HOSPITAL CIVIL DE IPIALES
EMPRESA SOCIAL DEL ESTADO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

CODIGO: MN - 0444
VERSION: 5
VIGENCIA: 29/01/2026
REVISIÓN: 29/01/2026

ELABORÓ	REVISÓ	APROBÓ
Robinson Proaño Quistial Líder gerencia de la información	Gabriela Chamorro Huertas Asesora de planeación	Eduardo Narváez Cujar Gerente
FECHA 29 – Enero - 2026	**FECHA** 29 – Enero - 2026	**FECHA** 29 – Enero - 2026

Tabla de contenido

1. INTRODUCCIÓN.

El Plan de Seguridad y Privacidad de la Información (PSPI) del Hospital Civil de Ipiales E.S.E. establece los lineamientos institucionales para la protección de la información y los datos personales, en especial los datos sensibles en salud, garantizando su confidencialidad, integridad, disponibilidad y privacidad.

El presente plan se estructura conforme al Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio TIC, y se articula con el Modelo Integrado de Planeación y Gestión (MIPG) y el Formulario Único de Reporte de Avances de la Gestión (FURAG), contribuyendo al fortalecimiento del control interno, la gestión del riesgo y la confianza de los grupos de valor.

2. OBJETIVOS.

OBJETIVO GENERAL.

Establecer el marco institucional para la gestión de la seguridad y privacidad de la información del Hospital Civil de Ipiales E.S.E., mediante la definición de políticas, responsabilidades, controles y acciones orientadas a la protección de los activos de información y al cumplimiento de la normativa vigente..

OBJETIVOS ESPECIFICOS.

- Gestionar los riesgos asociados a la seguridad y privacidad de la información en los procesos misionales, estratégicos y de apoyo.
- Garantizar la aplicación de los principios de confidencialidad, integridad y disponibilidad de la información.
- Proteger los datos personales y sensibles conforme a la Ley 1581 de 2012 y la normatividad aplicable al sector salud.
- Fortalecer la cultura institucional en seguridad de la información.
- Asegurar la continuidad de los servicios de información ante incidentes o eventos adversos.
- Articular la seguridad de la información con el MIPG, el FURAG y el Plan Estratégico de Tecnologías de la Información (PETI).

3. ALCANCE.

El PSPI aplica a:

- Todos los procesos institucionales (estratégicos, misionales y de apoyo).
- Todos los activos de información en medios físicos y digitales.
- Servidores públicos, contratistas, proveedores y terceros que tengan acceso a información del Hospital.
- Sistemas de información en salud, historias clínicas, bases de datos, infraestructura tecnológica y servicios de TI.RESPONSABLES**.**

4. EJES ESTRATÉGICOS TIC 2024–2028.

El siguiente cuadro indica las metas propuestas para lograr que la política de seguridad y privacidad de la información para que sea eficiente y en un proceso de mejora progresivo solvente las deficiencias encontradas en el autodiagnóstico realizado.

EJE ESTRATEGICO PLAN DE DESARROLLO	OBJETIVO ESTRATEGICO	FUENTE DE COMPROMISOS	DIMENSIONES DEL MIPG	POLITICA DE GESTION Y DESEMPEÑO INSTITUCIONAL	ALINEACION CON OTROS PLANES	PROCESO ASOCIADO	META	ACTIVIDADES PLANEADAS	
Realizar el diagnóstico de seguridad y privacidad de la información para la vigencia, constituyéndola a través de la herramienta de autodiagnóstico del modelo de seguridad y privacidad de la información (MSPI)	Incrementar los niveles de satisfacción del usuario y su familia mediante la prestación de servicios de salud con calidad, oportunidad, seguridad y humanización.	Plan de desarrollo institucional 2024-2028	Información con valores para resultados	Gobierno y seguridad digital	Acreditación, PETI, Plan de seguridad de la información	GESTION TIC	Lograr el 100% del diagnóstico de seguridad y privacidad de la información	P	Cronograma para el diagnóstico de seguridad y privacidad de la información
								H	Ejecutar el diagnostico de seguridad y privacidad de la información mediante la herramienta de autodiagnóstico del modelo de seguridad y privacidad de la información (MSPI)
								V	Revisión de cumplimiento de actividades propuestas
								A	Toma de decisiones de acuerdo a los hallazgos encontrados
Aprobación, implementación y actualización de la política de seguridad y privacidad	Incrementar los niveles de satisfacción del usuario y su familia mediante la prestación	Plan de desarrollo institucional 2024-2028	Información con valores para resultados	Gobierno y seguridad digital	Acreditación, PETI, Plan de seguridad de la información	GESTION TIC	Lograr el 100% de actualización de la política de seguridad y privacidad de la informació	P	Elaborar un cronograma de capacitaciones y difusión de la política de seguridad

