documentando el resultado de las entrevistas, la fecha de la entrevista y el cargo del entrevistado, y adjuntando cuando aplique (como documento embebido) la evidencia de una prueba o hallazgo. El diligenciamiento debe hacerse a nivel dos (2) de cada Identificador de Ítem, por ejemplo T.1.1, A.1.2, etc. Por lo que se deben combinar las celdas.
- **Brecha:** Este campo debe diligenciarse por el evaluador, indicando que le hace falta al control o requisito para cumplir frente a la Norma ISO 27001:2013, también se incluyen los requisitos de Gobierno en Línea y el MSPI.
- **Nivel de cumplimiento:** Este campo debe diligenciarse por el evaluador, y solo acepta los valores 0, 20, 40, 60, 80 y 100, de acuerdo a la Hoja Escala de Evaluación, que ya fue explicada en el numeral 4.1.1, de este documento.

5.7. HOJA 7 -> AVANCE PHVA:

A continuación, se muestran y explican los componentes de la hoja de pruebas técnicas:

A través del diligenciamiento y la formulación de esta hoja se determina el nivel de cumplimiento de acuerdo al ciclo PHVA del modelo de seguridad MSPI, el ciclo evaluado incluye

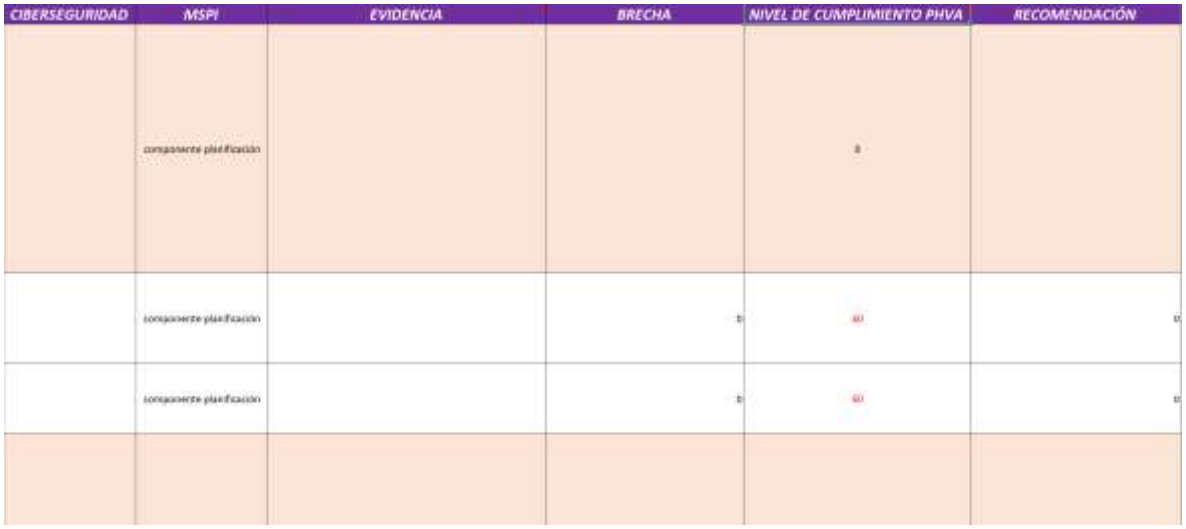
cuatro (4) componentes Planificación, Implementación, Gestión y Mejora Continua.

