PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

	NOMBRE	CARGO	FECHA
ELABORÓ	Jaime Andrés Sánchez Diaz	Líder de Sistemas	01/2026
VALIDÓ	Diego Fernando Rivera Castro	Jefe de la Oficina Asesora de Planeación	01/2026
APROBÓ	Comité Institucional de Gestión y Desempeño		01/2026

CONTENIDO

1. INTRODUCCIÓN....3
2. OBJETIVOS....3
   2.1. Objetivo General....3
   2.2. Objetivos Específicos....3
3. TÉRMINOS Y DEFINICIONES....3
4. MARCO LEGAL....4
5. RECURSOS....4
   5.1. Talento Humano....4
   5.2. Equipos Físicos....4
   5.3. Recursos Tecnológicos....5
   5.4. Recursos económicos....5
6. ENFOQUE DIFERENCIAL....5
7. **DIAGNOSTICO PARA EL PLANTEAMIENTO DE ACCIONES**....5
8. PLAN DE ACCIÓN....6
9. BIBLIOGRAFÍA....7
10. CONTROL DE CAMBIOS....7

1.

1. INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información del Hospital Regional de Moniquirá ESE tiene como finalidad la implementación de las mejores prácticas establecidas por el Departamento Administrativo de la Función Pública, en el marco del Modelo Integrado de Planeación y Gestión (MIPG), y por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), a través del Modelo de Seguridad y Privacidad de la Información (MSPI). Este plan se alinea con el objetivo principal del área de sistemas de brindar a los usuarios recursos informáticos en condiciones adecuadas de calidad, disponibilidad y continuidad, garantizando la prestación de servicios tecnológicos confiables los 365 días del año.

El hospital dispone de una cantidad significativa de recursos de cómputo y de telecomunicaciones que soportan los procesos asistenciales y administrativos, los cuales deben ser protegidos de manera integral para asegurar su correcto funcionamiento. En este sentido, el presente plan aplica a los clientes internos, externos y demás partes interesadas que interactúan con la información y los sistemas de información del hospital, promoviendo una gestión adecuada de la seguridad de la información y de los activos de información institucionales.

El Plan de Seguridad y Privacidad de la Información cubre los procesos estratégicos, misionales y de apoyo del Hospital Regional de Moniquirá ESE. Sus lineamientos y requisitos deberán ser conocidos, adoptados y cumplidos por todo el personal, incluidos servidores públicos, contratistas, proveedores y terceros que tengan acceso a los sistemas de información, plataformas tecnológicas o instalaciones físicas del hospital.

Este plan se construye con base en el Modelo de Seguridad y Privacidad de la Información (MSPI) definido por el MinTIC, el cual cuenta con amplia documentación, lineamientos, guías y herramientas orientadas a apoyar a las entidades públicas en la implementación, operación y mejoramiento continuo de la seguridad y privacidad de la información. En este contexto, el plan tiene como propósito orientar la implementación y socialización del componente de Seguridad y Privacidad de la Información, como parte del marco de Gobierno Digital.

El MSPI contempla acciones transversales orientadas a proteger la información y los sistemas de información frente a accesos no autorizados, uso indebido, divulgación, alteración, interrupción o destrucción, salvaguardando tanto la información asistencial como la

administrativa del hospital. De esta manera, se busca garantizar los principios de confidencialidad, integridad y disponibilidad de la información, mediante la adopción de controles y mecanismos que soporten la autenticación y el no repudio en los procesos informáticos.

El presente plan será actualizado de manera periódica, como mínimo de forma anual, con el fin de asegurar su alineación con los objetivos estratégicos institucionales y con el marco

.

2. OBJETIVOS

2.1. Objetivo General

El Plan de Seguridad y Privacidad de la Información, tiene como propósito plantear las diferentes actividades a realizar con el fin de identificar los activos y riesgos de información asociados a los diferentes procesos que el Hospital Regional de Moniquirá ESE. posee dentro del modelo organización, de tal manera que se puedan medir los riegos inherentes y residuales de la entidad.

2.2. Objetivos Específicos

- **Establecer y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) robusto:** Implementar, mantener y mejorar continuamente un SGSI alineado con estándares internacionales (como ISO 27001) para proteger los activos de información del Hospital. Esto incluye la creación y revisión periódica de políticas, procedimientos, y la realización de evaluaciones de riesgos.
- **Cumplimiento normativo y legal:** Asegurar el cumplimiento estricto de toda la legislación aplicable en materia de protección de datos personales y seguridad de la información, tanto a nivel nacional como internacional.
- **Concientización y capacitación:** Promover una cultura de seguridad de la información en toda la organización a través de programas de capacitación dirigidos a todos los niveles, desde la alta dirección hasta los empleados de primera línea.

- **Optimización de procesos y tecnologías:** Implementar tecnologías y herramientas de seguridad de última generación para mejorar la protección de los activos de información, y optimizar los procesos internos relacionados con la seguridad, como el acceso a la información y la gestión de incidentes.

3. TÉRMINOS Y DEFINICIONES

Las únicas fuentes validas, son las de referentes académicos o páginas estatales y/o gubernamentales.

ID	Termino	Definición	Fuente
1	**Activos de Información**	Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.	TI
2	**Aviso de Privacidad**	Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.	TI
3	**Identificación De Activos De Información**	Es un código para ordenar y localizar los activos de información.	TI
4	**Clasificación De Información**	Es la clasificación que se debe dar en función de los requisitos legales, valor, criticidad, y susceptibilidad a divulgación o modificaciones no autorizadas.	TI
5	**Integridad**	La información y sus métodos de procesamiento deben ser completos y exactos.	TI

ID	Termino	Definición	Fuente
6	**Disponibilidad**	La información y los servicios deben estar disponibles en el momento que sea requerido.	TI
7	**Confidencialidad**	La información debe ser accesible sólo a aquellas personas autorizadas.	TI
8	**Control**	Los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.	TI
9	**Dato Personal**	Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley.	TI
10	**Dato Público**	Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.	TI
11	**Dato Semiprivado**	Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o	TI

ID	Termino	Definición	Fuente
		divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.	
12	**Dato Privado**	Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.	TI
13	**Dato Sensible**	Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.	TI
14	**Documento en Construcción**	Es aquella información preliminar o no definitiva.	(artículo 6, literal k Ley 1712 de 2014).
15	**Información Clasificada**	Es aquella información que estando en poder o custodia de un sujeto, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado de manera motivada	(Artículo 6, literal c y 18 Ley 1712 de 2014).

ID	Termino	Definición	Fuente
		y por escrito, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados estipulados en el artículo 18 de la Ley 1712 de 2014 y su acceso pudiere causar un daño a los siguientes derechos: a. El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado; b. El derecho de toda persona a la vida, la salud o la seguridad; c. Los secretos comerciales, industriales y profesionales, así como los estipulados en el parágrafo del artículo 77 de la Ley 1474 de 2011. Estas excepciones tienen una duración ilimitada y no deberán aplicarse cuando la persona natural o jurídica ha consentido en la revelación de sus datos personales o privados o bien cuando es claro que la información fue entregada como parte de aquella información que debe estar bajo el régimen de publicidad aplicable.	
16	**Información Pública Reservada**	Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía de manera motivada y por escrito, por daño a intereses públicos y bajo el cumplimiento de la totalidad de	(Artículo 6, literal d y artículo 19 Ley 1712 de 2014).