de la información mediante el proceso de mejora continua	**de servicios de salud con calidad, oportunidad, seguridad y humanización.**						**n mediante el proceso de mejora continua**		y privacidad de la información para todos los colaboradores incluyendo los proveedores de servicios externos, contratistas y demás grupos de valor del hospital civil de Ipiales.
								H	Realizar capacitaciones y difusión de la política de seguridad y privacidad de la información para todos los colaboradores incluyendo los proveedores de servicios externos, contratistas y demás grupos de valor del hospital civil de Ipiales.
								V	Revisión de cumplimiento de actividades propuestas
								A	Toma de decisiones de acuerdo a los hallazgos encontrados
Implementar procedimientos de seguridad y privacidad de la	**Incrementar los niveles de satisfacción del usuario y su familia mediante**	**Plan de desarrollo institucional 2024-2028**	**Información con valores para resultados**	**Gobierno y seguridad digital**	**Acreditación, PETI, Plan de seguridad de la**	**GESTION TIC**	**Lograr Implementar en un 80% los procedimientos de seguridad y**	**P**	Teniendo en cuenta el diagnóstico de seguridad y privacidad

información aprobados y actualizados mediante un proceso de mejora continua	**la prestación de servicios de salud con calidad, oportunidad, seguridad y humanización.**				**información**		**privacidad de la información aprobados y actualizados mediante un proceso de mejora continua**		de la información mediante la herramienta de autodiagnóstico del modelo de seguridad y privacidad de la información (MSPI) analizar que procedimientos de seguridad y privacidad se pueden implementar conjuntamente con el comité de seguridad y confidencialidad de la información aprobado mediante resolución No 3626 de 7 de dic de 2023
								H	Implementar procedimientos de seguridad y privacidad de la información
								V	Revisión de cumplimiento de actividades propuestas
								A	Toma de decisiones de acuerdo a los hallazgos encontrados
Actualización de los activos de la información mediante el proceso	**Incrementar los niveles de satisfacción del usuario y su familia mediante**	**Plan de desarrollo institucional 2024-2028**	**Información con valores para resultados**	**Gobierno y seguridad digital**	**Acreditación, PETI, Plan de seguridad de la información**	**GESTION TIC**	**Lograr la actualización del 100% de los conjuntos de datos mínimos**	**P**	Elaborar un cronograma para la actualización de activos de la

de mejora continua	**la prestación de servicios de salud con calidad, oportunidad, seguridad y humanización.**						**que se publican en la página de datos abiertos mediante el proceso de mejora continua**		información vigencia 2025
								H	Realizar la actualización de activos de la información
								V	Revisión de cumplimiento de actividades propuestas
								A	Toma de decisiones de acuerdo a los hallazgos encontrados
Elaborar, aprobarlo e implementar un plan operacional de seguridad y privacidad de la información	**Incrementar los niveles de satisfacción del usuario y su familia mediante la prestación de servicios de salud con calidad, oportunidad, seguridad y humanización.**	**Plan de desarrollo institucional 2024-2028**	**Información con valores para resultados**	**Gobierno y seguridad digital**	**Acreditación, PETI, Plan de seguridad de la información**	**GESTION TIC**	**Lograr un 50% la elaboración, aprobación e implementación del plan operacional de seguridad y privacidad de la información**	**H**	Elaborar del plan operacional de seguridad y privacidad de la información
								H	aprobar del plan operacional de seguridad y privacidad de la información
								H	implementar del plan operacional de seguridad y privacidad de la información
								V	Revisión de cumplimiento de actividades propuestas
								A	Toma de decisiones de acuerdo a los hallazgos encontrados
Actualizar y aprobar los indicadore	**Incrementar los niveles de satisfacci**	**Plan de desarrollo institucion**	**Información con valores**	**Gobierno y seguridad digital**	**Acreditación, PETI, Plan de**	**GESTION TIC**	**Lograr el 100% de actualización y**	**P**	Analizar los indicadores que