COMPONENTE	ID	CARGO	ITEM	DESCRIPCIÓN	PRUEBA
PLANIFICACIÓN	P.1	Responsable	Alcande MSPI (Modelo de Seguridad y Privacidad de la Información)	Se debe determinar los límites y la aplicabilidad del SGSI para establecer su alcance.	Interior de la Entidad, por la alta dirección. Determine si en la definición del alcance se considerará: 1) Aspectos internos y externos referidos en el 4.1.: La Entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el SGSI. Nota. La terminación de estos
	P.2	Responsable SI	Políticas de seguridad y privacidad de la información	Se debe definir un conjunto de políticas para la seguridad de la informaciôln aprobada por la dirección, publicada y comunicada a los empleados y a la partes externas pertinentes	Solicite la política de seguridad de la información de la entidad y evalúe: a) Si se definen los objetivos, alcance de la política b) Si esta se encuentra alineada con la estrategia y objetivos de la entidad
	P.3	Calidad	Procedimientos de control documental del MSPI	La información documentada se debe controlar para asegurar que: a. Esté disponible y adecuado para su uso, cuando y donde se requiere b. Esté protegida adecuadamente.	gestión institucional, por ejemplo el sistema de calidad SGC. Verifique: 1) Cómo se controla su distribución, acceso, recuperación y uso 2) Cómo se almacena y se asegura su preservación 3) Cómo se controlan los cambios
	P.4	Responsable	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información	Solicite el acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (ó e que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección. Revise la estructura del SGSI: 1) Tiene el SGSI suficiente apoyo de la alta dirección?, esto se ve reflejado en comités donde se discutan temas como la política de SI, los riesgos o
	P.5	Responsable	Inventario de activos	Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	la alta Dirección y revise: 1) Ultima vez que se actualizó 2) Que señale bajo algún criterio la importancia del activo 3) Que señale el propietario del activo Indague quien(es) el(los) encargado(s) de actualizar y revisar el inventario de activos y cada cuanto se realiza esta revisión. De acuerdo a NIST se deben considerar como activos el personal, dispositivos, sistemas e instalaciones físicas que permiten a la entidad
	P.6	Responsable	Identificación y valoración de riesgos	Metodología de análisis y valoración de riesgos e informe de análisis de riesgos	aprobado por la alta Dirección que incluya: 1. Criterios de Aceptación de Riesgos o tolerancia al riesgo que han sido informados por la alta Dirección. 2. Criterios para realizar evaluaciones de riesgos. 2) Solicite los resultados de las evaluaciones de riesgos y establezca:
	P.8	Responsable	Tratamiento de riesgos de seguridad de la información	Los riesgos deben ser tratados para mitigarlos y llevarlos a niveles tolerables por la Entidad	aplicabilidad verifique que: a. Se seleccionaron opciones apropiadas para tratar los riesgos, teniendo en cuenta los resultados de la evaluación de riesgos. b. Se determinaron todos los controles necesarios para implementar las opciones escogidas para el tratamiento de riesgos. c. Compare los controles determinados en el plan de tratamiento con los
	P.9	Responsable	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	Entreviste a los líderes de los procesos y pregúnteles que saben sobre la seguridad de la información, cuales son sus responsabilidades y como aplican la seguridad de la información en su diario trabajo. Pregunte como se asegura que los funcionarios, Directores, Gerentes y contratistas tomen conciencia en seguridad de la información, alineado
	P.10	Responsable	Plan y Estrategia de transisicón de IPv4 a IPv6	Las razones de que se requiera el cambio del protocolo de V4 a V6, se resumen a continuación: 1) Debido al aumento de la utilización de las redes de telecomunicaciones las direcciones de internet que permiten establecer conexiones para cada elementos conectado a la red, conocidas como direcciones IP (Internet Protocol Versión 4), han entrado en una fase de agotamiento. 2) Mejora de la seguridad de la red en virtud de la arquitectura del nuevo protocolo y sus servicio.	Verifique: 1) El Inventario de TI (Hardware, software) levantado 2) El análisis de la infraestructura actual de red de comunicaciones, recomendaciones para adquisición de elementos de comunicaciones, cómputo y almacenamiento, compatibles con el protocolo IPv6
PROMEDIO					

Gráfica 58 - Hoja PHVA, columnas 1 a 6

La mayoría de filas de este documento se llenan automáticamente tomando las calificaciones de las hojas administrativas y técnicas, aquellas filas que no tienen sombreado son las que se deben diligenciar, a continuación, se explican los primeros 6 campos del documento:

- **Componente:** Nombre del componente del ciclo PHVA del MSPI
- **ID:** Identificador del requisito solicitado en el MSPI para dar cumplimiento a los componentes del ciclo, que se compone de la primera letra del componente y un número consecutivo, por ejemplo P.1, es el primer requisito del componente planificación.
- **Cargo:** Responsable o área que deberá facilitar el acceso a la información y evidencias sobre la definición e implementación del requisito a evaluar, solamente aplica para las filas que tienen sombreado, cuyas evaluaciones deben realizarse.
- **Ítem:** Nombre del requisito a evaluar.
- **Descripción:** Explicación de lo que se espera requisito.
- **Prueba:** Este campo es la guía para que el evaluador desarrolle las pruebas y revise el nivel de cumplimiento del requisito.



CIBERSEGURIDAD	MSPI	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO PHVA	RECOMENDACIÓN
	componente planificación			0	
	componente planificación		0	0	0
	componente planificación		0	0	0

Gráfica 19 - Hoja PHVA, columnas 7 a 12

A continuación, se explican los campos restantes correspondientes a la gráfica anterior:

- **Ciberseguridad:** Indica que requisito de Ciberseguridad definido NIST que corresponde con requisito evaluado en el ciclo PHVA.
- **MSPI:** Indica que requisito del Modelo de Seguridad definido por el ministerio de las TIC, corresponde con el requisito evaluado.

