TABLA DE CONTENIDO

1. INTRODUCCIÓN

El presente informe ha sido elaborado a solicitud de la Alta Dirección de la E.S.E. Hospital Regional de Duitama para revisar, analizar y clausurar la vigencia del Plan de Seguridad y Privacidad de la Información (PSPI) 2020-2024.[1] Con base en dicho diagnóstico, el objetivo central es establecer una estrategia robusta de Ciberresiliencia y cumplimiento normativo para el nuevo cuatrienio, proyectando el Plan de Seguridad y Continuidad de la Información para el periodo 2024-2028.

La E.S.E. ha reconocido la información como un activo crítico para la atención de pacientes y el desarrollo de sus procesos internos.[1] No obstante, el entorno actual del sector salud en Colombia exige una transformación desde un enfoque reactivo o de cumplimiento mínimo (Confidencialidad, Integridad y Disponibilidad - CIA) hacia una postura proactiva y de Resiliencia Operativa.[2] La creciente ola de ataques cibernéticos, especialmente de *ransomware*, dirigidos a infraestructuras sanitarias, pone en riesgo la operatividad de los servicios asistenciales y la confidencialidad de millones de historiales médicos.[3] Por lo tanto, la estrategia 2024-2028 debe enfocarse prioritariamente en la **Disponibilidad Asistencial** para garantizar la continuidad del servicio ante incidentes catastróficos. Este plan se enmarca en los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG) y busca la alineación con la Política de Gobierno Digital.[1]

1.1. Análisis de Cierre del Plan 2020-2024: Evaluación de la Ejecución

El Plan de Seguridad y Privacidad de la Información 2020-2024 definió un marco conceptual basado en estándares como ISO/IEC 27000 e ISO/IEC 27001:2013, así como en la normativa colombiana, incluyendo la Ley 1581 de 2012 para el tratamiento de datos personales.[1] La estrategia se estructuró en torno al ciclo de mejoramiento continuo PHVA (Planear, Hacer, Verificar y Actuar).[1]

Datos Clave del Cierre 2024 (Documento 2020-2024)

El análisis del portafolio de proyectos y el plan de acción revela que, si bien la Alta Dirección demostró su compromiso al establecer formalmente la Estrategia (Planear) y Priorizar iniciativas para los años 2021 y 2022 (Tabla 3) [1], la ejecución real de estos proyectos fue limitada.

El documento muestra que la fase de *Análisis y priorización de iniciativas* identificó 14 proyectos críticos, agrupados en la estrategia de seguridad de la información, gestión de riesgos, desarrollo del programa de seguridad y gestión de incidentes.[1] Sin embargo, la posterior revisión del *Portafolio de proyectos* (Tabla 2)

indica que una parte sustancial de las iniciativas priorizadas se encuentran en estado de "No iniciado" o "En proceso" al cierre de la vigencia.[1]

Detalle de las Brechas Críticas No Ejecutadas

La falta de ejecución en iniciativas clave representa una brecha de seguridad significativa al inicio del ciclo 2024-2028. Las iniciativas críticas no materializadas que comprometen la ciberresiliencia son:

- **Riesgo de Disponibilidad (Continuidad Asistencial) - Infraestructura:** La Iniciativa No. 8, referente a la Implementación de arquitecturas redundantes en dispositivos de seguridad (Firewall y Dispositivos de comunicaciones Core), fue priorizada para 2021, pero está marcada como "No iniciado" y requiere recursos financieros.[1] Este es un riesgo operativo inaceptable para una infraestructura hospitalaria, ya que un fallo de hardware o un ataque dirigido a un solo dispositivo podría paralizar completamente los servicios asistenciales críticos.
- **Riesgo de Disponibilidad (Continuidad Asistencial) - Planes de Recuperación:** Las iniciativas No. 6 y 7, relacionadas con el Diseño de los Planes de Continuidad del Negocio (BCP) que contemplen procesos críticos y la Documentación, Implementación y realización de pruebas de dichos planes, fueron prioritarias para el periodo 2022.[1] Al cierre, ambas figuran como "No iniciado".[1] La ausencia de un Plan de Recuperación ante Desastres (DRP) o BCP validado y probado anualmente incrementa la vulnerabilidad ante incidentes mayores, como ataques de *ransomware*.
- **Análisis de la Brecha de Backups vs. Redundancia:** Es importante destacar que la E.S.E. cuenta con un **Procedimiento de Copias de Seguridad** robusto.[1] Dicho procedimiento cumple con la **estrategia 3-2-1** (3 copias, 2 medios distintos, 1 copia externa/offsite) [1] y define la periodicidad (incrementales cada dos horas y totales semanales).[1] Crucialmente, el procedimiento exige **pruebas de restauración semanales**.[1] Por lo tanto, el riesgo de *pérdida total* de datos (Integridad) está mitigado por estos controles de copia. Sin embargo, el riesgo de **indisponibilidad por caída de hardware** (Inic. 8) y la falta de un **Plan de Continuidad Operativa (BCP/DRP)** probado y aprobado por la Alta Dirección (Inic. 6 y 7) implican que, aunque los datos se puedan recuperar, el **Tiempo Objetivo de Recuperación (RTO)** de la operación asistencial no está garantizado ni medido.
- **Riesgo de Gobernanza y Cultura:** La Iniciativa No. 3, sobre el diseño, documentación, implementación y evaluación del programa anual de capacitación y sensibilización sobre seguridad de la información, también requiere recursos financieros y se encuentra "No iniciado".[1] La falta de un programa continuo de cultura de seguridad mantiene la vulnerabilidad humana elevada, facilitando vectores de ataque como el *phishing* o la ingeniería social, que son comunes en el sector salud.[2]
- **Riesgo de Confidencialidad en Ambientes de Desarrollo:** La Iniciativa No. 9, que busca Definir un procedimiento formal para el tratamiento de información de producción en ambientes de desarrollo y prueba, también está "No iniciado".[1] Esto expone los Datos Personales Sensibles de los pacientes a riesgos de acceso no autorizado durante las etapas de desarrollo de *software*.

