



HOSPITAL SAN JUAN DE DIOS
Santa Rosa de Osos (Ant.)

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



CORPORACIÓN HOSPITAL
SAN JUAN DE DIOS - UNIREMINGTON
SANTA ROSA DE OSOS



PLAN DE SEGURIDAD Y PRIVACIDAD EN LA INFORMACION

CORPORACION HOSPITAL SAN JUAN DE DIOS – UNIREMINGTON, SANTA ROSA DE OSOS

INTRODUCCION

El Modelo de Seguridad y Privacidad de la Información se orienta hacia la preservación de la confidencialidad, integridad y disponibilidad de la información, asegurando al mismo tiempo la privacidad de los datos.

A través de la implementación de las Tecnologías de la Información y Comunicación (TIC) y el referido modelo de seguridad y privacidad de la información, se avanza en el fortalecimiento de la seguridad de los datos. El objetivo principal es garantizar la protección de la información y preservar la privacidad de los datos tanto de los ciudadanos como de los funcionarios de la entidad.

MARCO LEGAL

NORMA	TEMA
Ley 1712 de 2014, art 4	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.
(ISO/IEC 27000).	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.



Ley 594 de 2000, art 3	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.
-----------------------------------	---

NORMA	TEMA
Ley 1581 de 2012, art 3	Autorización Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales
Ley 1581 de 2012	Datos Personales Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
Decreto 1377 de 2013, 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.

1. OBJETIVO

La presente guía tiene como objetivo establecer lineamientos claros y efectivos en materia de seguridad y privacidad de la información para la CORPORACIÓN HOSPITAL SAN JUAN DE DIOS - UNIREMINGTON. La protección de la confidencialidad, integridad y disponibilidad de los datos es esencial para garantizar la privacidad de los ciudadanos y el adecuado funcionamiento de la entidad.



1.1 OBJETIVOS ESPECIFICOS

- Fomentar la adopción de las mejores prácticas en seguridad de la información, estableciéndolas como la piedra angular para la implementación del concepto de Seguridad Digital.
- Realizar una revisión exhaustiva de los roles vinculados con la privacidad y seguridad de la información dentro de la entidad, con el objetivo de optimizar su coordinación y funcionamiento interno.

2. DIAGNOSTICO

En la actualidad, la CORPORACIÓN HOSPITAL SAN JUAN DE DIOS - UNIREMINGTON dispone de un protocolo integral de seguridad de la información. Este protocolo abarca desde la custodia de los datos de los pacientes (clientes externos) hasta la protección de la información de nuestros empleados (clientes internos). Asimismo, se extiende a la gestión y resguardo de todo el material de apoyo y de trabajo de cada una de las dependencias que conforman la institución.

SITUACIÓN ACTUAL

ÁMBITO	SITUACIÓN ACTUAL
Diagnóstico de seguridad y Privacidad	Se cuenta con un inventario de equipos de cómputo, se tienen definidos procedimientos de almacenamiento de información y respaldo de soporte. También se cuenta con usuarios y contraseñas de la Institución.
Plan de Seguridad y privacidad	En la vigencia 2025, se crea y formaliza el plan de seguridad y privacidad de la información para las vigencias siguientes
Plan de Implementación	Se mantiene actualizada la declaración de aplicabilidad de la Corporación Hospital San Juan de Dios - Uniremington Santa Rosa de Osos Nit. 901249947-8 Carrera 28 26A - 34 Santa Rosa de Osos, Antioquia PBX 8605155 www.hospitalsantarosadeosos.gov.co



Gestión de Riesgos	Con el fin de garantizar la transferencia segura de datos de carácter personal requeridos por los entes de control y vigilancia en el marco de sus funciones misionales, se implementará el procedimiento de intercambio seguro de información
---------------------------	--

3. REPONSABLE

Líderes de Procesos

Todos los usuarios y/o funcionarios de la institución

4. FORMULACION DEL PLAN

La CORPORACIÓN HOSPITAL SAN JUAN DE DIOS - UNIREMINGTON, ubicada en Santa Rosa de Osos, integra en su modelo de gestión de calidad sistemas de información y comunicación como parte integral de los procesos de apoyo. Estos mecanismos se diseñan con un enfoque en la seguridad y privacidad de la información, considerándolos como elementos contingentes. Dichos sistemas proporcionan las herramientas necesarias para respaldar el presente plan, abarcando todos los aspectos relacionados con la seguridad y privacidad de la información.

HERRAMIENTAS DE APOYO

Disponemos de diversas alternativas de control y autocontrol aplicables a la seguridad y privacidad de la información, entre las cuales se incluyen:

- Respaldo externo de la información institucional.
- Herramientas de respaldo automático para los equipos de cómputo.
- Servidor de respaldo destinado a la copia de seguridad de todas las aplicaciones y plataformas instaladas en la institución.



5. ACTIVIDADES

- Llevar a cabo actividades preventivas de respaldo.
- Verificar la automatización de los procesos de respaldo para los equipos de cómputo.
- Verificar la automatización de los procesos de respaldo para los aplicativos o plataformas de información pertenecientes a la institución.

6. SEGUIMIENTO E IMPLEMENTACION

Según lo mencionado anteriormente, se describen las siguientes etapas y los plazos estimados para la implementación del presente plan:

- Revisión y/o Modificación del plan de Seguridad y Privacidad.
- Evaluación del Control de Acceso.



7. CRONOGRAMA Y HOJA DE RUTA

EJE	AREA	DESCRIPCIÓN	MARCO LEGAL	ENTREGABLE	E	F	M	A	M	J	J	A	S	O	N	D
transformación digital	Transferencia de información	Identificar los riesgos de seguridad digital y Diseñar los controles de seguridad necesarios para garantizar la seguridad digital y la protección de los datos personales en el marco de los acuerdos de intercambio de información de la entidad con otros	Decreto 2106/2018 Ley 1581/2012 PND Transformación Digital, Art 147	Matriz de riesgos de seguridad de la información para los convenios suscritos por la Entidad cargada en Sistema de Gestión Institucional												
	Seguridad para los Servicios ciudadanos digitales (sistemas digitales)	Documentar el manual de seguridad de la información para la protección de los datos personales en sistemas de información que realicen tratamiento de datos personales	Decreto 1377 de 2013, Ley 1581 de 2012	Manual Actualizado de protección de datos personales para sistemas de información con información de carácter personal												
Riesgos	Actualización de panorama de riesgos de seguridad digital	Acompañar los procesos institucionales en la identificación, valoración, evaluación y formulación de planes de tratamiento de riesgo de seguridad digital	Decreto 1078/2015, Política de gobierno Digital	Matriz de tratamiento de riesgos de seguridad Digital, cargados en sistema de gestión institucional												
Sensibilización	Planes de tratamiento de riesgos de seguridad Digital, cargados en sistema de gestión institucional	Apoyar las actividades realizar en las jornadas de inducción y reinducción de los funcionarios de la entidad con charlas en materia de seguridad de la información, protección de datos personales y controles del sistema de gestión	Plan nacional de desarrollo Art. 147 10. Inclusión de programas de uso de tecnología para participación ciudadana y Gobierno abierto en los procesos misionales de las entidades públicas.	Resultado de las charlas en seguridad de la información para directivos, servidores y contratistas												
Ciberseguridad - OTIC	Seguridad en puesto de trabajo	Apoyar técnicamente la implementación de soluciones de seguridad que protejan las estaciones de trabajo institucionales frente a software malicioso o fuga de información	Plan Nacional de desarrollo Art. 147. 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.	Implementación de controles de seguridad para asegurar estaciones de trabajo de usuario final												
	MINTIC	contar con información de punto de Contacto técnico con el Ministerio de las tecnologías de información y las comunicaciones en materia de seguridad Digital	Decreto 1078 de 2015, política gobierno digital	Informe de participación en actividades de seguridad digital adelantadas por MINTIC												



CONTROL DE CAMBIOS:

NUMERO DE VERSIÓN	TIPO DE MODIFICACIÓN	FECHA DE APROBACIÓN	ELABORADOR
01	Creación de documento	30 Enero 2024	Santiago Varela Macías
02	Actualización de documento	28 Enero 2025	Doria Ledy Rúfeles Toro

REVISIÓN Y APROBACIÓN DE LOS DOCUMENTOS:

PROYECTADO POR:	ELABORADO POR:	REVISADO POR:	APROBADO POR:
Yesenia Ruiz	Yesenia Ruiz	Carlos Andrés Pérez Lopera Juan Esteban Lopera Julieth Stephane Gil Salazar	Doria Ledy Rúfeles Toro
Aprendiz de calidad	Aprendiz de calidad	Subdirector administrativo y financiero. Subdirector Científico y Asistencial. Asesora de calidad	Director general