- **Evidencia:** Este campo debe diligenciarse por el evaluador solamente cuando no está sombreado, en los demás casos se llena automáticamente con las hojas administrativas y técnicas. Como ya se ha explicado anteriormente, en este campo se debe documentar el resultado de las entrevistas, su fecha y entrevistado, y adjuntar cuando aplique (como documento embebido) la evidencia de una prueba o hallazgo.
- **Brecha:** Este campo debe diligenciarse por el evaluador, indicando que le hace falta al control o requisito para cumplir frente a la Norma ISO 27001:2013, también se incluyen los requisitos de Gobierno en Línea y el MSPI.
- **Nivel de cumplimiento:** Este campo debe diligenciarse por el evaluador solamente cuando no está sombreado, en los demás casos se llena automáticamente con las hojas administrativas y técnicas. Solo acepta los valores 0, 20, 40, 60, 80 y 100, de acuerdo a la Hoja Escala de Evaluación, que ya fue explicada en el numeral 4.1.1, de este documento.
- **Recomendación:** Este campo debe diligenciarse por el evaluador, y debe indicar las actividades o acciones requeridas para cumplir con el componente del ciclo PHVA.

5.8. HOJA 8 -> CIBERSEGURIDAD:

En esta evaluación se pretende determinar cómo se encuentra la entidad frente a las mejores prácticas en ciberseguridad definidas por el NIST, con miras a ir realizando un diagnóstico frente a los lineamientos de la política de ciberseguridad y ciberdefensa definidos en el documento Conpes 3701 y el Conpes 3854.

Gráfica 60- Marco básico de funciones de Ciberseguridad[4]

El marco de Ciberseguridad de NIST fue creado en respuesta a la "orden ejecutiva 13636" del Departamento de Seguridad del Gobierno de los Estados Unidos (DHS por sus siglas en inglés) y propende por mejorar la seguridad de la infraestructura crítica de la nación frente a ciber ataques. Este marco es útil para guiar cualquier organización en la mejora de su estrategia y postura frente a la seguridad.

FUNCIÓN NIST	SUBCATEGORIA NIST	CONTROL ANEXO A ISO 27001	CARGO	REQUISITO	HOJA	CALIFICACIÓN
DETECTAR	DE.AE-1, DE.AE-3, DE.AE-4, DE.AE-5	n/a	Responsable de SI	La detección de actividades anómalas se realiza oportunamente y se entiende el impacto potencial de los eventos: 1) Se establece y gestiona una linea base de las operaciones de red, los flujos de datos esperados para usuarios y sistemas. 2) Se agregan y correlacionan datos de eventso de multiples fuentes y sensores. 3) Se determina el impacto de los eventos 4) Se han establecido los umbrales de alerta de los incidentes.	n/a	100
DETECTAR	DE.AE-1	n/a	Responsable de SI	La efectividad de las tecnologías de protección se comparte con las partes autorizadas y apropiadas.	n/a	20

Gráfica 71 - Hoja CiberSeguridad

[4] Tomado del sitio: https://www.praetorian.com/blog/nist-cybersecurity-framework-vs-nist-special-publication-800-53

- **Función NIST:** La mejores prácticas de ciberseguridad del NIST, descritas en el documento marco para mejorar la ciberseguridad de la infraestructura crítica[5], están agrupadas en Funciones definidas en el marco de este documento. En este campo se identifica la función a la que pertenecen cada una de las subcategorías.
- **Subcategoría:** Son los nombres de los requisitos y están nombrados de acuerdo a la función y categoría a la que pertenecen.
- **Control Anexo A ISO 27001:** Menciona el control del Anexo A de la norma ISO 27001, que corresponde con el requisito de la NIST.
- **Cargo:** Para aquellos requisitos que no tienen un control correspondiente en el Anexo A, se menciona el responsable o área al que se debe entrevistar para determinar el nivel de cumplimiento del requisito. Las filas donde se requiere realizar entrevista se encuentran sombreadas, las demás se califican automáticamente de acuerdo a las evaluaciones de las hojas administrativas y técnicas.
- **Requisito:** Este campo es una guía para el evaluador y describe lo que se espera del requisito para efectuar las pruebas.
- **Hoja:** En los casos que se cuenta con un control correspondiente en el Anexo A de la norma ISO 27001, se menciona la hoja donde el control se encuentra que puede ser Administrativas o Técnicas.
- **Calificación:** En este campo se coloca la calificación del requisito que en su mayoría se efectúa de manera automática, de acuerdo a las calificaciones obtenidas por los controles en las hojas administrativas y técnicas, en las filas sombreadas se debe realizar una entrevista para poder colocar esta calificación manualmente.