Análisis de Gobernanza y Financiamiento

El análisis de la ejecución sugiere una desconexión crítica entre el compromiso estratégico de la dirección y la asignación efectiva de recursos financieros y humanos. Si la planificación fue completada (Planear), y la priorización fue definida (Iniciativas 2021/2022), el incumplimiento de proyectos que explícitamente requieren inversión (Iniciativas No. 3 y No. 8) sugiere una **falla en el Eje de Ejecución (Hacer)** y la materialización del capital.[1] Esta situación es consistente con el desafío que enfrentan muchas organizaciones de salud que operan con presupuestos y personal limitados para la ciberseguridad.[2]

En consecuencia, el fracaso en la ejecución de la vigencia 2020-2024 no se debe primariamente a una ausencia de planificación, sino a la falta de *accountability* y la incapacidad de la Alta Dirección para asignar y desembolsar el capital necesario para transformar el riesgo aceptado en controles mitigados. Esta conclusión estratégica implica que el Plan 2024-2028 debe comenzar con una gestión prioritaria para asegurar el presupuesto de las iniciativas críticas no ejecutadas.

A continuación, se presenta un resumen de la evaluación de las brechas críticas:

Tabla 1: Matriz de Cierre de Proyectos Críticos 2020-2024 (Baseline 2024)

ID Iniciativa	**Descripción (Síntesis)**	**Prioridad 2021/2022**	**Estado Cierre 2024 (Estimado)**	**Impacto en Ciberresiliencia**	**Acción Inmediata 2024-2026**
Inic. 8	Arquitecturas Redundantes (Firewall/Core)	2021	No Iniciado (Requiere SI)	Crítico: Punto único de falla (SPOF) en la infraestructura central; falla en RTO.	Prioridad 1: Gestión de recursos financieros (CAPEX) y Adquisición.
Inic. 6 & 7	Planes de Continuidad (BCP/DRP) y Pruebas	2022	No Iniciado	Crítico: Riesgo de indisponibilidad asistencial total; RTO desconocido.	Prioridad 2: Diseño e Implementación inmediata.

Inic. 3	Programa de Capacitación y Sensibilización	2022	No Iniciado (Requiere SI)	Alta: Vulnerabilidad humana (Ingeniería Social, Phishing).	Prioridad 3: Implementación de la Fase de Cultura SGSI.
Inic. 9	Procedimiento de Uso de Datos en Desarrollo	N/A	No Iniciado	Alta: Exposición de Datos Sensibles (Ley 1581).	Prioridad 4: Implementación de Control A.8.11 (Data Masking).

2. OBJETIVO GENERAL Y ESPECIFICOS

Establecer e implementar una estrategia integral de Ciberresiliencia y Seguridad Digital que, alineada con la norma ISO/IEC 27001:2022 y el Modelo de Seguridad y Privacidad de la Información (MSPI), garantice la **Disponibilidad Asistencial Crítica**, la **Integridad** de los datos clínicos, y la **Confidencialidad** de los Datos Personales Sensibles, impulsando el Nivel de Madurez al rango de Administrado Fortalecido para 2028.

1. **Cerrar la Brecha de Disponibilidad (Respuesta y Recuperación):** Ejecutar y documentar la implementación de la arquitectura de alta disponibilidad (Inic. 8) y formalizar el Plan de Continuidad del Negocio (BCP/DRP) con pruebas anuales (Inic. 6, 7) en el bienio 2024-2026.
2. **Asegurar el Cumplimiento Normativo Avanzado (Transición ISO 2022):** Completar la transición formal a ISO/IEC 27001:2022 e implementar los nuevos controles de protección de datos sensibles (A.8.11 Data Masking y A.8.12 DLP) para fortalecer la Responsabilidad Demostrada (Ley 1581).
3. **Elevar la Madurez Institucional (MSPI):** Alcanzar el 90% (Rango Bueno) en el Indicador TIC02 MSPI para el dominio de Seguridad y Continuidad al cierre de 2028, alineándose con la meta sectorial.[10]
4. **Fortalecer la Cultura de Seguridad (Prevención):** Implementar y evaluar de manera continua el programa anual de capacitación (Inic. 3), integrando la gestión de seguridad en todos los procesos misionales (Inic. 2).

3. ALCANCE

El plan define los documentos institucionales y lineamientos de la estrategia de Seguridad y Privacidad de la Información de la E.S.E. Hospital Regional de Duitama, los cuales deben ser conocidos y cumplidos por empleados, contratistas, terceros y partes interesadas que tengan acceso, almacenen, procesen o transmitan información de la institución o sus pacientes.[1]

4. RESPONSABLES.

5. MARCO TEÓRICO.

6. MARCO NORMATIVO.

Marco Normativo y Estándares de Referencia: Actualización Crítica a 2024

La base normativa del Plan 2020-2024 incluyó la ISO/IEC 27001:2013 y la Guía v 3.0.2 del Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC.[1] Para el ciclo 2024-2028, se requiere una actualización crítica para garantizar la conformidad y la efectividad del SGSI.

Transición ISO/IEC 27001:2022

En octubre de 2022, se publicó una versión nueva y mejorada de la norma ISO/IEC 27001, con el fin de abordar los desafíos crecientes en ciberseguridad global y mejorar la confianza digital.[5] La E.S.E. debe iniciar formalmente el proyecto de transición del SGSI a la versión 2022, ya que los cambios incluyen la reestructuración de la numeración, la alineación con el enfoque armonizado de ISO, y la adición de una nueva cláusula crucial: Cláusula 6.3 – Planificación de cambios.[5] Esta cláusula exige que se garantice que la seguridad de la información se considere de manera explícita en todos los cambios operativos y de infraestructura.

