

 HUS HOSPITAL UNIVERSITARIO DE LA SAMARITANA <i>Empresa Social del Estado</i>	PLAN		
	PROCESO	GESTIÓN DE LA INFORMACIÓN	
	NOMBRE:	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
	CÓDIGO DEL DOCUMENTO:	05GC08-V2	

1. APROBACIÓN				
	CARGO	NOMBRE	FECHA	FIRMA
ELABORÓ	SUBDIRECTOR DE SISTEMAS	Alfredo Téllez Arza	29/01/2021	
REVISÓ	DIRECTOR ADMINISTRATIVO	Sandra Eliana Rodriguez Garcia	29/01/2021	
APROBÓ	JEFE DE OFICINA ASESORA DE PLANEACIÓN Y GARANTÍA DE LA CALIDAD	Yesid Ramirez Mora	29/01/2021	
	GERENTE	Edgar Silvio Sánchez Villegas	29/01/2021	

2. JUSTIFICACIÓN
<p>La E.S.E Hospital Universitario de la Samaritana adopta el modelo de seguridad y privacidad de la información dado por el Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea. Este documento se elaboró con la recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL. El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.</p> <p>La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en la Entidad está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad.</p> <p>El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.</p> <p>A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.</p> <p>Para el desarrollo del componente de Seguridad y Privacidad de la Información, se ha elaborado un conjunto de documentos asociados al Modelo de Seguridad y Privacidad de la Información, los cuales, a lo largo de los últimos años, han sido utilizados por las diferentes entidades tanto del orden nacional como territorial, para mejorar sus estándares de seguridad de la información.</p> <p>El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; así mismo recoge además de los cambios técnicos de la norma, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.</p>

3. OBJETIVOS
<p>3.1. GENERAL: Establecer políticas, procesos y procedimientos para lograr la seguridad y privacidad de la información para la protección de los activos de información, los recursos y la tecnología, preservando la confidencialidad, integridad y disponibilidad de la información de la E.S.E Hospital Universitario de la Samaritana.</p>
<p>3.2. ESPECÍFICOS:</p>

Estado de documento: VIGENTE	Fecha de próxima revisión:	Cuatro años a partir de la fecha de elaboración.	Tipo de copia:	Nº	Tabla de Retención:	Página 1 de 7
---------------------------------	-------------------------------	---	-------------------	----	------------------------	---------------

<p>HUS HOSPITAL UNIVERSITARIO DE LA SAMARITANA <i>Empresa Social del Estado</i></p>	PLAN		
	PROCESO	GESTIÓN DE LA INFORMACIÓN	
	NOMBRE:	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
CÓDIGO DEL DOCUMENTO:			05GC08-V2

3. OBJETIVOS
<ul style="list-style-type: none"> • 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 del HUS • Fortalecer el uso de las Tecnologías de la Información al interior del HUS, desarrollando las actividades necesarias para garantizar su seguridad, monitoreo, seguimiento, control y mejora continua. • Garantizar la seguridad y la privacidad de la información. • Comprometer a todos los funcionarios del HUS en la formulación e implementación de controles y acciones encaminadas a prevenir los riesgos de la seguridad y privacidad de la información. • Fortalecer la cultura de seguridad y privacidad de la información en los funcionarios, contratistas, terceros, estudiantes, practicantes y proveedores.

4. ALCANCE
<p>El presente documento, está destinado a orientar a las áreas y colaboradores del HUS para la implementación de controles, adopción políticas y lineamientos que permitan preservar la confidencialidad, integridad y disponibilidad de la información que reciban, generen y procesen en medio físico o digital, con el fin de mitigar la afectación ante posibles amenazas.</p> <p>Se definen las actividades a ser lideradas por el HUS durante el 2021, en cumplimiento de sus funciones y para el logro de sus objetivos.</p>

5. DEFINICIONES
<p>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)</p> <p>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. (ISO/IEC 27000).</p> <p>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.</p> <p>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. (Ley 594 de 2000, art 3)</p> <p>Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).</p> <p>Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).</p> <p>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).</p> <p>Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)</p> <p>Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)</p> <p>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).</p> <p>Ciberspacio: 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</p>

Estado de documento: VIGENTE	Fecha de próxima revisión:	Cuatro años a partir de la fecha de elaboración.	Tipo de copia:	Nº	Tabla de Retención:	Página 2 de 7
--	-----------------------------------	--	-----------------------	----	----------------------------	---------------

 <p>HUS HOSPITAL UNIVERSITARIO DE LA SAMARITANA <i>Empresa Social del Estado</i></p>	PLAN		
	PROCESO	GESTIÓN DE LA INFORMACIÓN	
	NOMBRE:	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
	CÓDIGO DEL DOCUMENTO:	05GC08-V2	

5. DEFINICIONES

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).

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. (Decreto 1377 de 2013, art 3)

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles 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, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, 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).

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).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

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 continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Estado de documento: VIGENTE	Fecha de próxima revisión:	Cuatro años a partir de la fecha de elaboración.	Tipo de copia:	Nº	Tabla de Retención:	Página 3 de 7
---------------------------------	-------------------------------	---	-------------------	----	------------------------	---------------

<p>HUS HOSPITAL UNIVERSITARIO DE LA SAMARITANA <i>Empresa Social del Estado</i></p>	PLAN		
	PROCESO	GESTIÓN DE LA INFORMACIÓN	
	NOMBRE:	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
	CÓDIGO DEL DOCUMENTO:	05GC08-V2	

5. DEFINICIONES
<p>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).</p> <p>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.</p> <p>Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)</p> <p>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.</p> <p>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).</p> <p>Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).</p> <p>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).</p> <p>Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).</p>

6. MARCO NORMATIVO
<ul style="list-style-type: none"> - Anexo 1 - Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública - Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública - Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones - Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública - Ley 57 de 1985 - Publicidad de los actos y documentos oficiales - Ley 594 de 2000 - Ley General de Archivos - Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones - Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones - Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática - Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones - Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad - Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones - Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo - Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos

Estado de documento: VIGENTE	Fecha de próxima revisión: Cuatro años a partir de la fecha de elaboración.	Tipo de copia:	Nº	Tabla de Retención:	Página 4 de 7
--	---	-----------------------	-----------	----------------------------	----------------------

 HUS HOSPITAL UNIVERSITARIO DE LA SAMARITANA <i>Empresa Social del Estado</i>	PLAN		
	PROCESO	GESTIÓN DE LA INFORMACIÓN	
	NOMBRE:	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
	CÓDIGO DEL DOCUMENTO:	05GC08-V2	

6. MARCO NORMATIVO
<ul style="list-style-type: none"> - Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones - Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos - Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública - Decreto 2364 de 2012 - Firma electrónica - Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos - Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales - Ley 527 de 1999 - Ley de Comercio Electrónico - Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública - Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones - Ley Estatutaria 1581 de 2012 - Protección de datos personales - Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información

7. METODOLOGÍA PARA LA IMPLEMENTACIÓN
<p>La implementación del Sistema de gestión de seguridad y privacidad de la información, toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar), el modelo MSPI de MINTIC, el modelo integrado de planeación y gestión – MIPG y la norma ISO 27001:2013.</p>


 HUS HOSPITAL UNIVERSITARIO DE LA SAMARTIANA <i>Empresa Social del Estado</i>	PLAN		
	PROCESO	GESTIÓN DE LA INFORMACIÓN	
	NOMBRE:	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
	CÓDIGO DEL DOCUMENTO:	05GC08-V2	

7. METODOLOGÍA PARA LA IMPLEMENTACIÓN

FASE DE DIAGNÓSTICO - ETAPAS PREVIAS A LA IMPLEMENTACIÓN: En esta fase se pretende identificar el estado actual del HUS con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información,

En la fase de diagnóstico del MSPI se pretende alcanzar las siguientes metas:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
- Determinar el nivel de madurez de los controles de seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- Identificación del uso de buenas prácticas en ciberseguridad.

FASE DE PLANIFICACIÓN: Para el desarrollo de esta fase el HUS debe utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional del HUS, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

El alcance del MSPI permite a HUS definir los límites sobre los cuales se implementará la seguridad y privacidad. Este enfoque es por procesos y debe extenderse a toda el HUS. Para desarrollar el alcance y los límites del Modelo se deben tener en cuenta las siguientes recomendaciones: Procesos que impactan directamente la consecución de objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo con otros procesos.

FASE DE IMPLEMENTACIÓN: Esta fase le permitirá al HUS, llevar a cabo la implementación de la planificación realizada en la fase anterior del MSPI.

FASE DE EVALUACIÓN DE DESEMPEÑO: El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

FASE DE MEJORA CONTINUA: En esta fase el HUS debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

8. LÍNEAS ESTRATÉGICAS DEL PLAN E INDICADORES

Fortalecer a un nivel optimizado, controles del Sistema de Gestión de Seguridad de la información.

- Componente GEL: TIC para la Gestión
- Dominios del Marco TI: Servicios tecnológicos, uso y apropiación
- Objetivo estratégico Institucional: Garantizar un Sistema de Información integral, eficiente y eficaz.

Implementar estrategias de sensibilización en seguridad de la información.

- Componente GEL: TIC para la Gestión
- Dominios del Marco TI: Servicios tecnológicos, uso y apropiación
- Objetivo estratégico Institucional: Garantizar un Sistema de Información integral, eficiente y eficaz.

Propender por la continuidad, funcionamiento, disponibilidad de los sistemas de información misionales y de apoyo

- Componente GEL: TIC para la Gestión

Estado de documento: VIGENTE	Fecha de próxima revisión: Cuatro años a partir de la fecha de elaboración.	Tipo de copia:	Nº	Tabla de Retención:	Página 6 de 7
--	---	-----------------------	-----------	----------------------------	----------------------

	PLAN		
	PROCESO	GESTIÓN DE LA INFORMACIÓN	
	NOMBRE:	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
	CÓDIGO DEL DOCUMENTO:	05GC08-V2	

<p>8. LÍNEAS ESTRATÉGICAS DEL PLAN E INDICADORES</p> <ul style="list-style-type: none"> - Dominios del Marco TI: Sistemas de Información, Servicios Tecnológicos, Gestión de la Información, Uso y Apropiación: - Objetivo estratégico Institucional: Garantizar un Sistema de Información integral, eficiente y eficaz <p>INDICADORES:</p> <p>Porcentaje de ejecución de Las actividades de ejecución del plan de la vigencia Formula: (N° de actividades ejecutadas / N° de actividades programadas) * 100 Frecuencia de Medición: Semestral</p>

<p>9. PLAN DE SEGUIMIENTO</p> <p>El seguimiento del presente plan será verificado cada año, de tal manera que se haga el respectivo monitoreo y actualización según se determine la necesidad.</p>

<p>10. CRONOGRAMA DE EJECUCIÓN</p> <p>Ver Anexo Cronograma</p>

11. CONTROL DE CAMBIOS			
VERSION	FECHA	ITEM MODIFICADO	JUSTIFICACION
1	29/09/2018	N/A	Primera vez dando cumplimiento en el decreto 612 de 2018
2	29/01/2021	Actualización de Numeral 8	Actualización del Plan