[5] http://www.nist.gov/cyberframework/

5.9. HOJA 9 -> MADUREZ MSPI:

En el Instrumento de Evaluación, hoja madurez MSPI, se identificaron cada uno de los requisitos para cumplir los niveles de madurez definidos en el MSPI. Estos requisitos en su mayoría han sido previamente evaluados en las hojas Administrativas, Técnicas y PHVA. Existen tres requisitos de madurez que no fue posible identificar en las hojas mencionadas, en estos casos el evaluador deberá realizar la valoración y calificar manualmente (existen tres casos), en el resto de la tabla los controles se califican automáticamente con el diligenciamiento de las otras hojas mencionadas.

ID REQUISITO	CARGO	REQUISITOS	HOJA	ELEMENTO
R1	n/a	1) Si Se identifican en forma general los activos de información de la Entidad, estan en 40. 2) Si se cuenta con un inventario de activos de información física y lógica de toda la entidad, documentado y firmado por la alta dirección, estan en 60. 3) Si se revisa y monitorean periódicamente los activos de información de la entidad, estan en 80.	Administrativas	A.4.1.1
R2	n/a	Se clasifican los activos de información lógicos y físicos de la Entidad.	Administrativas	A.4.2.1
R3	n/a	1. Si Los funcionarios de la Entidad no tienen conciencia de la seguridad y privacidad de la información y se han diseñado programas para los funcionarios de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, estan en 20. 2. Si se observa en los funcionarios una conciencia de seguridad y privacidad de la información y los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, estan aprobados y documentados, por la alta Dirección, estan en 40. 3. Si se han ejecutado los planes de toma de conciencia, comunicación y divulgación, de las políticas de seguridad y privacidad de la información, aprobados por la alta Dirección, , estan en 60.	Administrativas	A.3.2.2
R4	n/a	Existe la necesidad de implementar el Modelo de Seguridad y Privacidad de la Información, para definir políticas, procesos y procedimientos claros para dar una respuesta proactiva a las amenazas que se presenten en la Entidad.	PHVA Administrativas PHVA	P.1 A.1.1 P.4
R5	Responsable de SI	1. Si se tratan temas de seguridad y privacidad de la información en los comités del modelo integrado de gestión, coloque 20 2.Los temas de seguridad de la información se tratan en los comités directivos interdisciplinarios de la Entidad, con regularidad, coloque 40	Madurez	R5
R6	n/a	1. Si se empiezan a definir las políticas de seguridad y privacidad de la información basada en el Modelo de Seguridad y Privacidad de la Información, estan en 20. 2. Si se revisan y se aprueban las políticas de seguridad y privacidad de la información, , estan en 40. 3. Si se divulgan las políticas de seguridad y privacidad de la información, estan en 60.	Administrativas	A.1.1
R7	n/a	Establecer y documentar el alcance, limites, política, procedimientos, roles y responsabilidades y del Modelo de Seguridad y Privacidad de la Información.	PHVA	P.1
R8	n/a	Determinar el impacto que generan los eventos que atenten contra la integridad, disponibilidad y confidencialidad de la información de la Entidad.	Tecnicas	T.7.1.4
LIMITE DE MADUREZ INICIAL				

Gráfica 82 - Madurez MSPI, columnas 1 a 5

A continuación, se explican los campos mostrados en la gráfica anterior, correspondientes a la hoja Madurez MSPI:

- **ID Requisito:** Corresponde al identificador del requisito.
- **Cargo:** Solamente aplica para las tres filas de requisitos que no fueron evaluadas en las pruebas administrativas, técnicas o del PHVA e indica el responsable o área que debe ser entrevistado para evaluar el requisito de madurez.
- **Requisito:** Corresponde a lo que se está solicitando en el MSPI para cumplir con un nivel de madurez determinado.
- **Hoja:** Señala la hoja en donde se encuentra el requisito o control correspondiente que puede ser Administrativas, Técnicas o PHVA.
- **Elemento:** Es el ID del control o requisito correspondiente que permite tomar la calificación de manera automática.