ID	Termino	Definición	Fuente
		los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. Se podrá negar el acceso a esta información cuando concurra una de las siguientes circunstancias y siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional: a. La defensa y seguridad nacional; b. La seguridad pública; c. Las relaciones internacionales; d. La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso; e. El debido proceso y la igualdad de las partes en los procesos judiciales; f. La administración efectiva de la justicia; g. Los derechos de la infancia y la adolescencia; h. La estabilidad macroeconómica y financiera del país; i. La salud pública. Se exceptúan también los documentos que contengan las opiniones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos.	
17	**Transferencia**	La transferencia de datos tiene lugar cuando el responsable y/o Encargado del Tratamiento de	TI

ID	Termino	Definición	Fuente
		datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.	
18	**Modelo de Seguridad y Privacidad de la Información (MSPI)**	Conjunto de lineamientos, políticas, procesos, procedimientos, roles, responsabilidades y controles definidos por el Estado colombiano para proteger la confidencialidad, integridad y disponibilidad de la información, garantizando su adecuado tratamiento, gestión del riesgo y cumplimiento normativo en las entidades públicas, en concordancia con la estrategia de Gobierno Digital y el Modelo Integrado de Planeación y Gestión (MIPG).	Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC / Departamento Administrativo de la Función Pública

4. MARCO LEGAL

ID	Norma	Número	Año	Emisor	Define
1	Ley de Transparencia y Acceso a la Información Pública	1712	2014	Congreso de la República	Regula el derecho fundamental de acceso a la información pública. Establece categorías de información, reservas y lineamientos relacionados con la seguridad de la

ID	Norma	Número	Año	Emisor	Define
					información.
2	Resolución de Estándares de Publicación de Información	3564	2015	MinTIC	Define los estándares para la publicación y divulgación de información en medios digitales del Estado.
3	Ley Estatutaria de Protección de Datos Personales	1581	2012	Congreso de la República	Establece disposiciones generales para la protección de datos personales.
4	Decreto Reglamentario de la Ley 1581	1377	2013	Gobierno Nacional	Reglamenta parcialmente la Ley de Protección de Datos Personales.
5	Decreto sobre Firma Electrónica	2364	2012	Gobierno Nacional	Reglamenta el uso de la firma electrónica en Colombia.
6	Decreto sobre Entidades de Certificación Digital	1747	2000	Gobierno Nacional	Regula las entidades de certificación y los certificados digitales.
7	Ley Antitrámites	Decreto Ley 019	2012	Gobierno Nacional	Suprime y reforma trámites innecesarios en la administración pública.
8	Decreto Antitrámites	2106	2019	Gobierno Nacional	Establece medidas para la simplificación, digitalización y automatización de trámites, promoviendo el uso de medios electrónicos y servicios digitales seguros.
9	Código de Procedimien	1437	2011	Congreso de la	Regula las actuaciones administrativas,

ID	Norma	Número	Año	Emisor	Define
	to Administrativo y de lo Contencioso Administrativo			República	incluyendo el uso de medios electrónicos y la gestión documental digital.
10	Ley de Participación Ciudadana	1757	2015	Congreso de la República	Promueve la participación democrática y el control social mediante el uso de mecanismos presenciales y digitales.
11	Plan Nacional de Desarrollo – Pacto por Colombia, Pacto por la Equidad	Ley 1955	2019	Congreso de la República	Define lineamientos estratégicos en materia de Gobierno Digital, interoperabilidad, servicios ciudadanos digitales y fortalecimiento de la seguridad de la información (arts. 147 y 148).
12	Decreto Único Reglamentario del Sector TIC	1078	2015	Gobierno Nacional	Compila las normas del sector TIC, incluyendo Gobierno Digital, Seguridad Digital y el Modelo de Seguridad y Privacidad de la Información.
13	Política de Gobierno Digital	Decreto 767	2022	Gobierno Nacional	Actualiza la Política de Gobierno Digital, su implementación diferencial y la articulación con MIPG y MSPI.
14	Lineamientos para el	Decreto 415	2016	Gobierno Nacional	Establece directrices para la organización y

ID	Norma	Número	Año	Emisor	Define
	fortalecimiento institucional en TIC				fortalecimiento de las áreas TIC en las entidades públicas.
15	Servicios Ciudadanos Digitales	Decreto 1413	2017	Gobierno Nacional	Reglamenta la prestación de los Servicios Ciudadanos Digitales, incluyendo autenticación digital, interoperabilidad y seguridad de la información.
16	Directiva Presidencial – Interacción Digital Estado–Ciudadano	Directiva 02	2019	Presidencia de la República	Impulsa la simplificación y digitalización de la interacción entre el Estado y la ciudadanía mediante el uso de plataformas digitales seguras.
17	Política Nacional de Seguridad Digital	CONPES 3854	2016	CONPES	Establece la Política Nacional de Seguridad Digital y la gestión de riesgos cibernéticos en el sector público.
18	Ley de Habeas Data Financiero	1266	2008	Congreso de la República	Regula el manejo de información financiera, crediticia y comercial.
19	Norma Técnica de Seguridad de la Información	NTC ISO/IEC 27001	2013	ICONTEC	Requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información.
20	Código de buenas prácticas de seguridad	NTC ISO/IEC 27002	2013	ICONTEC	Proporciona controles y buenas prácticas para la gestión de la seguridad de la información.

5. RECURSOS

5.1. Talento Humano

ID	Recurso	Cantidad
1	INGENIERO	2
2	TECNOLOGO	1
3	TECNICO	1

5.2. Equipos Físicos

ID	Recurso	Cantidad
1	EQUIPOS DE COMPUTO DE ESCRITORIO	7
2	EQUIPOS DE COMPUTO PORTATIL	1

5.3. Recursos Tecnológicos

ID	Recurso	Cantidad
1	EQUIPOS DE COMPUTO DE ESCRITORIO	7
2	EQUIPOS DE COMPUTO PORTATIL	1

5.4. Recursos económicos

ID	Recurso	Cantidad
1	Talento Humano	$137.376.000
2	Compra de insumos informáticos	$ 50.000.000

6. ENFOQUE DIFERENCIAL

Bajo este contexto el Hospital Regional de Moniquirá estableció el *Protocolo Enfoque Diferencial en todos los Servicios GIU-PT -01. Cargado en la pltaforma.*

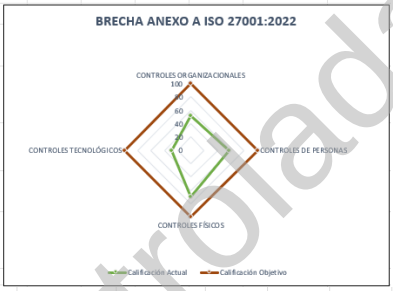
7. DIAGNOSTICO PARA EL PLANTEAMIENTO DE ACCIONES

Para alinear este enfoque con las metodologías del MinTic, se implementarán las siguientes acciones:

