



PLAN DE TRATAMIENTO DE RIESGOS DE
SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

EMPRESA SOCIAL DEL ESTADO
HOSPITAL SAN ANTONIO DE PADUA LA PLATA HUILA
PROCESO: GESTIÓN DE INFORMACIÓN Y
TECNOLOGÍAS

Fecha: 30/01/2025

Código: MAG-GIT-AS-PL-002

Versión: 06


Página: 1 de 14

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

DOCUMENTO CONTROLADO

— Salud Integral Impacto Real —

"Documento no valido en medio impreso sin la identificación de sello seco "Documento Controlado" Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital".

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Fecha: 30/01/2025
	EMPRESA SOCIAL DEL ESTADO	Código: MAG-GIT-AS-PL-002
	HOSPITAL SAN ANTONIO DE PADUA LA PLATA HUILA PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍAS	Versión: 06 Página: 2 de 14

INTRODUCCIÓN

Mediante la definición del Plan de Tratamiento de Riesgos se busca establecer medidas para mitigar los riesgos presentes en su análisis (pérdida de confidencialidad, pérdida de integridad y pérdida de disponibilidad de los activos de información) evitando situaciones que generen incertidumbre en el cumplimiento de los objetivos de la E.S.E Hospital Departamental San Antonio de Padua, lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3995 de 2020, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, a la Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital, establecidos en el Modelo Integrado de Planeación y Gestión

OBJETIVO


Revisar incidentes de seguridad y privacidad de la información, seguridad informática o seguridad digital, teniendo en cuenta los lineamientos y estándares definidos, a través de una oportuna identificación, atención y respuesta con el fin de mitigar el impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de la información de la E.S.E. Hospital Departamental San Antonio de Padua de La Plata Huila, adicional este plan esta enlazado por con nuevo plan de desarrollo institucional 2024 – 2028, donde comprende la carta de navegación junto con el PETI, en todo lo relacionado a la seguridad de la institución.

ALCANCE

La gestión de incidentes de seguridad inicia desde la identificación de un evento, detección, contención y solución de este, finalizando con la documentación y lecciones aprendidas. El documento aplica a nivel de la E.S.E. Hospital Departamental San Antonio de Padua de La Plata Huila.

— Salud Integral, Impacto Real —

"Documento no valido en medio impreso sin la identificación de sello seco "Documento Controlado" Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital".

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Fecha: 30/01/2025
	EMPRESA SOCIAL DEL ESTADO	Código: MAG-GIT-AS-PL-002
	HOSPITAL SAN ANTONIO DE PADUA LA PLATA HUILA	Versión: 06
	PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍAS	Página: 3 de 14

6. 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 credenciales 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.

— Salud Integral, Impacto Real —

"Documento no válido en medio impreso sin la identificación de sello seco "Documento Controlado" Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital".



PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

**EMPRESA SOCIAL DEL ESTADO
HOSPITAL SAN ANTONIO DE PADUA LA PLATA HUILA
PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍAS**

Fecha: 30/01/2025

Código: MAG-GIT-AS-PL-002

Versión: 06

Página: 4 de 14

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
<p>Extremadamente Dañino: Si el hecho llegara a presentarse tendría desastrosas consecuencias o efecto sobre la institución a nivel de:</p> <ul style="list-style-type: none">• Pérdidas económicas superiores a 2000 SMLV.• Perdida de la infraestructura de la entidad.• Afectación imagen de la Institución.• Sanciones de contraloría, procuraduría y fiscalía.	[Coloración oscura]
<p>Dañino mayor: Si el hecho llegara a presentarse tendría altas consecuencias o efecto sobre la institución a nivel de:</p> <ul style="list-style-type: none">• 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.	
<p>Moderado: Si el hecho llegara a presentarse tendría medianas consecuencias o efecto sobre la institución a nivel de:</p> <ul style="list-style-type: none">• 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

— Salud Integral, Impacto Real —

"Documento no valido en medio impreso sin la identificación de sello seco "Documento Controlado" Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital".



PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Fecha: 30/01/2025

**EMPRESA SOCIAL DEL ESTADO
HOSPITAL SAN ANTONIO DE PADUA LA PLATA HUILA
PROCESO: GESTIÓN DE INFORMACIÓN Y
TECNOLOGÍAS**

Código: MAG-GIT-AS-PL-002

Versión: 06

Página: 5 de 14


	<p>Menor: Si el hecho llegara a presentarse tendría bajas consecuencias o efecto sobre la institución a nivel de:</p> <ul style="list-style-type: none">• 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.	
	<ul style="list-style-type: none">• Sanciones a nivel de proceso. <p>Ligeramente Dañino: Si el hecho llegara a presentarse tendría mínimas consecuencias o efecto sobre la institución a nivel de:</p> <ul style="list-style-type: none">• 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
	El incidente de seguridad de la información debe atenderse de forma inmediata (0-120) minutos.
MEDIO	El incidente de seguridad de la información debe atenderse de forma inmediata (0-240) minutos.
BAJO	El incidente de seguridad de la información debe atenderse de forma inmediata (0-1440) minutos.

— Salud Integral, Impacto Real —

"Documento no válido en medio impreso sin la identificación de sello seco "Documento Controlado" Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital".

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Fecha: 30/01/2025
	EMPRESA SOCIAL DEL ESTADO HOSPITAL SAN ANTONIO DE PADUA LA PLATA HUILA PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍAS	Código: MAG-GIT-AS-PL-002
		Versión: 06 Página: 6 de 14

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.

— Salud Integral, Impacto Real —

"Documento no valido en medio impreso sin la identificación de sello seco "Documento Controlado" Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital".