s midiendo la eficiencia y eficacia del sistema de seguridad y privacidad de la información	**ón del usuario y su familia mediante la prestación de servicios de salud con calidad, oportunidad, seguridad y humanización.**	**al 2024-2028**	**para resultados**		**seguridad de la información**		**aprobación de los indicadores midiendo la eficiencia y eficacia del sistema de seguridad y privacidad de la información**		actualmente de tiene para verificar la eficiencia y eficacia del sistema de seguridad y confidencialidad de la información
								H	Elaborar la actualización de los indicadores que midan la eficiencia y eficacia del sistema de seguridad y confidencialidad de la información
									aprobación de los indicadores que midan la eficiencia y eficacia del sistema de seguridad y confidencialidad de la información
								V	Revisión de cumplimiento de actividades propuestas
								A	Toma de decisiones de acuerdo a los hallazgos encontrados

5. GOBIERNO Y RESPONSABILIDADES.

5.1 Estructura de gobierno.

La gestión de la seguridad y privacidad de la información se soporta en la siguiente estructura:

- Gerente: Responsable último del cumplimiento del PSPI.
- Comité Institucional de Gestión y Desempeño: Instancia de aprobación, seguimiento y toma de decisiones.
- Comité de Seguridad y Privacidad de la Información: Instancia técnica de apoyo y coordinación.
- Líder del Proceso de Gerencia de la información: Responsable de la implementación operativa del PSPI.
- Responsables de la Información: Dueños de los activos de información por proceso.
- Custodios de la Información: Encargados de aplicar los controles definidos.
- Usuarios de la información: Funcionarios y terceros que acceden a los activos conforme a su rol.

6. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Hospital Civil de Ipiales E.S.E. se compromete a proteger la información y los datos personales bajo su custodia, mediante la implementación de controles técnicos, administrativos y físicos que reduzcan los riesgos de seguridad, aseguren la continuidad de los servicios y garanticen el cumplimiento de la normativa vigente, en coherencia con la misión, visión y objetivos estratégicos institucionales. Esta política es de obligatorio cumplimiento para todos los servidores públicos, contratistas y terceros.

7. GESTIÓN DE ACTIVOS DE INFORMACIÓN.

La Entidad mantiene un Inventario de Activos de Información, el cual incluye información, software, hardware, servicios, recurso humano y otros activos relevantes.

Cada activo es clasificado según los criterios de:

- Confidencialidad
- Integridad
- Disponibilidad

La clasificación se realiza conforme a los niveles Alto, Medio y Bajo, permitiendo establecer la criticidad del activo y definir los controles de protección correspondientes.

Activos de la información:

El hospital Civil de Ipiales realizó el levantamiento de los activos de la información en base a lo solicitado en el logro “Definición del marco de seguridad y privacidad de la información y de los sistemas de información”, contenido el autodiagnóstico de la política de gobierno digital, buscando con lo anterior proteger la información frente a la posible materialización de riesgos que afecten su disponibilidad, confiabilidad e integridad de la misma.

En esta matriz se buscó caracterizar los siguientes ítems:

Información básica: identificador: Número consecutivo único que identifica al activo en el inventario

Proceso: Nombre del proceso al que pertenece el activo.

Nombre del activo: Nombre de identificación del activo dentro del proceso al que pertenece.

Descripción/observaciones: Es un espacio para describir el activo de manera que sea claramente identificable por todos los miembros del proceso.

Tipo: Define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores: Información, Software, Recursos humanos, servicio, hardware, otro.

Tipo	**Define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores.**
Información:	Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.
Software:	Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.
Recurso humano:	Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.
Servicio:	Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.

