HUS Hospital Universitario de la Samaritana – Empresa Social del Estado	PLAN		Calidad soy yo!
	PROCESO	GESTIÓN DE LA INFORMACIÓN	
	NOMBRE:	PLAN DE TRATAMIENTO DE RIESGOS 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 Ramírez Mora	29/01/2021	
	GERENTE	Edgar Silvio Sánchez Villegas	29/01/2021	

2. JUSTIFICACIÓN

La E.S.E. Hospital Universitario de la Samaritana en busca de la mejora continua define un plan que permita identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados el manejo de la información institucional, para lograr que estos no afecten de una manera relevante a la misma.

A través de ésta Plan se busca orientar al HUS a gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) buscando la integración con la Metodología de riesgos del DAFP. Ayudando al HUS logre vincular la identificación y análisis de Riesgos hacia los temas de la Seguridad de la Información.

El MECI dispone la implementación del componente de administración del riesgo, cuyos elementos son: contexto estratégico, identificación, análisis, valoración y políticas de administración de riesgos. Estos elementos hacen parte del plan. Lo anterior, buscando el cumplimiento de la Seguridad y Privacidad de la Información.

3. OBJETIVOS

3.1. GENERAL: Desarrollar un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información el cual sea una guía para el control y minimización de los de los riesgos y así proteger la privacidad de la información y los datos tanto de los procesos como de las personas vinculadas con la información de la institución.

3.2. ESPECÍFICOS:

- Categorizar y valorar los activos de información
- Establecer los controles y políticas de la seguridad de la información que garantice la confidencialidad integridad y disponibilidad de la información.
- Ajustar el mapa de riesgos de los procesos donde se incluyan los riesgos definidos para los activos de información.

4. ALCANCE

El plan de Riesgos de Seguridad y Privacidad aplica a todos los procesos de la institución los cuales manejen, procesen o interactúen con información institucional.
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.

5. DEFINICIONES

Seguridad informática: Se ocupa de la implementación técnica y de la operación para la protección de la información.
Seguridad de la información: Se Ocupa de evaluar el riesgo y las amenazas, traza el plan de acción y esquemas normativos. Es la línea estratégica de las Seguridad.
Amenazas: Cualquier evento, persona, situación o fenómeno que pueda causar daño.
Vulnerabilidades: Falla o debilidad en un sistema que puede ser explotada por quien la conozca.
Riesgo: Probabilidad de ocurrencia de una amenaza.
Controles: Conjunto de mecanismos que regulan el funcionamiento de un sistema.
ISO: Organización Internacional de Normalización es una organización para la creación de estándares internacionales.
Activo: Bienes, recursos o derechos que tenga valor para una organización.
Activo de Información: Toda la información que maneja con la que cuenta una organización para un correcto funcionamiento.
Análisis de brechas: es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado.
Análisis de Riesgo: Método empleado para evaluar los riesgos informáticos y obtener respuesta de peligro.
Gestión del Riesgo Informáticos: Actividades empleadas para mitigar los riesgos informáticos.
Incidente de seguridad informática: daño que puede comprometer las operaciones de la alcaldía municipal.
Evento: Acción que puedo haber causado daño, pero fue controlado.
Información: Conjunto de datos que tienen un significado.
Probabilidad: Posibilidad de que una amenaza se materialice
Impacto: Daño que provoca la materialización de una amenaza.
SGSI: Sistema de Gestión de seguridad de la Información
MSPI: Modelo de seguridad y privacidad de la información
PHVA: Planear, hacer, verificar, actuar.

