TABLA DE CONTENIDO

1. OBJETIVO

OBJETIVO GENERAL

Generar un documento institucional guiado en lineamientos de buenas prácticas en seguridad y Privacidad de la información en la E.S.E. Hospital Departamental Tomás Uribe Uribe.

OBJETIVO ESPECIFICO

• Promover el uso de mejores prácticas de seguridad de la información en la institución.

• Optimizar la gestión de la seguridad de la información al interior y hacia el exterior de la entidad.

• Aplicar de manera correcta la legislación relacionada con la protección de datos personales.

• Optimizar la labor de acceso a la información pública.

2. ALCANCE

El plan de Seguridad y Privacidad de la información aplica a todos los procesos de la institución los cuales manejen, procesen o interactúen con datos digitales y físicos tanto internamente como externamente en la institucional.

Este documento busca lograr la implementación en el Hospital Departamental Tomás Uribe Uribe las mejores prácticas dadas por el Departamento de Administrativo de la Función Pública con su estrategia MIPG y el Ministerio de las Tecnologías de la Información en el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información. El plan de Seguridad y Privacidad de la

Información, pretende lograr en la institución y sus clientes internos, externos y partes interesadas confianza en el manejo de la información garantizando para cada uno la privacidad, continuidad, integralidad y disponibilidad de los datos.

3.RESPONSABLE

• Coordinador de Sistemas.

• Profesional Universitarios de Calidad

• Ingenieros de Sistemas.

• Técnico en gestión documental.

• Oficina de estadística.

• Área de comunicación e imagen.

4. 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 de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

• **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.

• **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).

• **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).

• **Control:** Las políticas, 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. 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).

• **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).

• **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).

• **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).

• **Ley de Habeas Data**: Se refiere a la Ley Estatutaria 1266 de 2008.

• **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.

• **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.

• **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).

• **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.

• **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).

• **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).

• **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).

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

5. DESCRIPCIÓN

5.1 Articulación institucional de la seguridad y privacidad de la información

La implementación de la seguridad y privacidad de la información se desarrollará de manera articulada con los instrumentos institucionales establecidos para Gobierno Digital, seguridad digital, gestión de riesgos, gerencia de la información, protección de datos y gestión tecnológica.

La Política de Gobierno y Seguridad Digital establece las directrices institucionales el Manual de Seguridad Digital desarrolla los principales controles y buenas prácticas la Matriz de Riesgos y el Plan Institucional de Tratamiento de Riesgos de Seguridad y Privacidad de la Información orientan la identificación y tratamiento de los riesgos y el presente Plan establece las actividades generales para mantener y fortalecer su implementación.

5.2 Gestión de acceso y uso seguro de los recursos tecnológicos

La institución mantendrá mecanismos orientados al control de acceso a sistemas de información, redes y recursos tecnológicos, procurando que los accesos correspondan a las funciones y autorizaciones de cada usuario.

Las actividades relacionadas con creación de usuarios, asignación de perfiles, protección de credenciales, uso aceptable de recursos tecnológicos, instalación de software y demás controles asociados serán gestionadas conforme a las políticas, manuales, procedimientos y registros institucionales vigentes.

Los usuarios deberán cumplir las disposiciones contenidas en el Manual de Seguridad Digital, Compromiso de buen uso de tecnologia y seguridad digital y demás instrumentos aplicables.

5.3 Protección de la información y copias de seguridad

La información institucional deberá contar con medidas de protección acordes con su naturaleza y criticidad.

El Área de Sistemas de Información mantendrá mecanismos de respaldo de la información y servicios tecnológicos priorizados, de acuerdo con los procedimientos institucionales de copias de seguridad y continuidad.

La custodia, almacenamiento y recuperación de los respaldos se realizará conforme a los mecanismos tecnológicos disponibles y a las necesidades institucionales.

5.4 Seguridad de infraestructura y redes

Se mantendrán controles orientados a proteger la infraestructura tecnológica, servidores, redes, dispositivos de comunicaciones y demás componentes que soportan los servicios institucionales.

Estos controles podrán incluir mecanismos de seguridad perimetral, monitoreo, mantenimiento, actualización, segmentación, gestión de accesos, condiciones ambientales y renovación progresiva de infraestructura, de acuerdo con las necesidades y capacidades institucionales.

Las necesidades de fortalecimiento que requieran inversión serán gestionadas mediante los instrumentos de planeación tecnológica y presupuestal correspondientes.

5.5 Gestión de riesgos y vulnerabilidades

Los riesgos de seguridad y privacidad de la información serán gestionados de acuerdo con la Matriz de Riesgos institucional y el Plan Institucional de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Las vulnerabilidades identificadas mediante auditorías, proveedores tecnológicos, incidentes, actividades de monitoreo, revisiones internas u otras fuentes serán analizadas por el Área de Sistemas de Información para determinar su relación con los riesgos institucionales y establecer las acciones que correspondan.

Las evidencias de identificación, tratamiento y seguimiento se conservarán mediante los mecanismos definidos por el proceso de Sistemas de Información.

5.6 Gestión de incidentes de seguridad

Los eventos o incidentes que puedan afectar la confidencialidad, integridad o disponibilidad de la información deberán ser reportados al Área de Sistemas de Información mediante los canales institucionales disponibles.

El Área de Sistemas realizará el análisis inicial y aplicará las acciones de contención, recuperación, escalamiento o seguimiento que correspondan de acuerdo con la naturaleza del evento.

Cuando un incidente genere aprendizajes, cambios en controles o identificación de nuevos riesgos, se evaluará la necesidad de actualizar los instrumentos institucionales correspondientes.

5.7 Continuidad y recuperación

La institución mantendrá mecanismos orientados a reducir el impacto de fallas o interrupciones de los servicios tecnológicos que soportan los procesos asistenciales y administrativos.

Estos mecanismos se articularán con el Plan de Contingencia, los procedimientos de copias de seguridad y las actividades de mantenimiento y fortalecimiento de infraestructura tecnológica.

Las pruebas, simulacros o validaciones que se realicen permitirán identificar oportunidades de mejora para los mecanismos de continuidad existentes.

5.8 Sensibilización y cultura de seguridad

Se promoverán actividades de sensibilización y apropiación de buenas prácticas de seguridad y privacidad de la información dirigidas a colaboradores y demás partes interesadas.

Estas actividades podrán desarrollarse mediante inducciones, reinducciones, boletines, comunicaciones institucionales, compromisos de buen uso u otros mecanismos disponibles.

5.9 Seguimiento y mejora

El Área de Sistemas de Información realizará seguimiento a las actividades de seguridad y privacidad de la información mediante los mecanismos institucionales disponibles, considerando los resultados de la Matriz de Riesgos, incidentes, auditorías, reportes técnicos y demás fuentes de información relevantes.

Los resultados del seguimiento podrán generar acciones de mejora, actualización de controles, ajustes documentales o inclusión de necesidades dentro de la planeación tecnológica institucional.

6. DOCUMENTOS RELACIONADOS

- MD-DE-PO-046 Política de Gobierno y Seguridad Digital.
- MA-SI-MA-027 Manual de Seguridad Digital.
- MA-SI-PL-021 Plan Institucional de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- Matriz de Riesgos vigente – proceso de Sistemas de Información.
- MA-SI-MA-013 Manual de Gerencia de la Información.
- MD-DE-PO-036 Política de Gerencia de la Información.
- Política de Privacidad y Tratamiento de Datos Personales vigente.
- MA-GT-PL-005 Plan de Contingencia.
- MA-SI-PR-024 Procedimiento para Copias de Seguridad (Backup).
- MA-SI-PL-020 Plan Estratégico de Tecnologías de la Información – P **ETI.**

7. REGISTROS RELACIONADOS

- MA-SI-RE-020 Aviso de Privacidad y Tratamiento de Datos.
- MA-SI-RE-039 Lista de Chequeo Ronda de Seguridad – Sistemas.
- MA-SI-RE-046 Compromiso de Buen Uso de Tecnología Informática y Seguridad Digital.
- MA-SI-RE-017 Creación de Usuarios – Sistemas.

8. CONTROL DE CAMBIOS

Cambios: Se actualiza el Plan de Seguridad y Privacidad de la Información, fortaleciendo su articulación con la Política de Gobierno y Seguridad Digital, el Manual de Seguridad Digital, la Matriz de Riesgos y el Plan Institucional de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. Se actualizan los lineamientos relacionados con control de acceso, protección de la información, infraestructura tecnológica, gestión de riesgos y vulnerabilidades, incidentes de seguridad, continuidad, sensibilización y seguimiento. Asimismo, se actualizan responsables, definiciones, documentos y registros relacionados.

Justificación: Fortalecer la implementación y seguimiento institucional de la seguridad y privacidad de la información, articulando el Plan con los instrumentos vigentes de Gobierno Digital, gestión de riesgos y seguridad digital.

Elaboró:	Revisó:	Aprobó:
Sandra Patricia Vargas Garcia Coordinador de Sistemas	Andres Santacoloma Analista de Gestión de Procesos de Calidad Sandra Patricia Vargas Garcia Coordinador de Sistemas	Nini Yojana Renteria Angulo Coordinador de Calidad

Andres Santacoloma @ 2026-08-24, 9:45:17