Hardware:	Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos.
Otros:	Activos de información que no corresponden a ninguno de los tipos descritos anteriormente pero deben ser valorados para conocer su criticidad al interior del proceso.

Ubicación: de qué forma se encuentra el activo que toma los siguientes valores: física, electrónica o física y electrónica

Detalles de la ubicación: se detalla el sitio excepto del activo por ejemplo en un servidor, un archivo, oficina de algún proceso etc.

Clasificación: Hace referencia a la protección de información de acuerdo a Confidencialidad, Integridad y Disponibilidad.

CRITERIOS DE CLASIFICACION		
CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
IPR INFORMACION PUBLICA RESERVADA	**(A) ALTA**	**(1) ALTA**
IPC INFORMACION PUBLICA CLASIFICADA	**(M) MEDIA**	**(2) MEDIA**
IP INFORMACION PUBLICA	**(B) BAJA**	**(3) BAJA**

NC NO CLASIFICADA	NC NO CLASIFICADA	NC NO CLASIFICADA

ALTA	**Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.**
MEDIA	**Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.**
BAJA	**Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.**

Justificación: Para cada valoración, describe el impacto que causaría la pérdida de la propiedad (Confidencialidad, Integridad y Disponibilidad), o el argumento del porque se asignó dicha valoración.

Criticidad: Es un cálculo automático que determina el valor general del activo, de acuerdo con la clasificación de la Información:

Propiedad: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente. Deben definir y revisar periódicamente las restricciones y clasificaciones del acceso.

Custodio: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario. (Para sistemas de información o información consignada o respaldada, generalmente es TI o para información física, los custodios pueden ser los funcionarios o

el proceso de archivo o correspondencia, el custodio generalmente se define donde reposa el activo original).

Acceso/usuarios: Son quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información.

Gestión/fecha de ingreso: Fecha de ingreso del activo de información en el inventario

Gestión/Fecha salida: Fecha de exclusión del activo de información del inventario.

Lo anterior va a permitir a la institución aplicar las siguientes actividades

- Verificar El nivel de entendimiento y aplicación de los lineamientos establecidos para garantizar la seguridad de la información en la Entidad u organismo.

- Aplicar medidas de seguridad implementadas para el procesamiento, acceso e intercambio de información.

- La evaluación continua y sistemática de los componentes.

- La identificación de desviaciones y la definición de acciones de mejora.

8. GESTIÓN DEL RIESGO DE SEGURIDAD Y PRIVACIDAD.

La gestión del riesgo se realiza conforme a los lineamientos del MSPI e ISO/IEC 27005, e incluye:

- Identificación de amenazas y vulnerabilidades.
- Análisis y valoración de riesgos.
- Definición e implementación del plan de tratamiento del riesgo.
- Articulación con el mapa de riesgos institucional y el MIPG.

En el Plan estratégico de tecnologías de la información se realizó un cuadro de identificación, análisis y valoración de riesgos relacionados con la seguridad, privacidad y disponibilidad de la información como se muestra en la siguiente tabla:

Riesgo institucional identificado	Probabilidad	Impacto	Proyecto PETIC que actúa como control
Pérdida, acceso indebido o daño de información	Alta (80%)	Económico / Reputacional	P4 – Seguridad de la Información
Fraude interno por uso indebido de información	Alta (80%)	Económico / Reputacional	P4 – Seguridad de la Información
Daño de hardware crítico	Alta (80%)	Continuidad del servicio	P8 – Infraestructura tecnológica

Riesgo institucional identificado	Probabilidad	Impacto	Proyecto PETIC que actúa como control
Indisponibilidad de sistemas asistenciales	Alta (80%)	Alto	P1 – HIS / P8 – Infraestructura
Reporte incorrecto de indicadores	Media (60%)	Estratégico	P6 – Tablero institucional / P7 – Analítica
Pérdida de historias clínicas físicas	Alta (80%)	Económico / Reputacional	P1 – HIS / P4 – Seguridad
Acceso indebido a historia clínica física	Alta (80%)	Económico / Reputacional	P4 – Seguridad / P1 – HIS
Fallas en comunicación institucional	Media (60%)	Reputacional	P5 – Trámites digitales / P9 – Web
Riesgos por incendios o inundaciones	Alta (80%)	Crítico	P4 – Continuidad / P8 – Infraestructura

Tabla de valoración de riesgos institucionales 2025.

9. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN.

El Hospital implementa controles orientados a:

- Control de accesos lógicos y físicos.
- Gestión de usuarios y contraseñas.
- Acceso remoto controlado.
- Copias de seguridad y recuperación de la información.
- Protección contra malware (antivirus corporativo).
- Seguridad en la infraestructura tecnológica.
- Gestión de proveedores y servicios de TI.

10. PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD.

El tratamiento de datos personales se realiza conforme a los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

Se establecen medidas reforzadas para la protección de datos sensibles en salud, incluyendo historias clínicas, conforme a la Resolución 1995 de 1999 y la Ley 1581 de 2012.

11. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Entidad cuenta con un procedimiento para:

- Reportar incidentes de seguridad.
- Evaluar su impacto.
- Aplicar acciones de contención y recuperación.
- Documentar lecciones aprendidas y acciones de mejora.

11.1 Objetivo.

Establecer el procedimiento para la identificación, reporte, análisis, respuesta, recuperación y cierre de los incidentes de seguridad y privacidad de la información que puedan afectar los activos de información del Hospital Civil de Ipiales E.S.E., garantizando la continuidad de los servicios, la protección de los datos personales y la mejora continua del Sistema de Gestión de Seguridad de la Información.

11.2 Alcance.

Este procedimiento aplica a todos los servidores públicos, contratistas, proveedores y terceros que utilicen, administren o tengan acceso a los activos de información de la Entidad, incluyendo sistemas de información en salud, infraestructura tecnológica, información física y digital.

11.3 Definición de incidente de seguridad de la información.

Se entiende por incidente de seguridad de la información todo evento real o potencial que comprometa o pueda comprometer la confidencialidad, integridad, disponibilidad o privacidad de la información, tales como:

- Acceso no autorizado a sistemas o información.
- Pérdida, robo o divulgación indebida de datos personales o sensibles.
- Infección por malware, ransomware u otro código malicioso.
- Fallas de infraestructura que afecten la disponibilidad de la información.
- Uso indebido de credenciales.
- Pérdida de información de los aplicativos institucionales.

11.4 Roles y responsabilidades.

- Usuarios: Reportar de manera inmediata cualquier evento o sospecha de incidente.
- Líder del Proceso de Gestión TIC: Recibir, registrar, analizar y coordinar la atención del incidente.
- Responsables de la Información: Apoyar la evaluación del impacto sobre los activos afectados.
- Comité de Seguridad y Privacidad de la Información: Analizar incidentes críticos y definir acciones estratégicas.
- Gerencia: Tomar decisiones cuando el incidente tenga impacto institucional alto.

11.5 Clasificación de los incidentes.

Los incidentes se clasifican según su impacto:

Bajo: No afecta la operación ni datos sensibles.

Medio: Afecta parcialmente la operación o información no sensible.

Alto: Compromete datos sensibles en salud, continuidad del servicio o genera impacto legal o reputacional.

11.6 Procedimiento de gestión de incidentes.

El procedimiento se desarrolla en las siguientes etapas:

Detección y reporte: El usuario identifica el incidente y lo reporta inmediatamente al área de Gestión TIC por los canales definidos.

Registro del incidente: Gestión TIC registra el incidente en el formato o herramienta definida, asignando un número de seguimiento.

Análisis y evaluación: Se determina el tipo de incidente, activos afectados, nivel de impacto y causa raíz preliminar.

Respuesta y contención: Se aplican acciones inmediatas para contener el incidente y reducir su impacto.

Recuperación: Se restauran los servicios y la información afectada, utilizando copias de seguridad u otros mecanismos.

Cierre y documentación: Se documentan las acciones realizadas, resultados y lecciones aprendidas.

Acciones de mejora: Se definen acciones correctivas y preventivas para evitar la recurrencia del incidente.

11.7 Notificación a autoridades.

Cuando el incidente involucre datos personales o sensibles y represente un riesgo significativo para los titulares, la Entidad evaluará la notificación a:

- Superintendencia de Industria y Comercio (SIC), conforme a la Ley 1581 de 2012.
- Otras autoridades competentes, cuando aplique.

11.8 Indicadores de gestión de incidentes.

- Número de incidentes reportados por periodo.
- Tiempo promedio de atención de incidentes.
- Porcentaje de incidentes cerrados.
- Número de incidentes recurrentes.

12. CAPACITACIÓN Y SENSIBILIZACIÓN.

Se implementa un plan anual de capacitación en seguridad y privacidad de la información dirigido a funcionarios, contratistas y terceros, con el fin de fortalecer la cultura organizacional y reducir los riesgos asociados al factor humano.

Tema	Objetivo de la capacitación	Población objetivo	Responsable	Modalidad	Periodicidad
Introducción a la Seguridad de la Información	Sensibilizar sobre la importancia de la seguridad de la información	Todo el personal	Gestión TIC	Presencial / Virtual	Anual
Protección de datos personales – Ley 1581	Garantizar el adecuado tratamiento de datos personales	Todo el personal	Gestión TIC / Jurídica	Virtual	Anual
Manejo de datos sensibles en salud	Prevenir el uso indebido de información clínica	Personal asistencial	Gestión TIC	Presencial	Anual
Gestión segura de contraseñas y accesos	Reducir riesgos de accesos no autorizados	Todo el personal	Gestión TIC	Virtual	Semestral

Phishing e ingeniería social	Reconocer y prevenir ataques de engaño	Todo el personal	Gestión TIC	Virtual	Semestral
Uso seguro del correo electrónico y equipos	Promover buenas prácticas tecnológicas	Todo el personal	Gestión TIC	Virtual	Anual
Gestión de incidentes de seguridad de la información	Capacitar en el reporte y manejo de incidentes	Todo el personal	Gestión TIC	Presencial / Virtual	Anual
Continuidad del servicio y copias de seguridad	Asegurar la disponibilidad de la información	Gestión TIC	Gestión TIC	Presencial	Semestral

12.1 Indicadores de gestión de incidentes y capacitaciones.

Nombre del indicador	Objetivo	Fórmula	Tipo de indicador	Frecuencia de medición	Meta	Fuente de información	Responsable
Incidentes de seguridad reportados	Medir la cantidad de incidentes de seguridad identificados en la entidad	Número total de incidentes reportados en el periodo	Eficacia	Mensual	100% de incidentes reportados	Formato FO Registro de incidentes	Gerencia de la información
Tiempo promedio de atención de incidentes	Medir la oportunidad en la atención de incidentes	Suma de tiempos de atención / Número de incidentes	Eficiencia	Mensual	≤ 48 horas	Registro de incidentes	Gerencia de la información
Incidentes cerrados	Medir el cierre efectivo de incidentes de	(Incidentes cerrados / Incidentes	Eficacia	Trimestral	≥ 95%	Registro de incidentes	Gerencia de la información

	seguridad	reportados) x 100					

Nombre del indicador	Objetivo	Fórmula	Tipo de indicador	Frecuencia de medición	Meta	Fuente de información	Responsable
Cobertura de capacitación en seguridad de la información	Medir el porcentaje de personal capacitado	(Personal capacitado / Personal total) x 100	Cobertura	Anual	≥ 90%	Listas de asistencia, PIC	Gestión TIC / Talento Humano
Ejecución del plan de capacitaciones	Verificar el cumplimiento del plan anual	(Capacitaciones ejecutadas / Capacitaciones programadas) x 100	Eficacia	Anual	100%	Plan de capacitaciones	Gestión TIC
Capacitaciones en datos personales	Verificar formación en protección de datos personales	(Capacitaciones ejecutadas / Capacitaciones programadas en datos personales) x 100	Eficacia	Anual	>=90 %	Registros de capacitación	Gestión TIC / Jurídica
Incidentes asociados a error humano	Medir impacto del factor humano	(Incidentes por error humano / Incidentes totales) x 100	Impacto	Anual	≤ 10%	Registro de incidentes	Gestión TIC