7.1. Diagnóstico de la implementación de MSPI

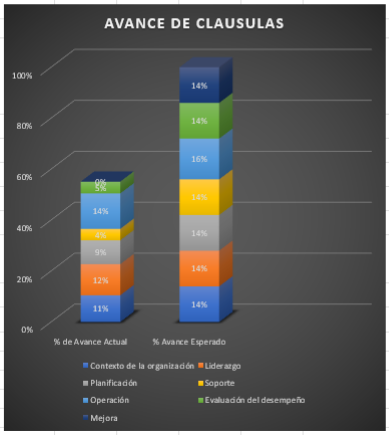
EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2022 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	52	100	EFECTIVO
A.6	CONTROLES DE PERSONAS	58	100	EFECTIVO
A.7	CONTROLES FÍSICOS	70	100	GESTIONADO
A.8	CONTROLES TECNOLÓGICOS	29	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		52	100	EFECTIVO



AVANCE CLÁUSULAS DEL MODELO DE OPERACIÓN (PHVA)

AÑO	COMPONENTE (PHVA)	CLAUSULAS	% de Avance Actual	% Avance Esperado
2025	Planificación	Contexto de la organización	11%	14%
		Liderazgo	12%	14%
		Planificación	9%	14%
		Soporte	4%	14%
	Implementación	Operación	14%	16%
	Evaluación de Desempeño	Evaluación del desempeño	5%	14%
	Mejora Continua	Mejora	0%	14%
TOTAL			55%	100%



Función	Categoría	Identificador de Categoría	CALIFICACIÓN	Clausula / Control ISO 27001
Governar (GV)	Contexto organizativo	GV.OC	75	4. Contexto de la Organización
Governar (GV)	Estrategia de gestión de riesgos	GV.RM	0	6.1 Acciones para tratar con los riesgos y oportunidades
Governar (GV)	Funciones, responsabilidades y autoridades	GV.RR	86,66666667	5.2. Funciones y responsabilidades de seguridad de la información. 5.3

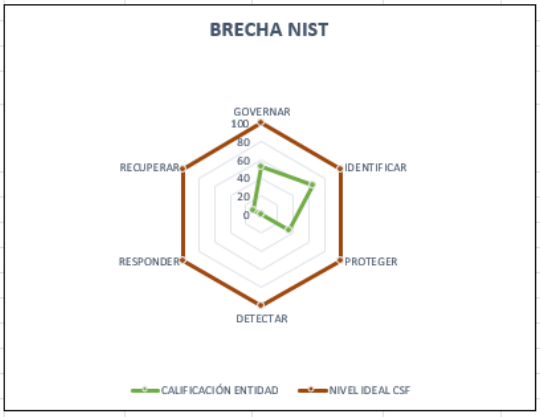
Función	Categoría	Identificador de Categoría	CALIFICACIÓN	Clausula / Control ISO 27001
				Segregación de funciones. 5.5 Contacto con las autoridades
Governar (GV)	Política	GV.PO	90	Clausula 5.2 Política. 5.1 Políticas de seguridad de la información
Governar (GV)	Supervisión	GV.OV	60	8.16 Actividades de supervisión
Governar (GV)	Gestión de riesgos de la cadena de suministro en materia de seguridad cibernética	GV.SC	0	5.21 Gestión de seguridad de la información en la gestión de la cadena de suministro TIC
Identificar (ID)	Gestión de activos	ID.AM	93	5.9 Inventario de información y otros activos asociados. 5.10 Uso aceptable de la información y otros activos asociados 5.11 Devolución de activos
Identificar (ID)	Evaluación de riesgos	ID.RA	100	Clausula 8.2 Evaluación de riesgos de seguridad de la información.
Identificar (ID)	Mejora	ID.IM	0	Clausula 10.1 Mejora continua. 10.2 No conformidad y acciones correctivas
Proteger (PR)	Gestión de identidades, autenticación y control de acceso	PR.AA	57,5	8.2 Derechos de acceso privilegiado. 8.3 Restricción de acceso a la información. 8.4 Acceso al código fuente. 8.5 Autenticación segura 5.15 Control de

Función	Categoría	Identificador de Categoría	CALIFICACIÓN	Clausula / Control ISO 27001
				acceso. 5.16 Gestión de identidad. 5.17 Información de autenticación. 5.18 Derechos de acceso
Proteger (PR)	Concienciación y capacitación	PR.AT	60	6.3 Concientización, educación y capacitación en seguridad de la información
Proteger (PR)	Seguridad de datos	PR.DS	50	8.11 Enmascaramiento de datos. 8.12 Prevención de filtración de datos
Proteger (PR)	Seguridad de plataformas	PR.PS	0	8.21 Seguridad de los servicios de red
Proteger (PR)	Resistencia de la infraestructura tecnológica	PR.IR	0	8.27 Arquitectura del sistema seguro y principios de ingeniería
Detectar (DE)	Monitoreo continuo	DE.CM	0	Clausula 9.1. Seguimiento, medición, análisis y evaluación
Detectar (DE)	Análisis de eventos adversos	DE.AE	0	5.25 Evaluación y Decisión sobre Eventos de Seguridad de la Información
Responder (RS)	Gestión de incidentes	RS.MA	0	5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información
Responder (RS)	Análisis de incidentes	RS.AN	0	5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información
Responder (RS)	Notificación y comunicación de la	RS.CO	0	5.26 Respuesta a incidentes de

Función	Categoría	Identificador de Categoría	CALIFICACIÓN	Clausula / Control ISO 27001
	respuesta al incidente			seguridad de la información
Responder (RS)	Mitigación de incidentes	RS.MI	0	5.26 Respuesta a incidentes de seguridad de la información
Recuperar (RC)	Ejecución del Plan de Recuperación de Incidentes	RC.RP	0	5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información
Recuperar (RC)	Comunicación de la recuperación del incidente	RC.CO	0	5.26 Respuesta a incidentes de seguridad de la información
			30,57	

CALIFICACIÓN FRENTE A MEJORES PRÁCTICAS EN CIBERSEGURIDAD (NIST)

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	**CALIFICACIÓN ENTIDAD**	**NIVEL IDEAL CSF**
GOVERNAR	52	100
IDENTIFICAR	64	100
PROTEGER	34	100
DETECTAR	0	100
RESPONDER	0	100
RECUPERAR	10	100



7.1.3. Interpretación de Resultados:

El ejercicio de autoevaluación del Modelo de Seguridad y Privacidad de la Información (MSPI), realizado mediante el instrumento oficial del MinTIC y

alineado con la norma ISO/IEC 27001:2022, permitió al Hospital Regional de Moniquirá ESE obtener una visión integral, objetiva y estructurada del estado actual de la seguridad y privacidad de la información.

Como principal aprendizaje organizacional, se evidencia que la entidad cuenta con avances importantes en los componentes de planeación normativa y control administrativo, reflejados en altos niveles de cumplimiento en categorías como Política (90%), Gestión de Activos (93%), Funciones y Responsabilidades (86,7%) y Evaluación de Riesgos (100%). Esto demuestra que el hospital ha priorizado la formalización documental, la definición de roles y la identificación de riesgos, especialmente desde una perspectiva de cumplimiento normativo.

Sin embargo, la autoevaluación también permitió identificar brechas críticas en la operación del modelo, particularmente en los dominios asociados a la ejecución, seguimiento, respuesta y recuperación ante incidentes de seguridad de la información. Las calificaciones del 0% en funciones como Monitoreo Continuo, Gestión de Incidentes, Respuesta, Recuperación, Seguridad de Plataformas y Resiliencia de la Infraestructura evidencian que, si bien existen lineamientos y diagnósticos, estos no se han traducido aún en capacidades operativas, técnicas y procedimentales consolidadas.