Nuevos Controles de Seguridad de la Información (ISO/IEC 27002:2022)

Los cambios principales de la ISO/IEC 27001:2022 se centran en las actualizaciones del Anexo A, alineándose con la ISO/IEC 27002, que introduce nuevos controles técnicos y administrativos.[5] Tres de estos nuevos controles son de importancia crítica para la protección de datos sensibles en el sector salud:

1. **A.8.11 Enmascaramiento de Datos (*Data Masking*):** Este control tiene como propósito limitar la exposición de datos sensibles, incluyendo Información de Identificación Personal (PII), y garantizar el cumplimiento de requisitos legales y contractuales.[6] Este control es la herramienta técnica requerida

para solventar la Iniciativa No. 9 pendiente (manejo de datos en desarrollo).[1]

2. **A.8.12 Prevención de Fuga de Datos (*Data Leakage Prevention - DLP*):** Su objetivo es detectar y prevenir la divulgación y extracción no autorizada de información por parte de individuos o sistemas.[6] Este control es fundamental para proteger el gran volumen de historiales clínicos que maneja la E.S.E.
3. **A.7.4 Inteligencia de Amenazas (*Threat Intelligence*):** Este control es necesario para recolectar y analizar información sobre amenazas existentes, cambiando el enfoque de la entidad de ser reactivo a ser proactivo.[5]

Análisis de Riesgo Regulatorio

La E.S.E., al tratar datos personales sensibles (datos de salud), está sujeta a la Ley Estatutaria 1581 de 2012, cuyo objeto es desarrollar el derecho constitucional de conocer, actualizar y rectificar las informaciones recogidas en bases de datos.[8] La Iniciativa No. 9, referente al manejo seguro de información en ambientes de desarrollo y pruebas, ha estado pendiente.[1]

La no adopción de técnicas de Enmascaramiento de Datos (A.8.11), ahora formalizadas en el estándar internacional, implica un riesgo elevado de incumplimiento de las obligaciones de protección de confidencialidad de la Ley 1581. La falta de este control técnico necesario para gestionar la información de producción de manera segura en entornos no productivos podría ser interpretada como una falta de **Responsabilidad Demostrada** ante la Superintendencia de Industria y Comercio (SIC), lo que representa un riesgo legal y reputacional significativo. Por lo tanto, el control A.8.11 debe ser una prioridad de ejecución obligatoria en el nuevo plan.

Tabla 2: Síntesis de la Transición ISO/IEC 27001:2022 y su Impacto en la E.S.E.

Cambio Clave ISO 27001:2022	Relevancia Clínica (E.S.E.)	Estado en PSPI 2020-2024	Impacto Estratégico 2024-2028
A.8.11 Enmascaramiento de Datos	CRÍTICO: Protección de Historias Clínicas en entornos de desarrollo/pruebas.	No explicitado (Inic. 9 pendiente).	Implementación obligatoria para Ley 1581 y cumplimiento de confidencialidad.

A.8.12 Prevención de Fuga de Datos (DLP)	CRÍTICO: Evitar la exfiltración masiva de datos sensibles.	No explicitado.	Mitigación del riesgo de reputación y financiero por robo de datos.[2]
Cláusula 6.3 Planificación de Cambios	Asegura que la seguridad se considere en todos los cambios operativos.	Gestión de Cambios (PD-GT-2) existe, pero debe ser formalmente alineado.[4]	Fortalece la gestión del riesgo operativo y evita fallas de seguridad inadvertidas.[5]
A.7.4 Monitoreo de Amenazas	Fortalece la capacidad de prevención y detección proactiva.	No explicitado.	Esencial para la defensa contra Ransomware específico del sector.[3]

7. DIAGNÓSTICO Y/O SITUACIÓN ACTUAL

1.3. Diagnóstico MSPI y Contexto Sectorial 2024-2028: La Meta de Ciberresiliencia

Nivel de Madurez MSPI (Indicador TIC02)

El Plan 2020-2024 estableció el Indicador TIC02, Nivel de Madurez del Modelo de Seguridad y Privacidad de la Información (MSPI), como la métrica principal para la evaluación del plan, con una meta del 50% de construcción (rango "Intermedio").[1] Las fases que componen la construcción del modelo son: Diagnóstico, Planificación, Operación, Evaluación de Desempeño y Mejoramiento Continuo.[1]

Dado que proyectos esenciales que corresponden a las fases de Operación (implementación de redundancia) y Evaluación de Desempeño (pruebas de continuidad) quedaron sin iniciar [1], se estima que la E.S.E. se encuentra estancada en la transición de un nivel bajo de madurez (posiblemente Nivel 2 – Repetible [10]) hacia el Nivel 3 (Definido). El cumplimiento de los procedimientos existentes debe ser evaluado mediante el instrumento MSPI para obtener el dato exacto de la madurez.[4]

Meta Sectorial Estratégica

La Estrategia Nacional de Ciberseguridad de Colombia y los lineamientos sectoriales impulsan la mejora continua. El Ministerio de Salud y Protección Social (MSPS) ha definido una meta sectorial de alcanzar el

Nivel 4 – Administrado fortalecido para el dominio de Tecnología y Seguridad/Continuidad al año 2028.[10]

Para lograr el Nivel 4, la E.S.E. debe demostrar una gestión proactiva de la seguridad, donde los procesos sean medidos y monitoreados.[4] La información recopilada en la fase de diagnóstico debe servir como base para desarrollar estrategias efectivas, asegurando la triada CIA.[4]

Enfoque en Ciberresiliencia

Los datos analizados indican que la vulnerabilidad más grande del hospital es la **Disponibilidad Asistencial**, debido a la ausencia de infraestructura redundante (Inic. 8) y la falta de un plan de recuperación probado (Inic. 6 y 7).[1] Dado que los ataques de *ransomware* atacan directamente la disponibilidad de los datos y sistemas críticos [3], la principal función del SGSI 2024-2028 debe ser garantizar la **Continuidad Operativa**.[2]

Los proyectos de Resiliencia (Inic. 6, 7, 8) trascienden la esfera de TI y deben ser considerados **proyectos misionales de la Gerencia**. El marco de referencia para la Resiliencia Operativa debe alinearse con los pilares estratégicos de ciberseguridad definidos en el ámbito de la salud: **Prevención, Detección, Respuesta y Recuperación, y Disuasión**.[11]

Análisis de Estrategia y Prioridad de la E.S.E.

La Iniciativa 2 del plan anterior buscaba Definir e integrar la seguridad de la información en los procesos institucionales.[1] Esta integración es crucial, especialmente en un entorno hospitalario donde la información es la base del proceso asistencial. Un proceso clínico (como el registro de un paciente o la dispensación de medicamentos) sin seguridad de la información integrada es un proceso con riesgo misional.

Por lo tanto, la reactivación inmediata de la Iniciativa 2 debe ser el mecanismo primario para formalizar los riesgos identificados en el Plan de Tratamiento de Riesgos (Inic. 5), asegurando que los líderes clínicos entiendan cómo la falta de redundancia en TI o la caída de sistemas afecta directamente su capacidad de proveer servicios. La estrategia 2024-2028 debe priorizar la mitigación del riesgo de indisponibilidad para asegurar la función esencial de la E.S.E.

8. DEFINICIONES.

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Activos de información: Los activos de información son el resultado de la construcción de un inventario y clasificación de los activos que posee la entidad de acuerdo con la Política General de Seguridad y Privacidad de la información, la cual determina que activos posee la entidad, cómo deben ser utilizados, así como los roles y responsabilidades que tienen los funcionarios sobre los mismos. 1 en cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC27000).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Control: Es toda actividad o procesos encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas que pueden ser de carácter administrativo, técnico o legal y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: 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. (Decreto 1377 de 2013, art 3).

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: 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. (Decreto 1377 de 2013, art 3)

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Disponibilidad: Asegura que los usuarios autorizados pueden acceder a la información cuando la necesitan.

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Evento de seguridad de la información: Es la presencia identificada de un estado que indica un incumplimiento posible de la política de seguridad de la información, una falla de los controles de seguridad, o una situación desconocida que puede ser pertinente para la seguridad de la información.
Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Guía: Documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.

Incidente de seguridad de la información: Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de los activos de información. Los incidentes de seguridad de la información son hechos inevitables sobre cualquier ambiente de información, y estos pueden ser bastante notorios e involucrar un impacto fuerte sobre la información de la organización.

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, 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, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6) .

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 por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712
de 2014. (Ley 1712 de 2014, art 6).

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

MSPI: Modelo de Seguridad y Privacidad de la Información

Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Parte interesada: (Stakeholder) Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Propietario/responsable de activo de información: Individuo, entidad o unidad de negocio que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

Política: Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.

Procedimiento: Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.

Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Servicio: Es cualquier acto o desempeño que una persona puede ofrecer a otra que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC27000).

Usuario: Es el nombre (o alias) que se le asigna a cada persona para ser identificado por el servidor, de esta manera el proveedor de Internet o de correo electrónico lo identifica, es única en cada servidor, y cada usuario tiene asignado una contraseña para poder acceder a su cuenta.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

9. RECURSOS, MATERIALES, INSUMOS Y EQUIPOS.

10. DESARROLLO.

Riesgos Estratégicos y Enfoque del Plan de Tratamiento 2024-2028

El Plan de Tratamiento de Riesgos de Seguridad (Inic. 5) debe ser actualizado inmediatamente para reflejar las prioridades asistenciales y las amenazas cibernéticas modernas. La matriz de riesgos debe centrarse en los siguientes riesgos estratégicos y sus enfoques de tratamiento asociados:

- **Riesgo Estratégico 1: Indisponibilidad Crítica por Ransomware (Impacto Asistencial Máximo):** Este riesgo amenaza directamente la capacidad de la E.S.E. para atender a los pacientes. Aunque se cuenta con un procedimiento de backups robusto (regla 3-2-1 y pruebas semanales [1]), el tratamiento requiere priorizar la inversión en controles de Disponibilidad **Operativa** (Inic. 8, Inic. 6, 7) para reducir el RTO y reforzar los controles de Detección y Prevención (WAF Inic. 12, Gestión de Privilegios Inic. 10/11).
- **Riesgo Estratégico 2: Fuga Masiva de Datos Sensibles (Impacto Legal y Reputacional):** El robo de datos clínicos compromete la privacidad y expone a la E.S.E. a sanciones regulatorias. El

tratamiento se enfoca en controles de Confidencialidad y Trazabilidad, tales como la implementación de Data Masking (A.8.11), DLP (A.8.12) y el fortalecimiento de la Cultura de Seguridad (Inic. 3).

- **Riesgo Estratégico 3: Obsolescencia Normativa y Tecnológica (Impacto en la Gobernanza):** La falta de adaptación a nuevos estándares o tecnologías puede exponer vulnerabilidades no conocidas. El tratamiento incluye la ejecución del proyecto de Transición ISO 2022, la implementación del monitoreo de amenazas (A.7.4) y la revisión anual de la matriz de activos de información.[1]

Análisis del Efecto de Riesgo en el Hospital

La interconexión de los servicios sanitarios y el despliegue creciente de tecnologías digitales incrementan la superficie de exposición.[3] La E.S.E. ya identificó la necesidad de integrar la seguridad en los procesos institucionales (Inic. 2), buscando asegurar que los riesgos se identifiquen y traten como parte del proceso.[1]

El riesgo en el hospital no es solo técnico, sino misional. Por ejemplo, la falta de redundancia de TI (Inic. 8, pendiente) es la causa raíz de un riesgo asistencial: la imposibilidad de acceder a la historia clínica en caso de falla. La estrategia debe comunicar claramente que los proyectos de Resiliencia (Eje 1) son la inversión directa en la **mitigación del riesgo misional y la garantía de la continuidad asistencial**. El fracaso en la ejecución de estos proyectos impedirá la madurez del MSPI y, crucialmente, pondrá en peligro la vida del paciente.

Plan de Acción Detallado 2024-2028: Proyectos de Ciberresiliencia (Hacer)

El Plan de Acción 2024-2028 se construye sobre la base del Portafolio de Proyectos 2020-2024 pendiente [1], priorizando las iniciativas no ejecutadas (especialmente aquellas que afectan la Disponibilidad y la Confidencialidad) y alineándolas con los nuevos controles de la ISO 27001:2022. **Dado el momento actual (fines de 2026), la ejecución de los hitos críticos de 2024 debe estar en curso, y el enfoque pasa a la finalización en 2026.**

Eje 1: Resiliencia y Recuperación (Disponibilidad Asistencial)

Este eje busca cerrar las brechas críticas heredadas del ciclo anterior y asegurar la capacidad de la entidad para recuperarse de ataques, como el *ransomware*.

- **Proyecto 1.1: Implementación de Arquitecturas de Alta Disponibilidad (Inic. 8)**
  - **Justificación:** Eliminar el punto único de falla (SPOF) en la infraestructura de red central (Datacenter, Firewalls y Core Switches) mediante la adquisición e instalación de equipos redundantes.[1]
  - **Hitos 2024:** Aprobación presupuestal prioritaria (CAPEX), proceso contractual y gestión de la adquisición.[1] *(Nota 2025: Si esta adquisición no se materializó en 2024, debe ser la prioridad inmediata de la Alta Dirección en 2025.)*
  - **Hitos 2025:** Instalación física, configuración de redundancia activa-pasiva o activa-activa, y primeras pruebas de conmutación automatizada.
- **Proyecto 1.2: Diseño, Documentación y Pruebas BCP/DRP (Inic. 6 y 7)**
  - **Justificación:** Formalizar los planes de recuperación para procesos críticos, esenciales para la continuidad del negocio.[11]
  - **Hitos 2024:** Finalización del Análisis de Impacto en el Negocio (BIA) y documentación formal del Plan de Recuperación ante Desastres (DRP). Aprobación por la Alta Dirección.[1]
  - **Hitos 2025:** Ejecución del primer simulacro completo de recuperación, centrado en el escenario de indisponibilidad total de la Historia Clínica Electrónica, utilizando y validando el **Procedimiento de Copias de Seguridad** (3-2-1).[1] Generación de informes de lecciones aprendidas y ajuste del Plan de Continuidad.

Eje 2: Gobernanza y Cumplimiento Avanzado (Transición ISO/MSPI)

Este eje garantiza la sostenibilidad del SGSI, la alineación normativa y la gestión del riesgo cultural.

- **Proyecto 2.1: Transición SGSI a ISO/IEC 27001:2022 (Inic. 1 y 13)**
  - **Justificación:** Mantener la vigencia y relevancia del SGSI, incorporando los nuevos requisitos de planificación de cambios y controles avanzados.[5]
  - **Hitos 2024:** Realización de una Auditoría de Brecha (*Gap Analysis*) frente a la ISO 27001:2022. Actualización de la Declaración de Aplicabilidad (*SoA*).
  - **Hitos 2025:** Revisión y actualización del Manual de Seguridad y Privacidad de la Información.[4] Implementación formal de la Cláusula 6.3 (Planificación de cambios).
- **Proyecto 2.2: Implementación de la Cultura y Apropiación (Inic. 3)**
  - **Justificación:** Abordar la vulnerabilidad humana, que requiere recursos financieros.[1]
  - **Hitos 2024:** Diseño del programa anual de capacitación y ejecución del primer ciclo, enfocado en manejo de datos sensibles (Ley 1581) y simulación de *phishing*.[1] *(Nota 2026: Si el diseño no se completó, la ejecución inmediata del primer ciclo en 2026 es crítica).*

Eje 3: Controles de Prevención de Datos Sensibles (Ley 1581)

Este eje busca proteger la Confidencialidad de los activos de información, reforzando la Responsabilidad Demostrada.

- **Proyecto 3.1: Definición y Aplicación de Data Masking y DLP (Inic. 9 / A.8.11, A.8.12)**
  - **Justificación:** Cumplimiento de la Ley 1581 al garantizar que los datos sensibles se protejan mediante técnicas como el enmascaramiento en entornos de desarrollo (A.8.11) y la prevención de fuga en entornos operativos (A.8.12).[6]
  - **Hitos 2025:** Diseño del procedimiento formal para el uso de datos en desarrollo. Evaluación y adquisición de herramientas de Data Masking y DLP.
  - **Hitos 2026:** Implementación obligatoria del Data Masking en todos los entornos de pruebas. Despliegue de políticas DLP.
- **Proyecto 3.2: Implementación de WAF y Threat Intelligence (Inic. 12 / A.7.4)**
  - **Justificación:** Proteger las aplicaciones web de la E.S.E. de ataques externos y mejorar la capacidad de detección proactiva.[5]
  - **Hitos 2025:** Adquisición, configuración e implementación del *Web Application Firewall* (WAF) en los principales servicios de cara al ciudadano y al paciente.
  - **Hitos 2026:** Integración de la Inteligencia de Amenazas (A.7.4) en los procesos de gestión de incidentes.
- **Proyecto 3.3: Gestión de Identidades Privilegiadas (PIM) (Inic. 10 y 11)**
  - **Justificación:** Controlar el riesgo que representan los usuarios con altos privilegios de acceso a la infraestructura y bases de datos.[1]
  - **Hitos 2024:** Documentación y aplicación formal de políticas de gestión de usuarios privilegiados, asegurando la trazabilidad de las acciones.[1]
  - **Hitos 2026:** Evaluación de la necesidad de herramientas de *Privileged Identity Management* (PIM) para automatizar el control de acceso.

Análisis de Alineación Sectorial y Futura Inversión

La hoja de ruta propuesta para 2024-2028 equilibra la necesidad urgente de cerrar las brechas heredadas (Eje 1: Disponibilidad) con la implementación de controles avanzados de Prevención y Detección (Eje 3).

El énfasis en los primeros dos años en la **Respuesta y Recuperación** (Inic. 8 y 7) es un requisito estratégico para la supervivencia operativa de la E.S.E., dadas las tendencias de ciberataques en el sector salud.[2] Una vez asegurada la base de continuidad, la entidad puede invertir de manera más eficiente en Prevención avanzada (Data Masking, WAF) en los años subsiguientes (2026-2028). Este enfoque secuencial es crucial para el Nivel 4 del MSPI, que requiere que la entidad demuestre procesos bien definidos, medidos y sostenibles.[4]

Tabla 3: Portafolio de Proyectos Estratégicos 2024-2028 (Hoja de Ruta de Ciberresiliencia)

ID Eje	Proyecto (Iniciativa Original Ref.)	Prioridad	Recursos (SI/NO)	Vigencia 2024	Vigencia 2025	Vigencia 2026	Vigencia 2027-2028
Eje 1	Adquisición Redundancia (Inic. 8)	Crítica	SI	Aprobación/Contratación.	Instalación/Pruebas.	Operación Estándar.	Revisión Capacidad.
Eje 1	Documentación/ Pruebas BCP/DRP (Inic. 6, 7)	Crítica	NO	BIA/RA, Documentación.	1er Simulacro (Validación de RTO y Backups [1]).	2do Simulacro/Ajuste.	Operación y Mantenimiento.
Eje 2	Transición ISO 27001:2022 (Inic. 1)	Alta	NO	Gap Analysis, Revisión Documental.	Implementación Nuevos Controles.	Auditoría Interna.	Operación Estándar.
Eje 3	Gestión de Accesos Privilegiados	Alta	NO	Política PIM, Monitoreo Ciclo de Vida.	Implementación de Herramienta.	Optimización.	Operación Continua.

	(Inic. 10, 11)						
Eje 3	Implementación WAF (Inic. 12)	Alta	SI	Evaluación de Ofertas.	Adquisición e Instalación.	Puesta en Producción/Monitoreo.	Optimización.
Eje 3	Data Masking (Inic. 9 / A.8.11)	Alta	SI	Diseño de Solución /Política.	Adquisición e Implementación Piloto.	Expansión/Auditoría.	Operación Estándar.
Eje 2	Capacitación/Cultura (Inic. 3)	Alta	SI	Diseño y 1er Ciclo.	2do Ciclo, Medición de Apropiación.	3er Ciclo, Revisión de Metodología.	Operación Continua.

Mantenimiento, Auditoría y Mejoramiento Continuo (Actuar)

La mejora continua (fase final del ciclo PHVA) requiere que los resultados de la medición se traduzcan en acciones correctivas y preventivas.[4]

- **Auditoría del SGSI:** Se debe establecer un Plan de Ejecución de Auditorías anual [4], evaluando la eficacia de los nuevos controles (ISO 27001:2022) y la trazabilidad del dato sensible. La auditoría interna debe ser una herramienta para identificar fortalezas y debilidades.[4]
- **Gestión de Incidentes:** Es crucial fortalecer el proceso de Gestión de Incidentes de Seguridad de la Información. Las *Lecciones Aprendidas* de los simulacros de BCP/DRP (Proyecto 1.2) y de los incidentes reales deben alimentar directamente los Planes de Mejoramiento (Planes de Mejoramiento Externo e Interno).[4]
- **Revisión por la Dirección:** La Alta Dirección debe formalizar la revisión trimestral del desempeño del SGSI. Esta revisión no solo debe enfocarse en la madurez documental, sino principalmente en el

avance de la ejecución de los proyectos críticos de Resiliencia (Eje 1) y los indicadores de disponibilidad asistencial (MTTR), asegurando que el ciclo de mejoramiento continuo se mantenga activo y eficiente.

Conclusión Ejecutiva

El Plan de Seguridad y Privacidad de la Información 2020-2024, aunque bien planificado, cerró con un déficit de ejecución en iniciativas críticas que ponen en riesgo la continuidad asistencial de la E.S.E. Hospital Regional de Duitama. La principal conclusión diagnóstica es que la entidad padece una **falla en la materialización de inversiones de seguridad**.[2]

El Plan de Ciberresiliencia 2024-2028 debe enfocarse de manera ineludible en el pilar de **Respuesta y Recuperación** durante el bienio 2024-2026, para cerrar la brecha de vulnerabilidad.

Recomendaciones Prioritarias 2024-2026 (Ejecución Inmediata):

1. **Aseguramiento Financiero Inmediato (Disponibilidad):** La Alta Dirección debe asignar y asegurar inmediatamente los recursos financieros necesarios para la Iniciativa No. 8 (Arquitecturas Redundantes).[1] Esta inversión debe ser tratada como un proyecto misional de mitigación de riesgo asistencial, dada la criticidad de eliminar el Punto Único de Falla en la infraestructura central.
2. **Implementación y Prueba de Continuidad:** Ejecutar el Análisis de Impacto en el Negocio (BIA) y documentar los Planes de Continuidad del Negocio (BCP/DRP).[1] El primer simulacro de recuperación debe completarse obligatoriamente en 2026, integrando la validación del procedimiento de backups existente [1], para medir el RTO y validar la capacidad de la E.S.E. de resistir y recuperarse de un ciberataque.
3. **Alineación Normativa y Protección de Datos:** Iniciar el proyecto de Transición a ISO/IEC 27001:2022 e implementar los controles de protección de datos sensibles (Data Masking A.8.11) para subsanar la Iniciativa No. 9 pendiente y cumplir con la Ley 1581 de 2012.

La ejecución exitosa de esta hoja de ruta permitirá a la E.S.E. asegurar la Disponibilidad Asistencial, cumplir con la meta sectorial de madurez MSPI al Nivel 4 en 2028 y fortalecer la confianza pública en un entorno digital de alta amenaza.

EVOLUCIÓN DEL DOCUMENTO: SÍNTESIS DE CAMBIOS Y ACTUALIZACIONES

A continuación, se presenta una evidencia de los cambios fundamentales realizados al "Plan de Seguridad y Privacidad de la Información Vigencia 2020-2024" original para su actualización y proyección al periodo **2024-2028**:

Elemento Revisado	**Documento Original (2020-2024)**	**Documento Actualizado (2024-2028)**	**Justificación y Proyección**
Vigencia y Enfoque	2020-2024. Enfocado en la triada CIA y el SGSI (MSPI).	**2024-2028**. Enfocado en la **Ciberresiliencia** y la **Disponibilidad Asistencial** Crítica.	Proyección requerida para el nuevo cuatrienio, priorizando la **Respuesta y Recuperación** debido al riesgo de *ransomware* en el sector salud.[3]
Estándar de Referencia	ISO/IEC 27001:2013.	**ISO/IEC 27001:2022**.	Actualización obligatoria para garantizar la vigencia del SGSI y alinearse con los nuevos desafíos de seguridad digital.[5]
Controles de Confidencialidad (Nuevos)	No explicitados.	Inclusión de **A.8.11 Enmascaramiento de Datos (Data Masking)** y **A.8.12 Prevención de Fuga de Datos (DLP)**.	Integración de los nuevos controles críticos para la protección de Datos Personales Sensibles y el cumplimiento de la Ley 1581 de 2012.[6]
Diagnóstico (Ejecución)	*Priorización de Proyectos* (Tabla 3) con iniciativas marcadas como "No iniciado" o "En proceso" para 2021/2022.[1]	**Análisis de Brechas Críticas No Ejecutadas** (Sección 1.1). Se identifican fallas en la materialización de la inversión (Inic. 8, 6, 7).	Se traslada el análisis del portafolio al diagnóstico de cierre para enfatizar las brechas no resueltas que heredan el nuevo plan 2024-2028.

Procedimiento de Backups	Se identificó la necesidad de Planes de Continuidad (Inic. 6 y 7) como "No Iniciado".[1]	Se integra la existencia de un **Procedimiento de Copias de Seguridad** (Regla 3-2-1, pruebas semanales).[1]	Se diferencia: la E.S.E. sí tiene backups robustos, pero le falta la **Redundancia Operativa (Inic. 8)** y la **Prueba de RTO** (Inic. 6/7) para garantizar la *continuidad* misional, lo cual sigue siendo el riesgo crítico.
Meta de Madurez MSPI (TIC02)	Meta de 50% de construcción (Rango "Intermedio").[1]	Proyección a **90%-100% (Nivel 4 – Administrado fortalecido)** para 2028 (Tabla 4).	Alineación con la meta estratégica del sector salud definida por el MSPS al año 2028.[10]
Hoja de Ruta	Plan de Acción 2022 detallado (Tabla 4).[1]	**Hoja de Ruta Estratégica 2024-2028** (Tabla 3) con priorización secuencial por Ejes (Resiliencia, Gobernanza y Controles).	Se proyectan las iniciativas críticas pendientes (Inic. 8, 6, 7, 3, 9) para su ejecución prioritaria en el bienio 2024-2026.

11. INDICADORES.

Evaluación, Medición y Mejora Continua (Verificar y Actuar)

La fase de evaluación es fundamental para medir la efectividad de los controles implementados y validar el avance hacia el nivel de madurez deseado.

4.1. Monitoreo y Medición del Desempeño (Indicadores - Inic. 14)

La Iniciativa No. 14, Implementar y monitorear los indicadores del sistema de gestión de seguridad de la información [1], debe ser reactivada y robustecida.

Indicador Estratégico Clave: TIC02 Nivel de Madurez MSPI

La meta para 2028 es alcanzar el **Nivel 4 - Administrado fortalecido**, lo cual se traduce en un Nivel de Madurez MSPI superior al 90% (Rango "Bueno").[10] La medición de este indicador se mantendrá anualmente, considerando las 5 fases del modelo (Diagnóstico, Planificación, Operación, Evaluación de Desempeño y Mejoramiento Continuo).[4] La formulación consiste en el número de fases completadas bajo los requisitos definidos dividido por 5.[1]

Indicadores Operacionales y de Valor

Para demostrar el valor de la inversión en ciberresiliencia, los indicadores deben ir más allá del cumplimiento documental y medir la **eficacia operativa y la reducción del riesgo asistencial** [12]:

- **Indicador de Eficacia del DRP:** Medición del Tiempo promedio de recuperación (*MTTR - Mean Time To Recovery*) para servicios misionales críticos (ej. Sistema de Historias Clínicas Electrónicas). Este valor se calculará durante los simulacros anuales.
- **Indicador de Resiliencia Financiera:** Porcentaje de proyectos con requerimientos financieros (CAPEX) ejecutados versus proyectos planeados.
- **Indicador de Cumplimiento de Controles Críticos:** Porcentaje de cumplimiento de los controles más relevantes de la ISO 27002:2022, como la implementación del control A.8.11 (*Data Masking*) y A.8.12 (*DLP*).