13. MARCO CONCEPTUAL (DEFINICIONES RELEVANTES).

- Constitución Política de Colombia (Art. 15): Define el derecho al Habeas Data (conocer, actualizar y rectificar información en bases de datos).
- Ley 1273 de 2009 (Ley de Delitos Informáticos): Modifica el Código Penal para tipificar conductas como el acceso abusivo, interceptación de datos y daño informático.
- Ley Estatutaria 1581 de 2012: Marco general para la Protección de Datos Personales en Colombia.
- Nota: Ten en cuenta el Proyecto de Ley 274 de 2025 (en curso hacia 2026) que busca actualizar esta ley con sanciones de hasta el 5% de ingresos operativos.
- Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública.
- Decreto 1078 de 2015 (DUR-TIC): Decreto Único Reglamentario del sector TIC. Es la "biblia" normativa de MinTIC.
- Decreto 338 de 2022: Establece los lineamientos para fortalecer la Gobernanza de la Seguridad Digital en Colombia y crea las instancias de coordinación nacional.
- CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital.
- Estrategia Nacional de Seguridad Digital 2025-2027: (Documento más reciente de MinTIC) Define la hoja de ruta para la ciber-resiliencia nacional y la protección de infraestructuras críticas.
- Resolución 500 de 2021 (MinTIC): Define los lineamientos y estándares para la Estrategia de Seguridad Digital y adopta oficialmente el MSPI (Modelo de Seguridad y Privacidad de la Información).
- Resolución 746 de 2022 (MinTIC): Fortalece el MSPI y define lineamientos adicionales de seguridad para las entidades públicas.
- Guía MSPI (Actualizada a ISO 27001:2022): El manual técnico de MinTIC que adapta los controles de la ISO al entorno público colombiano.
- Manual Operativo MIPG (Versión vigente): Específicamente la Dimensión 4 (Gestión con Valores para Resultados) donde reside la Política de Gobierno Digital, y la Dimensión 7 (Control Interno).

14. MARCO NORMATIVO.

- Anexo 1 - Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública
- Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública.

- Ley 57 de 1985 -Publicidad de los actos y documentos oficiales.

- Ley 594 de 2000 - Ley General de Archivos.

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática.

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad.

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos.

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos.

- Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

- Decreto 2364 de 2012 - Firma electrónica.

- Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos.

- Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales.

- Ley 527 de 1999 - Ley de Comercio Electrónico.

- Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Ley Estatutaria 1581 de 2012 - Protección de datos personales.

- Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información.

15. BIBLIOGRAFÍA.

- MinTIC. (2022). Guía de Seguridad y Privacidad de la Información (Modelo de Seguridad y Privacidad de la Información - MSPI). Marco de referencia de la Política de Gobierno Digital.
- MinTIC. (2023). Guía para la Gestión de Riesgos de Seguridad de la Información. (Metodologías alineadas con la norma ISO 31000).
- Congreso de la República. Ley 1581 de 2012. Régimen General de Protección de Datos Personales.
- Congreso de la República. Ley 1712 de 2014. Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- Departamento Administrativo de la Función Pública (DAFP). Manual Operativo del Modelo Integrado de Planeación y Gestión (MIPG). Dimensión 7: Control Interno y Dimensión 4: Gestión con Valores para Resultados (Política de Gobierno Digital).
- DAFP. Lineamientos de la Política de Seguridad Digital. Dimensión de Gestión Tecnológica.
- Manual del Formulario Único de Reporte de Avance a la Gestión (FURAG). Sección correspondiente a la implementación del MSPI y cumplimiento de requisitos de seguridad digital.
- ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. (La norma certificable).
- ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. (La guía de buenas prácticas para implementar los controles del Anexo A).
- ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks.

- NIST Special Publication 800-53. Security and Privacy Controls for Information Systems and Organizations. (Muy útil para profundizar en controles técnicos específicos).
- Guía de Ciberseguridad para Entidades Públicas. (Publicada por el CSIRT de Gobierno o el Comando Conjunto de Ciberdefensa).