Adicionalmente, el ejercicio permitió reconocer que la seguridad de la información ha sido abordada principalmente desde una lógica documental y de cumplimiento, más que como un proceso transversal, continuo y operativo, integrado al quehacer diario de las áreas misionales, asistenciales y de apoyo. Este aprendizaje resulta clave para orientar la transición hacia un enfoque de gestión efectiva de la seguridad de la información, conforme a los principios del MSPI y la Política de Seguridad Digital.

En este sentido, la autoevaluación no solo cumple una función diagnóstica, sino que se convierte en un insumo estratégico para la toma de decisiones, la priorización de inversiones, el fortalecimiento de capacidades institucionales y la definición de un plan de mejora realista y gradual.

7.1.4. Fase de madurez del Hospital Regional de Moniquirá ESE y acciones derivadas

Fase de madurez identificada

Con base en:

- El promedio general del instrumento MSPI (30,57%),
- Los resultados por función (Governar, Identificar, Proteger, Detectar, Responder y Recuperar),
- Y la evaluación de efectividad de controles ISO 27001:2022 (con predominio de niveles Repetible y Gestionado),

Se concluye que el Hospital Regional de Moniquirá ESE se encuentra en una fase de madurez **INICIAL – DEFINIDA**, caracterizada por:

- Existencia de políticas, lineamientos y responsabilidades formalmente documentadas.
- Identificación de activos y riesgos de seguridad de la información.
- Controles implementados de forma parcial y no homogénea.
- Ausencia de mecanismos sistemáticos de monitoreo, medición y respuesta.
- Débil integración de la seguridad de la información en la operación diaria y en la infraestructura tecnológica.

Esta fase corresponde a un nivel donde la organización sabe qué debe hacer, pero aún no lo ejecuta de forma consistente, medible y sostenible.

7.1.5. Acciones prioritarias derivadas según la fase de madurez

De acuerdo con el nivel de madurez identificado, las acciones deben enfocarse menos en crear nueva normativa y más en operacionalizar lo existente, priorizando las siguientes líneas:

a) Acciones de corto plazo (0–6 meses)

- Formalizar e implementar el Plan de Gestión de Incidentes de Seguridad de la Información, incluyendo roles, flujos de comunicación y procedimientos básicos.
- Designar y formalizar el responsable de Seguridad Digital y de la Información, conforme a la Política de Gobierno Digital.
- Iniciar la implementación de monitoreo básico de eventos de seguridad (logs, accesos, fallas de servicios).
- Fortalecer los controles de acceso, autenticación y gestión de identidades, especialmente en sistemas críticos hospitalarios.

b) Acciones de mediano plazo (6–12 meses)

- Implementar controles técnicos asociados a seguridad de plataformas y servicios de red.
- Desarrollar y socializar el Plan de Continuidad y Recuperación ante Incidentes de Seguridad de la Información, alineado con los servicios asistenciales críticos.
- Establecer indicadores de desempeño (KPIs) para el seguimiento del MSPI y la efectividad de controles.
- Consolidar programas de concienciación y capacitación continua para todo el personal.

2.3 Enfoque recomendado

Dado el contexto de un hospital público de segundo nivel, se recomienda adoptar un enfoque de madurez incremental, priorizando:

- Protección de información clínica y administrativa crítica.
- Disponibilidad de los sistemas que soportan la atención en salud.
- Respuesta oportuna a incidentes que puedan afectar la continuidad del servicio.

7.1.6. Análisis frente al Framework de Ciberseguridad NIST

La evaluación del Hospital Regional de Moniquirá ESE frente a las mejores prácticas del Framework de Ciberseguridad del NIST (CSF) evidencia una brecha significativa entre el estado actual de la entidad y el nivel ideal esperado, confirmando los resultados obtenidos en la autoevaluación del MSPI y la evaluación de controles ISO/IEC 27001:2022.

Resultados generales NIST CSF

Función NIST	Calificación Entidad	Nivel Ideal
Gobernar	52%	100%
Identificar	64%	100%
Proteger	34%	100%
Detectar	0%	100%
Responder	0%	100%
Recuperar	10%	100%

Estos resultados reflejan un desarrollo desigual de las capacidades de ciberseguridad, con avances concentrados en las funciones de Gobernar e Identificar, y brechas críticas en Detectar, Responder y Recuperar, que son esenciales para garantizar la continuidad y resiliencia de los servicios hospitalarios.

7.1.7.Brecha NIST

El análisis de la brecha NIST permite identificar los siguientes aprendizajes clave:

La entidad ha avanzado principalmente en componentes de planeación, definición de políticas, roles y gestión de activos, lo cual explica los resultados moderados en Gobernar (52%) e Identificar (64%).

La función Proteger (34%) presenta avances parciales, asociados a controles básicos de acceso, concienciación y protección de datos, pero carece de una implementación técnica robusta y estandarizada.

Las funciones Detectar (0%) y Responder (0%) evidencian la inexistencia de capacidades formales de monitoreo, análisis de eventos, gestión y respuesta a incidentes de ciberseguridad.

La función Recuperar (10%) muestra que no se cuenta con planes consolidados de recuperación ante incidentes de seguridad de la información ni con esquemas de continuidad operativa probados.

Este comportamiento confirma que la ciberseguridad en el hospital se encuentra en una etapa reactiva e incipiente, con alta dependencia de acciones manuales o ad hoc.

Correlación NIST – MSPI – ISO 27001:2022

- Los resultados del NIST CSF son coherentes con:
- El promedio general del MSPI (30,57%), que ubica a la entidad en una fase de madurez inicial.
- El bajo desempeño en los controles tecnológicos del Anexo A de ISO 27001:2022, especialmente en A.8 (Controles tecnológicos).
- La ausencia de procesos efectivos de monitoreo, respuesta y recuperación, identificados tanto en MSPI como en NIST.

En conjunto, los tres marcos evidencian que la entidad cuenta con fundamentos normativos, pero carece de capacidades operativas y técnicas consolidadas.

Ajuste de la fase de madurez con enfoque NIST

Integrando los resultados MSPI, ISO 27001:2022 y NIST CSF, se concluye que el Hospital Regional de Moniquirá ESE se encuentra en una:

Fase de Madurez: INICIAL / DEFINIDA (Nivel 1–2)

- Características del nivel:
- Políticas y lineamientos definidos.
- Gestión de activos y riesgos identificados.
- Controles aplicados de manera parcial y no sistemática.
- Ausencia de monitoreo continuo, respuesta estructurada y recuperación efectiva.
- Dependencia de acciones reactivas ante eventos de seguridad.

Acciones estratégicas derivadas del análisis NIST

Con base en las brechas identificadas, se priorizan las siguientes acciones alineadas al NIST CSF:

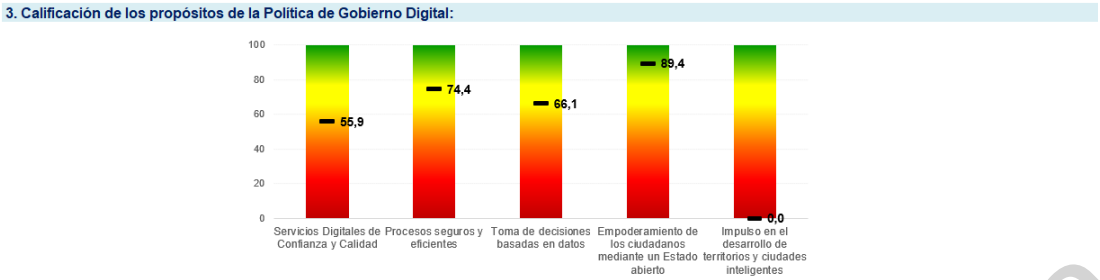
- Prioridad Alta (Gobernar – Identificar – Proteger)
    - Fortalecer la gobernanza de la seguridad digital, integrando MSPI y NIST al Comité Institucional de Gestión y Desempeño.
    - Consolidar el inventario de activos críticos y su clasificación.
    - Estandarizar controles de acceso, autenticación y protección de datos.
- Prioridad Crítica (Detectar – Responder)
    - Implementar capacidades mínimas de monitoreo de eventos de seguridad.
    - Diseñar e implementar el Proceso de Gestión de Incidentes de Seguridad de la Información.
    - Definir canales formales de notificación y escalamiento de incidentes.
- Prioridad Estratégica (Recuperar)

- Diseñar e implementar el Plan de Recuperación ante Incidentes de Seguridad de la Información.
- Integrar la recuperación de TI con los planes de continuidad de los servicios asistenciales.

La incorporación del análisis NIST refuerza que el Hospital Regional de Moniquirá ESE se encuentra en una fase temprana de madurez en ciberseguridad, con una base normativa aceptable, pero con brechas críticas en capacidades técnicas, operativas y de respuesta. El principal reto institucional no es normativo, sino de implementación efectiva y sostenibilidad del Modelo de Seguridad y Privacidad de la Información.

7.2. Autoevaluación de gobierno digital:

Evaluación del estado actual de los sistemas de información y tecnologías utilizadas con el instrumento de MIPG



7.2.1. Fortalecimiento de la Seguridad y Privacidad de la Información

De acuerdo con los resultados del autodiagnóstico de la Política de Gobierno Digital, el habilitador Fortalecimiento de la Seguridad y Privacidad de la Información obtuvo una calificación global del 50%, lo que evidencia un nivel de avance intermedio, con importantes fortalezas en el componente normativo y de planeación, pero con brechas relevantes en la implementación operativa y en la gestión de evidencias.

Análisis general del resultado

El resultado obtenido refleja que la entidad ha realizado esfuerzos significativos en la formulación y documentación de los elementos que componen el Modelo de Seguridad y Privacidad de la Información (MSPI). Sin embargo, dichos esfuerzos no se encuentran completamente materializados en la operación, ni cuentan de manera sistemática con evidencias que respalden su implementación efectiva, lo cual impacta negativamente la calificación final.

Este comportamiento es consistente con una entidad que se encuentra en una fase de transición entre la definición del modelo y su apropiación institucional, donde existen políticas, planes y procedimientos aprobados, pero aún no se han consolidado como prácticas transversales y sostenibles.

7.2.2. Diagnóstico de seguridad y privacidad de la información – 20%

La entidad cuenta con un diagnóstico de seguridad y privacidad de la información construido mediante la herramienta de autodiagnóstico del MSPI; no obstante, la baja calificación indica que dicho diagnóstico **no se encuentra plenamente institucionalizado**, ni se evidencia su uso

sistemático como insumo para la toma de decisiones, seguimiento o mejora continua.
Aprendizaje clave: El diagnóstico existe, pero requiere fortalecerse como un instrumento vivo, actualizado periódicamente y articulado con los planes de acción institucionales.

7.2.3. Política de Seguridad y Privacidad de la Información – 100%

La política se encuentra **aprobada, implementada y actualizada**, lo cual representa una fortaleza clara en el marco normativo de la entidad. Sin embargo, la observación evidencia que **no ha sido suficientemente socializada**, limitando su apropiación por parte de servidores, contratistas y terceros.
Aprendizaje clave: La formalización normativa es adecuada, pero la falta de socialización reduce su efectividad real.

7.2.4. Procedimientos de seguridad y privacidad – 60%

La entidad cuenta con procedimientos aprobados e implementados, pero la calificación intermedia indica que estos **no son ampliamente conocidos ni aplicados de forma homogénea**, lo que se ve reflejado en la falta de evidencias de ejecución.
Aprendizaje clave: Es necesario pasar del procedimiento documentado al procedimiento ejecutado y evidenciado.

7.2.5. Inventario de activos de información – 20%

Aunque existe información tanto en formato físico como digital y se realizan actualizaciones automáticas, la baja calificación indica que el inventario **no cumple completamente con los criterios del MSPI**, especialmente en lo relacionado con clasificación, formalización, trazabilidad y control.
Aprendizaje clave: La información existe, pero no se gestiona bajo un enfoque integral de activos de información.

7.2.6. Gestión de riesgos de seguridad y privacidad – 20%

La entidad realiza jornadas de identificación de riesgos; sin embargo, estas actividades **no se encuentran articuladas a un proceso continuo, documentado y con seguimiento**, lo que limita su impacto en la gestión institucional.

Aprendizaje clave: La gestión de riesgos se realiza de manera puntual y no como un proceso sistemático y permanente.

7.2.7. Plan de tratamiento de riesgos – 60%

El plan de tratamiento de riesgos se encuentra documentado, pero la ausencia de evidencias de ejecución indica que **no se ha implementado de forma efectiva**, o que su implementación no ha sido debidamente registrada.
Aprendizaje clave: Existe planeación, pero se requiere fortalecer la ejecución y la gestión documental de evidencias.

7.2.8. Plan operacional de seguridad y privacidad – 100%

La entidad cuenta con un plan operacional aprobado y actualizado, lo cual constituye una fortaleza importante. No obstante, la observación señala que **no se cuenta con evidencias claras de su ejecución**, lo que afecta la percepción de efectividad del plan.
Aprendizaje clave: El reto no es formular planes, sino demostrar su implementación real.

7.2.9. Indicadores del MSPI – 20%

Aunque los indicadores se encuentran definidos y documentados, la baja calificación refleja que **no se están midiendo, analizando ni utilizando para la toma de decisiones**, ni se evidencian procesos de seguimiento o mejora continua.
Aprendizaje clave: Sin medición ni análisis, el sistema de seguridad y privacidad no puede evolucionar ni madurar.

7.3. Recomendaciones FURAG

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA RECOMENDACIONES FURAG VIGENCIA 2024		
Entidad		
3539	**HOSPITAL REGIONAL DE MONIQUIRA**	**BOYACA**
Política	**Recomendación**	**Índice**
Seguridad Digital	Designar un área o responsable de la seguridad digital.	POL09

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA
RECOMENDACIONES FURAG VIGENCIA 2024

Entidad		
3539	**HOSPITAL REGIONAL DE MONIQUIRA**	**BOYACA**
Política	**Recomendación**	**Índice**
Seguridad Digital	Contar con un Plan de Recuperación de Desastres -DRP-, que esté definido, documentado e implementado para todos los procesos.	POL09
Seguridad Digital	Realizar pruebas de recuperación de cada uno de los sistemas de información críticos de la entidad.	POL09
Seguridad Digital	Identificar y gestionar los posibles riesgos de seguridad digital (Ciberseguridad) de sus infraestructuras on premise.	POL09
Seguridad Digital	Identificar y gestionar los posibles riesgos de seguridad digital (Ciberseguridad) en los servicios de Nube Pública/Privada que utiliza.	POL09
Seguridad Digital	Realizar análisis de vulnerabilidades de seguridad a los activos de información en su infraestructura On Premise.	POL09
Seguridad Digital	Realizar análisis de vulnerabilidades de seguridad a los activos de información de su infraestructura en Nube Pública/Privada.	POL09
Seguridad Digital	Verificar y asegurar que los proveedores y contratistas de la entidad cumplan con las políticas de ciberseguridad internas.	POL09
Seguridad Digital	Implementar un sistema para dar el cumplimiento a la Ley de protección de datos personales (ley 1581 de 2012)	POL09
Seguridad Digital	Establecer, documentar e implementar un procedimiento para la gestión de incidentes de seguridad	POL09

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA
RECOMENDACIONES FURAG VIGENCIA 2024

Entidad		
3539	**HOSPITAL REGIONAL DE MONIQUIRA**	**BOYACA**
Política	**Recomendación**	**Índice**
	digital (Ciberseguridad) que incluya la notificación a las autoridades pertinentes (CSIRT Gobierno / COLCERT).	
Seguridad Digital	Realizar retest para verificar la mitigación de vulnerabilidades y la aplicación de actualizaciones y parches de seguridad en sus sistemas de información.	POL09
Seguridad Digital	Contar con métodos de autenticación como DMARC, DKIM y SPF, para seguridad del correo electrónico y garantizar la autenticidad de los remitentes.	POL09
Gobierno Digital	Incluir en el Plan de Acción Anual de la entidad proyectos con enfoque experimental para generar soluciones novedosas y creativas que hagan uso de TIC, con la participación de actores de la ciudadanía, sector privado, academia y sector público.	POL10
Gobierno Digital	Implementar el Modelo de Gestión de Proyectos de Tecnologías de la Información (MGPTI) del Marco de Referencia de Arquitectura Empresarial (MRAE).	POL10
Gobierno Digital	Integrar el proceso de Arquitectura Empresarial al Sistema de Gestión de Calidad de la entidad.	POL10
Gobierno Digital	Establecer indicadores de seguimiento a la ejecución de los ejercicios de Arquitectura Empresarial en la entidad.	POL10
Gobierno	Ejecutar el proceso de Arquitectura	POL10

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA RECOMENDACIONES FURAG VIGENCIA 2024		
Entidad		
3539	**HOSPITAL REGIONAL DE MONIQUIRA**	**BOYACA**
Política	**Recomendación**	**Índice**
Digital	Empresarial en la entidad.	
Gobierno Digital	Desarrollar e implementar una estrategia de uso y apropiación de tecnologías actuales y emergentes (blockchain, inteligencia artificial, internet de las cosas, automatización robótica de procesos).	POL10
Gobierno Digital	Establecer estrategias para consolidar el conocimiento y las lecciones aprendidas del área de Tecnologías de la Información.	POL10
Gobierno Digital	Implementar en la entidad las 3 fases del modelo de adopción de IPv6: planeación, implementación y pruebas de funcionalidad.	POL10
Gobierno Digital	Realizar el plan de direccionamiento IPv6, como parte de las actividades de la fase 1 del modelo de adopción de IPv6 en la entidad.	POL10
Gobierno Digital	Realizar el diseño detallado de red, como parte de las actividades de la fase 1 del modelo de adopción de IPv6 en la entidad.	POL10
Gobierno Digital	Realizar el plan de contingencias de IPv6, como parte de las actividades de la fase 1 del modelo de adopción de IPv6 en la entidad.	POL10
Gobierno Digital	Realizar el documento de activación de políticas de seguridad para IPv6 como parte de las actividades de la fase 2 y 3 del modelo de adopción de IPv6 en la entidad.	POL10
Gobierno Digital	Realizar el informe de pruebas piloto y de implementación de IPv6, como	POL10

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA RECOMENDACIONES FURAG VIGENCIA 2024		
Entidad		
3539	**HOSPITAL REGIONAL DE MONIQUIRA**	**BOYACA**
Política	**Recomendación**	**Índice**
	parte de las actividades de la fase 2 y 3 del modelo de adopción de IPv6 en la entidad.	
Gobierno Digital	Realizar el acta de cumplimiento a satisfacción sobre el funcionamiento e implementación de los elementos que fueron intervenidos con IPv6, como parte de las actividades de la fase 2 y 3 del modelo de adopción de IPv6 en la entidad.	POL10
Gobierno Digital	Realizar el reporte de la entidad en la herramienta habilitada por el Ministerio TIC para el seguimiento del avance en la adopción de IPv6.	POL10
Gobierno Digital	Capacitar a los grupos de valor e interés (ciudadanía, sector privado, sociedad civil, academia, otras entidades públicas) en temáticas de la Política de Gobierno Digital.	POL10
Gobierno Digital	Elaborar un diagnóstico de seguridad y privacidad de la información para la entidad a través de la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI). Posteriormente, presentar y lograr la aprobación del diagnóstico en el Comité de Gestión y Desempeño Institucional.	POL10
Gobierno Digital	Definir, aprobar, implementar y actualizar los procedimientos de seguridad y privacidad de la información, mediante un proceso de mejora continua.	POL10
Gobierno	Aprobar, clasificar y actualizar el	POL10

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA
RECOMENDACIONES FURAG VIGENCIA 2024

Entidad		
3539	**HOSPITAL REGIONAL DE MONIQUIRA**	**BOYACA**
Política	**Recomendación**	**Índice**
Digital	inventario de activos de seguridad y privacidad de la información de la entidad, mendiante un proceso de mejora continua.	
Gobierno Digital	Definir indicadores para medir la eficiencia y eficacia del sistema de gestión de seguridad y privacidad de la información (MSPI) de la entidad, aprobarlos mediante el comité de gestión y desempeño institucional, implementarlos y actualizarlos mediante un proceso de mejora continua.	POL10
Gobierno Digital	Disponer de un servidor con las características establecidas en el anexo 2 del Decreto 620 de 2020 para vincularse al servicio de interoperabilidad, como lo establece la Guía para la Vinculación y Uso de los Servicios Ciudadanos Digitales del Ministerio de las TIC.	POL10
Gobierno Digital	Implementar la técnica de 'análisis prescriptivo' para el análisis de datos de la entidad. El uso de esta técnica permite establecer cuál es la mejor acción a tomar bajo un contexto específico.	POL10
Gobierno Digital	Elaborar un inventario y diccionario de datos de la entidad.	POL10
Gobierno Digital	Identificar cuáles de los datos maestros de la entidad son datos de referencia.	POL10
Gobierno Digital	Implementar el criterio de accesibilidad web 'CC27. Idioma' en la	POL10

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA RECOMENDACIONES FURAG VIGENCIA 2024		
Entidad		
3539	**HOSPITAL REGIONAL DE MONIQUIRA**	**BOYACA**
Política	**Recomendación**	**Índice**
	sede electrónica de la entidad, acorde con el anexo 1 de la Resolución 1519 de 2020.	
Gobierno Digital	Implementar el criterio de accesibilidad web 'CC32. Manejable por teclado' en la sede electrónica de la entidad, acorde con el anexo 1 de la Resolución 1519 de 2020.	POL10
Gobierno Digital	Generar y actualizar los conjuntos de datos abiertos propios de la entidad.	POL10
Gobierno Digital	Utilizar tecnologías emergentes de la cuarta revolución industrial para desarrollar procesos de innovación pública digital en la entidad, tales como tecnologías de desintermediación, DLT (Distributed Ledger Technology) como cadena de bloques (Blockchain) o contratos inteligentes; análisis masivo de datos (Big data); Inteligencia Artificial (AI); Internet de las Cosas (IoT); robótica y similares; realidad aumentada o realidad virtual; automatización robótica de procesos; entre otras.	POL10
Gobierno Digital	Utilizar los Acuerdos Marco de Precios (AMP) o Instrumentos de Agregación de demanda (IAD) disponibles en la Tienda Virtual del Estado Colombiano (TVEC); las grandes superficies disponibles en la Tienda Virtual del Estado Colombiano (TVEC); entre otras modalidades de adquisición de productos, bienes y servicios de TI en la entidad.	POL10