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Fecha: 30/01/2025
	EMPRESA SOCIAL DEL ESTADO	Código: MAG-GIT-AS-PL-002
	HOSPITAL SAN ANTONIO DE PADUA LA PLATA HUILA	Versión: 06
	PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍAS	Página: 7 de 14

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 postularán 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.

— Salud Integral, Impacto Real —

"Documento no válido en medio impreso sin la identificación de sello seco "Documento Controlado" Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital".



PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

**EMPRESA SOCIAL DEL ESTADO
HOSPITAL SAN ANTONIO DE PADUA LA PLATA HUILA
PROCESO: GESTIÓN DE INFORMACIÓN Y
TECNOLOGÍAS**

Fecha: 30/01/2025

Código: MAG-GIT-AS-PL-002

Versión: 06


Página: 8 de 14

DEFINICIONES

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

— Salud Integral, Impacto Real —

"Documento no valido en medio impreso sin la identificación de sello seco "Documento Controlado" Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital".

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Fecha: 30/01/2025
	EMPRESA SOCIAL DEL ESTADO HOSPITAL SAN ANTONIO DE PADUA LA PLATA HUILA PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍAS	Código: MAG-GIT-AS-PL-002
		Versión: 06 Página: 9 de 14

➤ **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,

— Salud Integral, Impacto Real —

"Documento no válido en medio impreso sin la identificación de sello seco "Documento Controlado" Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital".



PLAN DE TRATAMIENTO DE RIESGOS DE
SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

EMPRESA SOCIAL DEL ESTADO
HOSPITAL SAN ANTONIO DE PADUA LA PLATA HUILA
PROCESO: GESTIÓN DE INFORMACIÓN Y
TECNOLOGÍAS

Fecha: 30/01/2025

Código: MAG-GIT-AS-PL-002

Versión: 06

Página: 10 de 14

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 cardíacas 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

— Salud Integral, Impacto Real —

"Documento no valido en medio impreso sin la identificación de sello seco "Documento Controlado" Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital".

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Fecha: 30/01/2025
	EMPRESA SOCIAL DEL ESTADO HOSPITAL SAN ANTONIO DE PADUA LA PLATA HUILA PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍAS	Código: MAG-GIT-AS-PL-002
		Versión: 06 Página: 11 de 14

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

— Salud Integral, Impacto Real —

"Documento no válido en medio impreso sin la identificación de sello seco "Documento Controlado" Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital".

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Fecha: 30/01/2025
	EMPRESA SOCIAL DEL ESTADO	Código: MAG-GIT-AS-PL-002
	HOSPITAL SAN ANTONIO DE PADUA LA PLATA HUILA PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍAS	Versión: 06 Página: 12 de 14

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 (ciberspacio), 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.

— Salud Integral, Impacto Real —

"Documento no valido en medio impreso sin la identificación de sello seco "Documento Controlado" Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital".



**PLAN DE TRATAMIENTO DE RIESGOS DE
SEGURIDAD Y PRIVACIDAD DE LA INFORMACION**

**EMPRESA SOCIAL DEL ESTADO
HOSPITAL SAN ANTONIO DE PADUA LA PLATA HUILA
PROCESO: GESTIÓN DE INFORMACIÓN Y
TECNOLOGÍAS**

Fecha: 30/01/2025

Código: MAG-GIT-AS-PL-002

Versión: 06

Página: 13 de 14

➤ **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).

7. 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.

8. 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

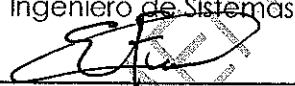
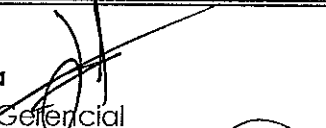
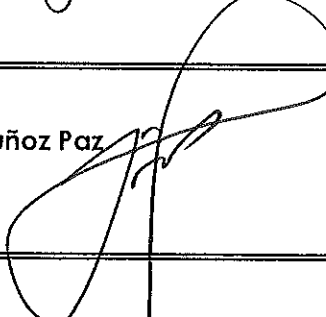
— Salud Integral, Impacto Real —

"Documento no válido en medio impreso sin la identificación de sello seco "Documento Controlado" Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital".

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	Fecha: 30/01/2025
	EMPRESA SOCIAL DEL ESTADO HOSPITAL SAN ANTONIO DE PADUA LA PLATA HUILA	Código: MAG-GIT-AS-PL-002
	PROCESO: GESTIÓN DE INFORMACIÓN Y TECNOLOGÍAS	Versión: 06 Página: 14 de 14

CONTROL DE REVISIÓN

VERSIÓN	FECHA	COMENTARIO
01	25/01/2019	Elaboración Primera Versión
02	26/01/2021	Elaboración Segunda Versión
03	24/01/2022	Elaboración Tercera Versión
04	20/01/2023	Elaboración Cuarta Versión
05	29/01/2024	Elaboración Quinta Versión
06	30/01/2025	Elaboración Sexta Versión, alineado al nuevo Plan de Desarrollo 2024 - 2028

Elaborado por: Nombre: Edwin Fabian Castro Quintero Cargo: Ingeniero de Sistemas Firma: 	Fecha: 07/01/2025
Revisado por: Nombre: John David Villa Cargo: Apoyo Dinámica Gerencial Firma: 	Fecha: 13/01/2025
Aprobado por: Nombre: José Antonio Muñoz Paz Cargo: Gerente Firma: 	Fecha: 30/01/2025

— Salud Integral, Impacto Real —

"Documento no valido en medio impreso sin la identificación de sello seco "Documento Controlado" Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital".