PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

MARCO CONCEPTUAL

La Seguridad y Privacidad de la Información se entiende como el conjunto de principios, lineamientos y acciones orientadas a proteger los activos de información de la entidad, garantizando su confidencialidad, integridad y disponibilidad. En el contexto institucional, la información constituye un activo estratégico indispensable para la prestación de los servicios de salud, la gestión administrativa y la toma de decisiones.

La privacidad de la información hace referencia a la protección de los datos personales y sensibles tratados por la entidad, especialmente aquellos relacionados con la información clínica y administrativa de los usuarios, asegurando su tratamiento conforme a la normativa vigente y a los principios de legalidad, finalidad, confidencialidad y responsabilidad.

El Plan de Seguridad y Privacidad de la Información se concibe como un instrumento de planeación que orienta la adopción de medidas administrativas, técnicas y organizacionales, promoviendo una cultura institucional basada en el uso responsable de la información y las tecnologías de la información.

INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información se concibe como un instrumento estratégico que se articula de manera directa con el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, el cual desarrolla de forma operativa las acciones orientadas a mitigar los riesgos identificados. Esta articulación permite asegurar coherencia entre la planeación estratégica y la gestión del riesgo, garantizando que las acciones definidas en el Plan respondan a escenarios reales de amenaza y vulnerabilidad que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional.

La integración entre ambos planes fortalece la gestión institucional de la seguridad de la información, evita duplicidad de esfuerzos y permite una respuesta coordinada frente a incidentes de seguridad, asegurando el cumplimiento de la normativa vigente y de los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG.

OBJETIVO

El objetivo del Plan de Seguridad y Privacidad de la Información debe alinearse con la gestión de riesgos institucional, reconociendo que la protección de la información solo es efectiva cuando se identifican, analizan y tratan los riesgos que puedan materializarse en incidentes de seguridad. Esta alineación garantiza que el Plan no se limite a acciones

preventivas aisladas, sino que contemple mecanismos de respuesta, mitigación y mejora continua frente a eventos que comprometan los activos de información.

Incorporar esta perspectiva permite que el Plan responda de manera integral a los riesgos asociados al entorno digital, fortaleciendo la resiliencia institucional y asegurando la continuidad de los servicios críticos del Hospital.

METAS

- Fortalecer la gestión de la seguridad y privacidad de la información institucional durante la vigencia del Plan.
- Promover el cumplimiento de los lineamientos y buenas prácticas en el manejo de la información.
- Garantizar la protección de los datos personales y sensibles tratados por la entidad.
- Contribuir a la continuidad de los servicios institucionales mediante la protección de los activos de información.

ALCANCE

El alcance del Plan establece los límites y cobertura de las acciones orientadas a la seguridad y privacidad de la información, determinando los procesos, activos, sistemas de información y actores involucrados. Definir claramente el alcance es fundamental para garantizar que la gestión de la seguridad de la información sea coherente con la estructura organizacional y con los procesos misionales y de apoyo del Hospital.

Este apartado permite evidenciar que la seguridad de la información no se limita a la atención de incidentes, sino que abarca desde la identificación de eventos hasta la documentación, análisis y mejora continua, tal como se desarrolla en el Plan de Tratamiento de Riesgos.

EVALUACIÓN DE NECESIDADES (DIAGNÓSTICO)

El diagnóstico de la seguridad y privacidad de la información evidencia la necesidad de fortalecer los mecanismos de protección de los activos de información, considerando el crecimiento en el uso de herramientas tecnológicas, la dependencia de los sistemas de información y la criticidad de los datos manejados por la entidad.

Así mismo, se identifica la necesidad de consolidar lineamientos institucionales que orienten el manejo adecuado de la información, la gestión de incidentes de seguridad y la articulación con los procesos de gestión del riesgo, con el fin de reducir vulnerabilidades y fortalecer la resiliencia institucional.

POBLACIÓN OBJETIVO

El presente Plan está dirigido a todos los funcionarios, contratistas, personal asistencial, administrativo y terceros que tengan acceso a la información, sistemas de información y recursos tecnológicos del Hospital Departamental San Antonio de Padua, quienes son responsables del uso adecuado y seguro de la información en el desarrollo de sus funciones.