Análisis de Medición de Valor

La Alta Dirección requiere una justificación clara de la inversión realizada en seguridad, especialmente tras el incumplimiento del ciclo 2020-2024. La implementación de indicadores de desempeño en la gestión de seguridad de la información debe ser sencilla de expresar, leer e interpretar.[12]

El uso de métricas como el MTTR y el indicador de Resiliencia Financiera demuestra el Retorno de la Inversión (ROI) en seguridad. El MTTR cuantifica directamente la mejora en la capacidad de Respuesta y Recuperación (Eje 1), que es la principal preocupación misional del hospital. El indicador de Resiliencia Financiera mide la efectividad de la Gobernanza en la asignación y ejecución del presupuesto, cerrando la brecha identificada en el análisis de la vigencia anterior (Sección 1.1). Este enfoque fortalece el requisito de medición robusta para alcanzar el Nivel 4 del MSPI.

Tabla 4: Proyección y Metas del Indicador Estratégico TIC02 (Nivel de Madurez MSPI)

Vigencia	**Fase MSPI a Fortalecer**	**Nivel de Madurez (Meta TIC02)**	**Rango**	**Justificación Estratégica**
2024 (Diagnóstico)	Planeación, Operación	50% - 60%	Intermedio	Cierre de la documentación de Planeación y aseguramiento del presupuesto.
2025 (Implementación)	Operación, Evaluación	70% - 80%	Intermedio	Finalización de Inic. 8 (Redundancia) y primeras pruebas BCP/DRP.
2026 (Consolidación)	Evaluación de Desempeño	85% - 95%	Bueno	Implementación de controles técnicos avanzados (WAF, Data Masking) y auditoría interna ISO 2022.
2027-2028 (Mejora Continua)	Mejoramiento Continuo	90% - 100%	Bueno	Demostración de Resiliencia Operativa y alineación total

				con la meta sectorial 2028.[10]

12. BIBLIOGRAFÍA.

1. Plan de Seguridad y Privacidad de la Información 2022.pdf
2. Cyber Considerations 2025 - Sector Cuidado de la Salud - KPMG International, acceso: noviembre 27, 2025, https://kpmg.com/co/es/home/insights/2025/07/cyber-considerations-2025.html
3. Aprobada la Estrategia de Ciberseguridad del Sistema Nacional de Salud 2025-2028, acceso: noviembre 27, 2025, https://www.redseguridad.com/actualidad/ciberseguridad/aprobada-la-estrategia-de-ciberseguridad-del-sistema-nacional-de-salud-2025-2028_20251114.html
4. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ..., acceso: noviembre 27, 2025, https://www.scj.gov.co/sites/default/files/2024-10/Modelo%20de%20Seguridad%20y%20Privacidad%20de%20la%20Informaci%C3%B3n%20-%20MSPI.pdf
5. Actualización ISO 27001: 2022: todo lo que necesita saber - ISMS.online, acceso: noviembre 27, 2025, https://es.isms.online/information-security/everything-you-need-to-know-about-the-iso-27001-2022-standard-update/
6. ISO 27002:2022: The Full 93 Control Reference - High Table, acceso: noviembre 27, 2025, https://hightable.io/the-ultimate-guide-to-iso-27002-changes-2022/
7. ISO 27001:2022 Annex A 8.11 – Data Masking - ISMS.online, acceso: noviembre 27, 2025, https://www.isms.online/iso-27001/annex-a-2022/8-11-data-masking-2022/
8. Compilación Jurídica del MINTIC - Ley 1581 de 2012 - Normativa, acceso: noviembre 27, 2025, https://normograma.mintic.gov.co/mintic/compilacion/docs/ley_1581_2012.htm
9. Ley 1581 de 2012 - Gestor Normativo - Función Pública, acceso: noviembre 27, 2025, https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981
10. Plan Estratégico de Tecnologías de la Información – PETI Institucional (2024-2028) - Ministerio de Salud y Protección Social, acceso: noviembre 27, 2025, https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/OT/plan-estrategico-seguridad-informacion-sector.pdf
11. Plan de acción europeo sobre la ciberseguridad de los hospitales y los prestadores de asistencia sanitaria - Public Health - European Commission, acceso: noviembre 27, 2025, https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/european-action-plan-cybersecurity-hospitals-and-healthcare-providers_es
12. Lineamientos de Indicadores de Gestión de Seguridad de la Información - Gobierno digital, acceso: noviembre 27, 2025, https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401772_recurso_1.pdf

13. ANEXOS.

Control de Cambios			
Versión	**Fecha**	**Elaboro**	**Descripción del Cambio**
00	29/12/2020	Emerson González	Construcción del documento.
01	20/01/2022	Cristian Rincón Bosigas	Actualización del plan por cambio de vigencia.
01	04/10/2022	Cristian Rincón Bosigas	Actualización del formato del documento.
02	01/12/2025	Luis Gabriel Ramirez Nuñez	Actualización a documento y del modelo a la CIBERRESILIENCIA y aplicación de nuevas tecnologías para el 2025
03	07/01/2026	Luis Gabriel Ramirez Nuñez	Actualización a documento y del modelo a la CIBERRESILIENCIA y aplicación de nuevas tecnologías para el 2026.

*****Teniendo en cuenta que el documento "**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CIBERRESILIENCIA"** se ajusta a nueva estructura documental alineada a mapa de procesos institucional vigente, la versión se reinicia en 02.

Revisión y Aprobación		
Elaborado/Modificado por:	**Cargo:**	**Fecha:**
Luis Gabriel Ramírez Núñez	Líder de tecnologías y de la información T.I.	07/01/2026
Revisado por:	**Cargo:**	**Fecha:**
Nicolás Daniel Arévalo Rodríguez	Líder de Planeación y del Sistema Integrado de Gestión de Riesgos	28/01/2026
Iris Adriana Mojica Carvajal	Líder de Calidad y Acreditación	28/01/2026
Aprobado por:	**Cargo:**	**Fecha:**
Jairo Mauricio Santoyo Gutiérrez	Gerente	29/01/2026