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA RECOMENDACIONES FURAG VIGENCIA 2024		
Entidad		
3539	**HOSPITAL REGIONAL DE MONIQUIRA**	**BOYACA**
Política	**Recomendación**	**Índice**
Gobierno Digital	Realizar auditorías internas, externas y de certificación o recertificación respecto al estándar ISO 27001 en la entidad.	POL10
Gobierno Digital	Formular, aprobar en el Comité de Gestión y Desempeño Institucional, incluir en el Plan Estratégico de Tecnologías de la Información de la entidad y ejecutar proyectos de transformación digital.	POL10
Gobierno Digital	Disponer en línea los Otros Procedimientos Administrativos (OPAS) de la entidad inscritos en el Sistema Único de Información de Trámites (SUIT).	POL10
Gobierno Digital	Implementar estrategias de mejora de los trámites totalmente en línea de la entidad para aumentar el número de usuarios satisfechos con su uso.	POL10
Gobierno Digital	Implementar estrategias de mejora de los trámites parcialmente en línea de la entidad para aumentar el número de usuarios satisfechos con su uso.	POL10
Gobierno Digital	Digitalizar los trámites inscritos por la entidad en el Sistema Único de Información de Trámites (SUIT).	POL10
Gobierno Digital	Automatizar los trámites inscritos por la entidad en el Sistema Único de Información de Trámites (SUIT).	POL10
Gobierno Digital	Implementar el servicio de autenticación digital de los Servicios Ciudadanos Digitales en todos los trámites de la entidad que requieran verificar la identidad de sus usuarios.	POL10

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA RECOMENDACIONES FURAG VIGENCIA 2024		
Entidad		
3539	**HOSPITAL REGIONAL DE MONIQUIRA**	**BOYACA**
Política	**Recomendación**	**Índice**
Gobierno Digital	Usar el servicio de Carpeta Ciudadana Digital para que la entidad reduzca el el número de PQRSD, reduzca los tiempos de respuesta de los trámites, reduzca el consumo de papel necesario para dar respuesta a los trámites, entre otros.	POL10
Gobierno Digital	Establecer instancias/dependencias de toma de decisiones sobre la implementación de la Política de Gobierno Digital en la entidad, tales como el Comité de Gestión y Desempeño Institucional, la Oficina de Tecnologías de Información, la Oficina de Planeación, entre otras.	POL10

Las recomendaciones emitidas por el Departamento Administrativo de la Función Pública (DAFP) en el marco del FURAG vigencia 2024, asociadas al índice POL10 – Gobierno Digital, evidencian que el Hospital Regional de Moniquirá ESE se encuentra en una fase de desarrollo intermedia, con avances importantes en la planeación y formulación de lineamientos, pero con brechas significativas en ejecución, articulación y madurez tecnológica.

El volumen y alcance de las recomendaciones reflejan que la Política de Gobierno Digital no se encuentra plenamente institucionalizada como un eje estratégico transversal, sino que aún opera de manera fragmentada entre componentes tecnológicos, de seguridad de la información, arquitectura empresarial, datos, trámites y servicios digitales.

El análisis de las recomendaciones FURAG asociadas a la Política de Gobierno Digital (POL10) evidencia que el Hospital Regional de Moniquirá ESE cuenta con estructuras formales, lineamientos y diagnósticos

definidos, pero con debilidades en su ejecución, articulación y sostenibilidad operativa.

En materia de gobernanza, existen instancias como el Comité de Gestión y Desempeño Institucional; sin embargo, estas no se han consolidado como mecanismos efectivos de liderazgo, priorización y seguimiento de la Política de Gobierno Digital. De igual forma, la Arquitectura Empresarial y la gestión de TI no han sido integradas como herramientas estratégicas, manteniéndose una gestión predominantemente operativa y reactiva.

En cuanto a seguridad y privacidad de la información, se observan avances normativos y documentales alineados con el MSPI; no obstante, persisten brechas en la implementación efectiva, el seguimiento, la generación de evidencias y la mejora continua, lo que limita su madurez operativa.

Respecto a la gestión y aprovechamiento de datos, la entidad se encuentra en una etapa inicial, sin una estrategia consolidada de gobierno de datos ni uso sistemático de analítica para la toma de decisiones y la innovación pública. De manera similar, la digitalización de trámites y servicios presenta avances incipientes, con bajo impacto en la experiencia ciudadana y una alta dependencia de procesos manuales.

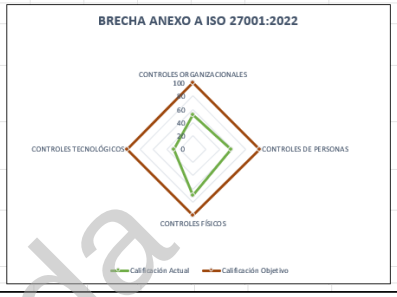
Adicionalmente, se identifican rezagos técnicos en accesibilidad web, interoperabilidad y adopción de IPv6, los cuales pueden afectar el cumplimiento normativo y la sostenibilidad de los servicios digitales.

De forma integrada, y en coherencia con el autodiagnóstico de Gobierno Digital, el MSPI, la norma ISO 27001:2022 y el NIST CSF, se concluye que la entidad se ubica en un nivel de madurez Básico – Intermedio, caracterizado por una planeación parcial, baja integración entre procesos, tecnología y estrategia, ejecución limitada y una transformación digital orientada principalmente al cumplimiento normativo.

Finalmente, el FURAG 2024 evidencia que el principal reto del Hospital Regional de Moniquirá ESE en Gobierno Digital no es normativo, sino estratégico y operativo. El desafío institucional consiste en integrar, priorizar y ejecutar de manera estructurada las recomendaciones, fortaleciendo la gobernanza, operacionalizando el MSPI, digitalizando efectivamente los trámites, aprovechando los datos y avanzando progresivamente en los componentes técnicos, con el fin de generar valor público y fortalecer la prestación de los servicios de salud.