ESTRATEGIA

La estrategia del Plan de Seguridad y Privacidad de la Información se fundamenta en la adopción de acciones preventivas y de fortalecimiento institucional orientadas a proteger la información como activo estratégico. Estas acciones se enfocan en la aplicación de lineamientos administrativos y técnicos que permitan reducir vulnerabilidades, fortalecer la cultura de seguridad de la información y asegurar el cumplimiento de la normativa vigente.

La estrategia contempla la articulación con otros instrumentos institucionales, especialmente aquellos relacionados con la gestión del riesgo, garantizando coherencia y complementariedad en la protección de la información.

ACTIVIDADES DEL PLAN

Actividad 1

- Realizar seguimiento y registro de los incidentes de seguridad de la información según su nivel de impacto.

Actividad 2

- Actualizar y hacer seguimiento a los requerimientos y creación de usuarios en los sistemas de información.

Actividad	Cómo se mide	Meta
Incidentes de seguridad	Registro por categoría	100% de incidentes registrados
Requerimientos y usuarios	Número de solicitudes atendidas	100% de solicitudes gestionadas

Las actividades definidas hacen parte del proceso de tratamiento y control de los riesgos asociados a la seguridad y privacidad de la información, cuyo objetivo es reducir la probabilidad de ocurrencia y el impacto de eventos que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información de la entidad.

La medición de estas actividades se realiza mediante indicadores de cumplimiento, dado que permiten verificar de forma objetiva la correcta gestión de los incidentes de seguridad de la información y el control de los accesos a los sistemas de información institucionales, los cuales constituyen riesgos críticos para la organización.

En relación con los incidentes de seguridad de la información, la medición se efectúa a través del registro y clasificación de cada evento según su nivel de impacto, lo cual garantiza la trazabilidad del riesgo, la identificación de tendencias y la definición de acciones de mitigación oportunas. Por esta razón, la meta establecida corresponde al 100% de los incidentes registrados, asegurando que todos los eventos asociados al riesgo sean debidamente tratados y documentados.

En cuanto a los requerimientos y creación de usuarios, la medición se basa en el número de solicitudes atendidas, debido a que la adecuada gestión de accesos es un control fundamental para mitigar los riesgos de acceso no autorizado, uso indebido de la información y vulneración de la privacidad. La meta del 100% de solicitudes gestionadas permite garantizar que todos los accesos sean autorizados, controlados y registrados conforme a los lineamientos de seguridad establecidos.

INDICADOR DE SEGUIMIENTO

ACTIVIDADES REALIZADAS/ ACTIVIDADES PROGRAMADAS X 100

PRESUPUESTO

La ejecución del Plan de Seguridad y Privacidad de la Información se realizará con los recursos asignados al área de Tecnologías de la Información y a los procesos institucionales responsables, de acuerdo con la disponibilidad presupuestal de la entidad para la vigencia correspondiente. Este enfoque garantiza la viabilidad del Plan y su alineación con la planeación financiera institucional.

CRONOGRAMA

El cronograma del Plan establece los periodos de ejecución de las actividades definidas, permitiendo su seguimiento y evaluación durante la vigencia. Las actividades se desarrollarán de manera semestral, facilitando la verificación de avances, la identificación de oportunidades de mejora y el cumplimiento de las metas propuestas.

ESTRUCTURA DEL PLAN O PROGRAMA

El Plan de Seguridad y Privacidad de la Información se estructura a partir de un diagnóstico institucional, la definición de objetivos y metas, el establecimiento de una estrategia general, la asignación de recursos, la programación de actividades y la evaluación de resultados. Esta estructura permite una implementación ordenada y coherente del Plan, facilitando su seguimiento y control.

EVALUACIÓN

La evaluación del Plan permitirá verificar el cumplimiento de las acciones y metas definidas, así como analizar su efectividad en la protección de la información institucional. Este proceso de evaluación constituye un insumo para la mejora continua y la toma de decisiones orientadas al fortalecimiento de la seguridad y privacidad de la información.

BENEFICIOS

La implementación del Plan de Seguridad y Privacidad de la Información contribuirá a la protección de los activos de información, al fortalecimiento de la gestión institucional y a la continuidad de los servicios. Así mismo, permitirá reducir la probabilidad de incidentes de

seguridad, fortalecer la confianza de los usuarios y asegurar el cumplimiento de la normativa vigente.

POLÍTICAS DE OPERACIÓN:

Los posibles incidentes de seguridad se reportarán al área de Sistemas a través de los siguientes canales:

- ✓ Enviando un mensaje de correo electrónico con la solicitud a la dirección sistemas@esesanantoniodepadua.gov.co
- ✓ Llamando al área de sistemas a la extensión 117.
- ✓ 8370149-8370163

El personal que identifique el posible incidente de seguridad debe reunir la información que llevó a determinar que es un posible incidente, el proceso se debe realizar durante los turnos y horarios establecidos para el desarrollo de sus actividades, donde la persona puede hacer uso de herramientas para recolección de información y reporte en la atención como, Ejemplo: capturas de pantalla, correos electrónicos, fotografías, videos entre otros.

Una vez se reciba el reporte del posible Incidente de seguridad, la mesa de servicio debe realizar la primera categorización en la herramienta que se maneja para iniciar con la atención de este, allí se generará los siguientes criterios básicos:

- ✓ Hubo daño o pérdida de información física o digital.
- ✓ Hubo fuga y/o robo de información física o digital.
- ✓ Hubo robo de credencias o información mediante Phishing.
- ✓ Se presentó modificación no autorizada de la información.
- ✓ Se presentó un comportamiento anormal del computador y/o sistema de información.
- ✓ Se presentó suplantación de identidad.
- ✓ Se presentó un acceso no autorizado.
- ✓ Se presentó pérdida o alteración de registros de base de datos.
- ✓ Se presentó una pérdida de un activo de información.
- ✓ Hubo presencia de código malicioso “malware”.
- ✓ Se presentó una denegación del servicio.
- ✓ Se presentó algún ciberataque.
- ✓ Uso indebido de imagen institucional.

Todos los incidentes de seguridad deberán estar registrados en la herramienta de gestión con la que tenga la E.S.E. Hospital Departamental San Antonio de Padua de La Plata Huila.

Una vez clasificado el incidente de seguridad procedemos a categorizarlo de la siguiente manera como se ve en la siguiente tabla.

Tabla 1: Impacto vs Valoración

		VALORACION
	Extremadamente Dañino: Si el hecho llegara a presentarse tendría desastrosas consecuencias o efecto sobre la institución a nivel de: • Pérdidas económicas superiores a 2000 SMLV. • Perdida de la infraestructura de la entidad. • Afectación imagen de la Institución. • Sanciones de contraloría, procuraduría y fiscalía.	**ALTO**
	Dañino mayor: Si el hecho llegara a presentarse tendría altas consecuencias o efecto sobre la institución a nivel de: • Pérdidas económicas entre 1501 a 2000 SMLV. • Perdida de la infraestructura de la entidad. • Afectación imagen de la Institución. • Sanciones de contraloría, procuraduría y fiscalía.	
	Moderado: Si el hecho llegara a presentarse tendría medianas consecuencias o efecto sobre la institución a nivel de: • Pérdidas económicas entre 1001 a 1500 SMLV. • Perdida de la infraestructura de la entidad. • Daños parciales de la infraestructura de la entidad. • Sanciones a nivel de oficina jurídica o control interno.	**MEDIO**

	Menor: Si el hecho llegara a presentarse tendría bajas consecuencias o efecto sobre la institución a nivel de: • Pérdidas económicas entre 501 a 1000 SMLV. • Daños pequeños de la infraestructura de la entidad. • Afectación imagen a nivel de grupo o área de proceso.	
	• Sanciones a nivel de proceso. **Ligeramente Dañino:** Si el hecho llegara a presentarse tendría mínimas consecuencias o efecto sobre la institución a nivel de: • Pérdidas económicas menores a 500 SMLV. • Daños pequeños de la infraestructura de la entidad. • Afectación imagen a nivel de grupo. • Sanciones a nivel de grupo.	**Baja**

Tabla 2: Urgencia

URGENCIA	DESCRIPCION
ALTO	El incidente de seguridad de la informacion debe antenderse de forma inmediata (0-120) minutos.
MEDIO	El incidente de seguridad de la informacion debe antenderse de forma inmediata (0-240) minutos.
BAJO	El incidente de seguridad de la informacion debe antenderse de forma inmediata (0-1440) minutos.