CALIFICACIÓN CMMI OBTENIDA	NIVEL 1 INICIAL	CUMPLIMIENTO NIVEL INICIAL	NIVEL 2 GESTIONADO	CUMPLIMIENTO NIVEL GESTIONADO	NIVEL 3 DEFINIDO	CUMPLIMIENTO NIVEL DEFINIDO	NIVEL 4 GESTIONADO CUANTITATIVAMENTE	CUMPLIMIENTO NIVEL 4 GESTIONADO CUANTITATIVAMENTE	NIVEL 5 OPTIMIZADO	CUMPLIMIENTO NIVEL 5 OPTIMIZADO
40	40	CUMPLE	60	MENOR	60	MENOR	80	MENOR	100	MENOR
20	20	CUMPLE	40	MENOR	60	MENOR	80	MENOR	100	MENOR
50	20	MAYOR	40	MAYOR	60	MENOR	80	MENOR	100	MENOR
0	20	MENOR	40	MENOR	60	MENOR	80	MENOR	100	MENOR

Gráfica 93 - Madurez MSPI, columnas 6 a 16

En la parte restante de la tabla se encuentran los siguientes campos:

- **Calificación obtenida:** Este campo corresponde a la calificación del requisito solicitado y proviene en casi todos los casos de las calificaciones otorgadas por el evaluador en las hojas Administrativas, Técnicas y PHVA, y

en solo 3 casos se califica de acuerdo a la Escala de Evaluación (aquellas filas sombreadas con trama de puntos).

- **Nivel inicial:** Este campo, sombreado en azul claro (en correspondencia con los colores del documento MSIP), presenta los requisitos correspondientes a nivel de madurez inicial identificados por tener un valor (los requisitos correspondientes a otros niveles tienen un N/A). Este es el valor mínimo que se debe alcanzar en la columna calificación obtenida, para quedar dentro del nivel inicial.
- **Cumplimiento nivel inicial:** Esta fórmula se presenta para cada requisito del nivel inicial, e indica sí se cumple con la calificación requerida (cumple y mayor) o si por el contrario no se cumple (menor).
- **Nivel gestionado:** Este campo, sombreado en azul oscuro (en correspondencia con los colores del documento MSIP), contiene los mismos requisitos del nivel inicial, con calificaciones superiores y nuevos requisitos, identificados por tener un valor (los requisitos correspondientes a otros niveles tienen un N/A). Este es el valor mínimo que se debe alcanzar en la columna calificación obtenida, para quedar dentro del nivel gestionado.
- **Cumplimiento nivel gestionado:** Esta fórmula se presenta para cada requisito del nivel gestionado e indica, sí se cumple con la calificación requerida (cumple y mayor) o si por el contrario no se cumple (menor).
- **Nivel definido:** Este campo, sombreado en verde (en correspondencia con los colores del documento MSIP), contiene los requisitos de los niveles inicial y gestionado, con calificaciones superiores y nuevos requisitos, identificados por tener un valor (los requisitos correspondientes a otros niveles tienen un N/A). Este es el valor mínimo que se debe alcanzar en la columna calificación obtenida, para quedar dentro del nivel definido.
- **Cumplimiento nivel definido:** Esta fórmula se presenta para cada requisito del nivel definido e indica, sí se cumple con la calificación requerida (cumple y mayor) o si por el contrario no se cumple (menor).
- **Nivel gestionado cuantitativamente:** Este campo, sombreado en naranja (en correspondencia con los colores del documento MSIP), contiene los mismos requisitos de los niveles inicial, gestionado y definido con calificaciones superiores y nuevos requisitos, identificados por tener un valor (los requisitos correspondientes a otros niveles tienen un N/A). Este es el valor mínimo que se debe alcanzar en la columna calificación obtenida, para quedar dentro del nivel gestionado cuantitativamente.
- **Cumplimiento nivel gestionado cuantitativamente:** Esta fórmula se presenta para cada requisito del nivel gestionado cuantitativamente e indica,

sí se cumple con la calificación requerida (cumple y mayor) o si por el contrario no se cumple (menor).

- **Nivel optimizado:** Este campo, sombreado en rojo (en correspondencia con los colores del documento MSIP), contiene los valores de los niveles inferiores y un único valor para un nuevo requisito Estos son los valores mínimos que se debe alcanzar en la columna calificación obtenida, para quedar dentro del nivel optimizado.
- **Cumplimiento nivel optimizado:** Esta fórmula presenta para cada requisito del nivel optimizado e indica, sí se cumple con la calificación requerida (cumple y mayor) o si por el contrario no se cumple (menor).