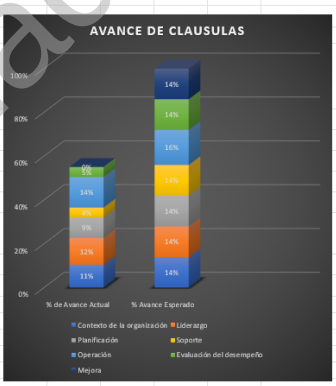
EVALUACIÓN DE EFECTIVIDAD DE CONTROLES – ISO 27001:2022 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	52	100	EFECTIVO
A.6	CONTROLES DE PERSONAS	58	100	EFECTIVO
A.7	CONTROLES FÍSICOS	70	100	GESTIONADO
A.8	CONTROLES TECNOLÓGICOS	29	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		52	100	EFECTIVO



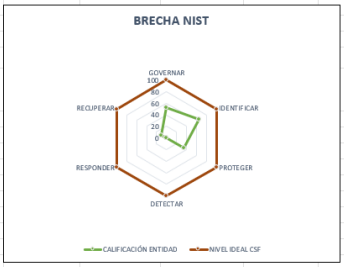
AVANCE CLÁUSULAS DEL MODELO DE OPERACIÓN (PHVA)

AÑO	COMPONENTE (PHVA)	CLAUSULAS	% de Avance Actual	% Avance Esperado
2025	Planificación	Contexto de la organización	11%	14%
		Liderazgo	12%	14%
		Planificación	9%	14%
		Soporte	4%	14%
	Implementación	Operación	14%	16%
	Evaluación de Desempeño	Evaluación del desempeño	5%	14%
	Mejora Continua	Mejora	0%	14%
TOTAL			55%	100%



CALIFICACIÓN FRENTE A MEJORES PRÁCTICAS EN CIBERSEGURIDAD (NIST)

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
GOVERNAR	52	100
IDENTIFICAR	64	100
PROTEGER	34	100
DETECTAR	0	100
RESPONDER	0	100
RECUPERAR	10	100



- Planificación Estratégica: Desarrollo de un plan estratégico que incluya la actualización y mejora continua de las tecnologías de la información, acorde con las necesidades identificadas.
- Capacitación del Personal: Formación continua del personal en el uso de las nuevas tecnologías y mejores prácticas en la gestión de sistemas.
- Monitoreo y Evaluación: Implementación de herramientas de monitoreo y evaluación para asegurar el cumplimiento de los estándares establecidos por el MinTic.

- Seguridad de la Información: Fortalecimiento de las medidas de seguridad de la información para proteger los datos sensibles y asegurar la confidencialidad y disponibilidad de los mismos.

8. PLAN DE ACCIÓN

ID	Actividad	Responsable	Indicador	Fecha de cumplimiento
1	Definición e implementación de indicadores del MSPI para seguimiento y control	Líder de Sistemas	Indicadores definidos y aprobados	**Febrero 2026**
2	Programa de concienciación y capacitación en Seguridad y Privacidad de la Información (planeación y cronograma)	Líder de Sistemas	Cronograma aprobado	**Febrero 2026**
3	Actualización general de los procedimientos de la Política de Seguridad y Privacidad de la Información	Líder de Sistemas	Procedimientos actualizados / requeridos	**Marzo 2026**
4	Definición e implementación del proceso de Gestión de Incidentes de Seguridad de la Información (incluye CSIRT / COLCERT)	Líder de Sistemas	Procedimiento implementado y socializado	**Marzo 2026**
5	Implementación de	Líder de Sistemas	Reportes de monitoreo	**Marzo 2026**

ID	Actividad	Responsable	Indicador	Fecha de cumplimiento
	capacidades básicas de monitoreo de eventos de seguridad (logs, firewall, accesos)		generados	
6	Implementar oráculos de información para alertas tempranas ante riesgos	Líder de Sistemas	Número de oráculos de monitoreo implementados	**Marzo 2026**
7	Análisis de vulnerabilidades en portal web, sede electrónica, sistemas expuestos, infraestructura On Premise y Nube	Líder de Sistemas	Informe de análisis de vulnerabilidades	**Marzo 2026**
8	Capacitación inicial del personal en Seguridad y Privacidad de la Información (ejecución)	Líder de Sistemas	Listados de asistencia	**Abril – Junio 2026**
9	Implementación de controles de acceso, autenticación y gestión de privilegios en sistemas críticos	Líder de Sistemas	Controles implementados	**Abril 2026**
1	Documentació	Líder de	Informe	**Abril 2026**

ID	Actividad	Responsable	Indicador	Fecha de cumplimiento
0	n y socialización de roles actuales y niveles de acceso de los usuarios	Sistemas	documentado y socializado	
11	Implementación de mecanismos para el cumplimiento de la Ley 1581 de 2012 (protección de datos personales)	Líder de Sistemas	Evidencias de implementación	**Abril 2026**
12	Formulación e implementación del Plan de Tratamiento y Mejora de Vulnerabilidades	Líder de Sistemas	Plan formulado y evidencias de ejecución	**Abril 2026**
13	Implementación del formato de aceptación de consultas SQL optimizadas	Líder de Sistemas	Formato aprobado por calidad	**Abril 2026**
14	Implementación de métodos de autenticación de correo electrónico (DMARC, DKIM, SPF)	Líder de Sistemas	Registros técnicos configurados	**Mayo 2026**
1	Verificación	Líder de	Informe de	**Mayo 2026**

ID	Actividad	Responsable	Indicador	Fecha de cumplimiento
5	del cumplimiento de requisitos de seguridad de la información por parte de proveedores y contratistas TI	Sistemas	verificación	
16	Identificación y gestión de riesgos de ciberseguridad en infraestructuras On Premise y servicios en la Nube	Líder de Sistemas	Informe de riesgos documentado	**Junio 2026**
17	Evaluación de conocimiento y efectividad del programa de capacitación	Líder de Sistemas	Informe de resultados	**Julio 2026**
18	Ejecución de pruebas básicas del Plan de Recuperación ante Incidentes de Seguridad de la Información	Líder de Sistemas	Informe de pruebas	**Julio 2026**
19	Seguimiento y medición de indicadores del MSPI	Líder de Sistemas	Informes de seguimiento	**Julio – Octubre 2026**
20	Elaboración del inventario	Líder de Sistemas	Inventario completo y	**Agosto 2026**

ID	Actividad	Responsable	Indicador	Fecha de cumplimiento
	de medios de transmisión de información		documentado	
21	Elaboración y consolidación del listado de proveedores TI	Líder de Sistemas	Inventario completo y documentado	**Agosto 2026**
22	Revisión del MSPI frente a autodiagnóstico y línea base	Líder de Sistemas	Informe comparativo	**Agosto 2026**
23	Retest de vulnerabilidades para verificar mitigación y aplicación de parches	Líder de Sistemas	Informe de retest	**Septiembre 2026**
24	Implementación de repositorios para almacenamiento y versionado de código fuente en sistemas propios	Analítica HRM	Cuenta privada de repositorio	**Septiembre 2026**
25	Formulación del BIA y Plan de Continuidad / DRP del proceso de TI	Líder de Sistemas	Informe BIA y DRP aprobados	**Octubre 2026**
26	Evaluación de madurez MSPI – NIST CSF – ISO/IEC	Líder de Sistemas	Informe de evaluación	**Octubre 2026**

ID	Actividad	Responsable	Indicador	Fecha de cumplimiento
	27001:2022			
27	Presentación de resultados y plan de mejora al Comité Institucional de Gestión y Desempeño	Líder de Sistemas	Acta de comité	**Noviembre 2026**
28	Monitoreo continuo de seguridad perimetral (Firewall)	Líder de Sistemas	Reportes generados	**Abril, julio y octubre 2026**

9. BIBLIOGRAFÍA

Archivo general de la nación: https://normativa.archivogeneral.gov.co/

Función pública – Gestor normativo: https://www.funcionpublica.gov.co/web/eva/gestor-normativo

10. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS			
Versión	**Descripción del Cambio**	**Aprobó**	**Fecha**

02	Actualización anual del plan	CIGYD	01-2026