Para el caso de la atención de incidentes de seguridad de la información se han establecido unos tiempos máximos de atención de estos, con el fin de atender adecuadamente los incidentes de acuerdo con su criticidad e impacto. Los tiempos expresados en la anterior tabla son un acercamiento al tiempo máximo en que el incidente debe ser atendido, y no al tiempo en el cual el incidente debe ser solucionado. Esto se debe a que la solución de los incidentes puede variar dependiendo del caso.

Los equipos de respuesta que atiendan incidentes de seguridad, estarán conformados como mínimo por el propietario y/o custodio del activo, el profesional de la Dirección de Información y Tecnología que apoya la gestión de incidentes de seguridad de la información del Hospital San Antonio de Padua y demás profesionales de las Subdirecciones de Recursos Tecnológicos o Sistemas Integrados de Información que tengan a cargo activos o servicios que se vean afectados por el mismo, además del Oficial de Datos Personales de la Dirección de Planeación y Control de Gestión que participará si se ve afectada una base de datos con datos o información sensible. Para el caso de los incidentes de seguridad informática, el equipo de respuesta estará conformado por el propietario y/o custodio del activo, el profesional de la Subdirección de Recursos Tecnológicos que apoya la supervisión del servicio de seguridad informática, el profesional de la Subdirección de Recursos Tecnológicos que apoya la supervisión del servicio afectado, el Especialista de TI del proveedor de servicios de TI del servicio afectado, el Gestor Seguridad Informática del proveedor de servicios de TI y el Oficial de Seguridad de la Información del proveedor de servicios de TI.

Los equipos que se conformen podrán solicitar información o la participación de otros colaboradores, procesos, especialistas y/o operadores estratégicos requeridos para la atención del incidente de seguridad.

En caso que un incidente de seguridad de la información se considere **CATASTRÓFICO**, se deberá informar al Líder del Eje (Director(a) de Información y Tecnología) la ocurrencia de dicho evento, quien deberá informar a la alta gerencia (Dirección y Secretaría General) para la instalación de la mesa de crisis, en donde se analizará los recursos financieros, humanos y tecnológicos correspondientes a la atención de la emergencia, al igual evaluar las alternativas para la contención, erradicación y solución del incidente, a través de la activación del Plan de continuidad de la Operación del Hospital San Antonio de Padua.

3.6 Se deben conservar las evidencias recopiladas, con el fin de reducir la probabilidad de que estas se modifiquen después y sean consideradas no admisibles ante un ente judicial.

Dependiendo de la evidencia que se genere en el tratamiento del incidente, se determinará el lugar en donde se conservaran, por ejemplo: las evidencias producto de un incidente de seguridad de la información asociado a un ataque informático (Logs de auditoría) se almacenarán en un repositorio, el cual deberá cumplir unos requisitos mínimos de seguridad (Se determinarán de acuerdo con la clasificación de la información) para garantizar la integridad, disponibilidad y confidencialidad de esta. Se deberá seguir lo establecido en el "G5.GTI Guía de Recolección de Evidencias de Elementos Informáticos".

3.7 Para los incidentes de seguridad que el equipo de respuesta a incidentes y/o el profesional de la Dirección de Información y Tecnología que apoya la gestión de incidentes de seguridad de la información, consideren se postularan a la base de datos de conocimiento, se deberá seguir lo establecido en el "P10.GTI Procedimiento Gestión del Conocimiento Tecnológico".

3.8 En algunos casos la solución del incidente puede ser dada desde la contención del mismo, pero en otros requiere la recuperación o restauración del servicio a su estado normal de operación.

3.9 Los incidentes de seguridad con impacto Mayor o Catastrófico deben ser documentados en la herramienta de gestión de servicios y adicionalmente debe generarse un reporte independiente del mismo donde se evidencie las actividades realizadas de contención y solución.

3.10 En caso de que se presente un incidente de seguridad relacionados con base de datos con Datos o información sensible, deberá ser reportado a la Superintendencia de Industria y Comercio, por el Oficial de Datos a través del formato de F2.P5.GTI Reporte Incidentes Bases de Datos Personales Superintendencia de Industria y Comercio.

RESULTADO FINAL

Incidente de seguridad atendido, tratado y documentado.

DEFINICIONES

- **Activo crítico:** Son aquellos elementos o componentes que hacen parte de la infraestructura critica.

- **Activo de Información:** Se denomina activo a aquello que tiene valor para la organización y por lo tanto debe protegerse.

- **Analista de Mesa de Servicio:** Recibe la información de los Colaboradores del Hospital, registra los casos en la herramienta de mesa de servicio y es el primer contacto para la gestión de los incidentes de seguridad de la información.

- **Ataque informático:** Conjunto de actividades realizadas por atacantes para vulnerar la seguridad informática de un sistema.

- **Bases de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento. Para el caso del Hospital, son bases de datos toda la información que repose en Sistemas de Información Oficiales y que sean objeto de la Política de Tratamiento de Datos Personales Hospital San Antonio de Padua.

- **COC:** Comando Conjunto Cibernético, Unidad Militar Conjunta (Ejército, Armada y Fuerza Aérea), que tiene como función principal prevenir, detectar, orientar, contener, decidir, responder y recuperar ante amenazas cibernéticas que afecten la sociedad, la soberanía nacional, independencia, integridad territorial, el orden constitucional y los intereses nacionales, todo esto, soportado en un marco jurídico y/o la Constitución Nacional.

- **Ciberataque:** es cualquier tipo de maniobra ofensiva hecha por individuos u organizaciones que ataquen a sistemas de información como lo son infraestructuras, redes computacionales, o bases de datos que están albergadas en servidores remotos. Estas maniobras son realizadas por medio de actos maliciosos usualmente originados de fuentes anónimas y direcciones que no pueden ser rastreadas.

- **Ciberincidente:** Cualquier acto malicioso o evento sospechoso que: comprometa, o intente comprometer la Seguridad del perímetro electrónico, la Seguridad del primero físico o un activo crítico.

- **Ciberseguridad:** ISACA: Es el proceso de proteger activos de información por medio del tratamiento de amenazas para información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.

- **Código malicioso:** Conjunto de instrucciones o códigos informáticos que se inserta en los programas de computador, tiene la capacidad de auto replicarse y usualmente porta una carga útil que afecta el funcionamiento del computador, destruye datos, altera y pone en riesgo la información.

- **COLCERT:** Por las siglas en inglés de Computer Emergency Response Team, es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, y tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual estará enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de Ciberseguridad que atenten o comprometan la seguridad y defensa nacional.

- **Contención de un incidente:** Son todas aquellas actividades encaminadas a reducir el impacto inmediato de un incidente de seguridad.

- **CSIRT:** Por las siglas en inglés de Computer Security Incident Response Team, es el equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL, creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones.

- **Dato Personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales, tales como nombre, apellido, cedula, edad, color de ojos, estatura, fotografía o video de la persona, entre otros. Estos datos se pueden clasificar como dato público, sensible y semiprivado.

- **Dato Público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al nombre, 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, boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

- **Dato Semiprivado:** Datos que son de carácter privado, este tipo de datos sólo le interesan al titular y a un grupo determinado de personas. (Ej. Datos financieros, crediticios).

- **Datos Sensibles:** Son 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, así como los datos relativos a la salud, a la vida sexual, videos, fotografías, datos biométricos (huella dactilar, iris del ojo, pulsaciones cardiacas entre otros).

- **Denegación del servicio:** Conjunto de actividades desarrolladas por atacantes informáticos para degradar o interrumpir el normal funcionamiento de un sistema o servicio informático.

- **Entorno digital:** Ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web. (CONPES 3854, pág. 87).

- **Entorno digital abierto:** entorno digital en el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica. (CONPES 3854, pág. 87).

- **Equipo de Respuesta a incidentes:** Conformado por Colaboradores del Hospital Departamental San Antonio de Padua y/o terceros asociados (operadores estratégicos) que cuentan con las habilidades y competencias para tratar los incidentes de seguridad de la información durante el ciclo de vida de éstos.

Evento: Ocurrencia o cambio de un conjunto particular de circunstancias.

- **Evento de seguridad de la información:** Ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información o falla de los controles, o una situación desconocida que puede ser relevante para la seguridad. [ISO/IEC 27000:2009].

- **Incidente de seguridad informática:** Una violación o inminente amenaza de violación de las políticas de seguridad informática, políticas de uso aceptable o prácticas del estándar seguridad. En el contexto de este procedimiento, una inminente amenaza es definida como una situación en la cual la organización tiene evidencias para creer que un incidente de seguridad va a ocurrir.

- **Incidente de seguridad de la información:** Es un acceso, intento de acceso, uso, divulgación, modificación o destrucción de información no autorizada; además de un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información que atente contra la misionalidad de la institución.

- **Incidente digital**: Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos. (CONPES 3854, pág. 87).

- **Infraestructura Crítica (IC)**: Son las infraestructuras estratégicas cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. Adaptación Ley 8/2011-Gobierno de España.

- **NITS**: Es el proceso de proteger información a través de la prevención, detección y respuesta hacia ataques.

- **Oficial de Seguridad de la Información:** Designación dada a una persona para cumplir con los temas relacionados frente a la seguridad de la información.

- **Phishing**: Es un método que los ciberdelincuentes utilizan para engañar y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito, de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso.

- **Plan de continuidad de la operación (BCP. Business Continuity Plan):** Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.

- **Ransomware:** Piezas de código desarrolladas por atacantes informáticos para secuestrar información de los equipos infectados a través de técnicas criptográficas y posteriormente solicitar el pago de rescate para la recuperación de información.

RNBD: Registro Nacional de Bases de datos

- **Seguridad Digital:** Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de Ciberdefensa que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

- **Servicio Esencial:** El servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la educación, la seguridad, el bienestar social y económico de una comunidad, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas. Adaptación Ley 8/2011-Gobierno de España.

- **SIC:** Superintendencia de Industria Comercio.

➢ **SOC:** Centro de operaciones de seguridad donde se monitorea el estado de la seguridad informática a través de la gestión temprana de alertas y eventos.

➢ **Suplantación de identidad:** Todas aquellas actividades realizadas por la que una persona se hace pasar por otra para llevar a cabo actividades de carácter ilegal.

➢ **SDG:** Sede de la Dirección General.

➢ **SRT:** Subdirección de Recursos Tecnológicos.

➢ **Vulnerabilidad:** Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (CONPES 3854, pág. 87).

DOCUMENTOS DE REFERENCIA

- Guía técnica colombiana GTC-ISO/IEC 27035.
- Norma técnica colombiana NTC-ISO/IEC 27001.
- ISO/IEC 27000
- Documento CONPES 3854.
- NIST SP 800-53.
- G10.GTI Guía para el Desarrollo de Inventario y Clasificación de Activos.
- G3.MI Guía Gestión de Riesgos.
- P3.GTI Procedimiento Gestión de Cambios de Emergencia de Tecnologías de la Información.
- P4.GTI Procedimiento Gestión de Cambios de Tecnologías de la Información.
- P10.GTI Procedimiento Gestión del Conocimiento Tecnológico.
- P11.GTI Procedimiento de gestión de eventos y alertas.
- G5.GTI Guía de Recolección de Evidencias de Elementos Informáticos.
- 5482_G21 Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.

RELACIÓN DE FORMATOS

(LOS SIGUIENTES FORMATOS DEBEN SER REGISTRADOS Y DEBIDAMENTE APROVADOS POR LAURA INDICADORES)

CÓDIGO **NOMBRE DEL FORMATO**

MAG -GIT-AS-F-001 Formato de Requerimientos Solicitudes
MAG -GIT-AS-F-002 Formato de Requerimientos Creación de Usuario Dinámica Gerencial

MARCO NORMATIVO O LEGAL

El Plan de Seguridad y Privacidad de la Información se fundamenta en el conjunto de disposiciones constitucionales, legales y reglamentarias que regulan la protección de los datos personales, la seguridad digital, el acceso a la información pública y la gestión de las Tecnologías de la Información y las Comunicaciones (TIC) en las entidades públicas, en especial aquellas del sector salud. Este marco normativo establece las obligaciones, principios y lineamientos que orientan a la entidad en la adopción de medidas administrativas, técnicas y organizacionales para garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional.

Desde el ámbito constitucional, el Plan se sustenta en el reconocimiento del derecho fundamental a la intimidad, al buen nombre y al habeas data, así como en la obligación del Estado de proteger la información personal y garantizar su adecuado tratamiento. Estas disposiciones constituyen el fundamento jurídico para la implementación de políticas y planes orientados a la protección de la información y a la salvaguarda de los derechos de los titulares de los datos.

En el marco legal y reglamentario, el Plan se alinea con la normativa que regula el tratamiento de datos personales, la transparencia y el acceso a la información pública, la seguridad digital y la gestión de las tecnologías de la información en las entidades públicas. Dichas normas establecen responsabilidades claras para las entidades en cuanto al manejo, custodia y protección de la información, así como la obligación de adoptar medidas preventivas que minimicen los riesgos asociados a incidentes de seguridad de la información.

Adicionalmente, el Plan se articula con los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG), el cual incorpora la seguridad y privacidad de la información como un componente transversal de la gestión institucional. Esta articulación permite asegurar coherencia entre la planeación estratégica, la gestión del riesgo, el control interno y la mejora continua, fortaleciendo la gobernanza de la información dentro de la entidad.

NORMOGRAMA

El normograma del Plan de Seguridad y Privacidad de la Información constituye una herramienta fundamental para la identificación, organización y sistematización del marco

normativo que regula la gestión de la seguridad y privacidad de la información en la entidad. Su finalidad principal es facilitar la consulta, comprensión y aplicación de las disposiciones legales, reglamentarias y técnicas que soportan el Plan, asegurando que las acciones definidas se encuentren alineadas con la normativa vigente.

Este instrumento permite evidenciar de manera clara y estructurada el cumplimiento normativo por parte de la entidad, al relacionar las disposiciones jurídicas con los lineamientos, estrategias y actividades contempladas en el Plan. De esta manera, el normograma fortalece los procesos de seguimiento, control y auditoría institucional, al proporcionar una trazabilidad normativa que facilita la verificación del cumplimiento de las obligaciones legales en materia de seguridad y privacidad de la información.

El normograma contribuye igualmente a la gestión del riesgo legal, al permitir identificar de forma oportuna las normas aplicables y sus implicaciones para la entidad, reduciendo la probabilidad de incumplimientos normativos asociados al manejo de la información. Así mismo, se convierte en un instrumento de apoyo para los responsables de la implementación del Plan, quienes pueden consultar de manera ágil las normas que orientan la adopción de medidas administrativas, técnicas y organizacionales.

CONTROL DE REVISIÓN

VERSIÓN	FECHA	COMENTARIO
01		Actualización

Elaborado por: **Nombre: EDWIN FABIAN CASTRO QUINTERO** **Cargo:** Ingeniero de Sistemas Agremiado **Firma:**	**Fecha:**
Revisado por **Nombre: JOHN DAVID VILLA** **Cargo:** Apoyo Dinámica Gerencial **Firma**	**Fecha:**
Revisado por **Nombre: DIEGO FERNANDO MOMPOTES** **Cargo:** Apoyo Profesional Planeación **Firma**	**Fecha:**

Aprobado por: **Nombre: JOSÉ ANTONIO MUÑOZ PAZ** **Cargo:** Gerente **Firma**	**Fecha:**