6. MARCO NORMATIVO

- 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

6. MARCO NORMATIVO

- Tecnologías de la Información y las Comunicaciones

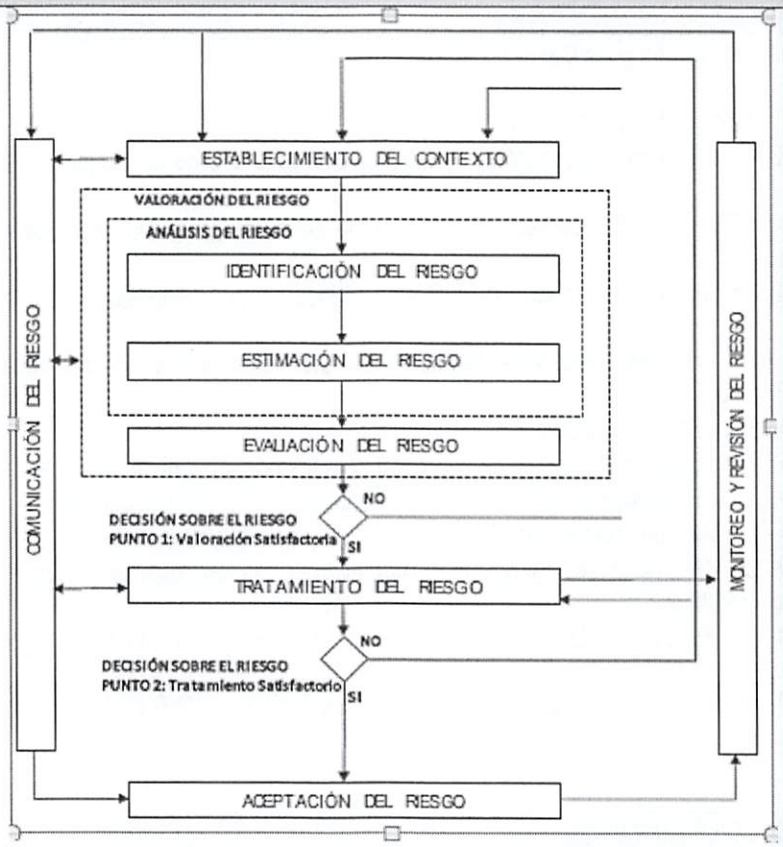
- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo
- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías 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 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.

8. METODOLOGÍA PARA LA IMPLEMENTACIÓN

La implementación del Sistema de gestión de seguridad y privacidad de la información, toma como base la metodología el modelo MSPI de MINTIC, el modelo integrado de planeación y gestión – MIPG y la norma ISO 27001:2013.

El HUS cuenta con un programa de Gestión y administración del riesgo 01GC04 que tiene como objetivo: "*Identificar los potenciales riesgos, adelantar las acciones para el adecuado tratamiento y reducción de los mismos, que eviten su materialización así como eventos no deseados, todo bajo un estrategia de priorización, cuyo manejo garantice el cumplimiento de los objetivos institucionales y de sus procesos, implementando acciones de monitoreo y retroalimentación pertinentes evitando así daños en los pacientes, usuarios y familiares, en los colaboradores del hospital, en el patrimonio e imagen de la entidad y en las partes interesadas*" y se tiene el procedimiento Administración del Riesgo 02GC05 que tiene como objetivo "*Mitigar el impacto y la frecuencia de ocurrencia del riesgo, a través de los controles establecidos,* estos documentos se articulan con este plan ya cumplen con la Guía No 7 de MINTIC donde determina el Proceso para la administración del riesgo en seguridad de la información

8. METODOLOGÍA PARA LA IMPLEMENTACIÓN



Adicionalmente MINTIC en su guía No. 7 define unas etapas sugeridas para la gestión del riesgo:

- La primera y más importante para lograr un adecuado avance en todo el proceso de administración del riesgo es el "Compromiso de las alta y media dirección"
- En segundo lugar, se encuentra la "Conformación de un Equipo MECI o de un grupo interdisciplinario", la idea de una integralidad en el tratamiento de los riesgos para poder tener una visión completa de la Entidad.
- Finalmente se encuentra la "Capacitación en la metodología", este punto es un poco más profundo, porque es claro que el equipo interdisciplinario debe capacitarse para poder analizar ahora los riesgos de seguridad.

Las etapas anteriores el HUS ya cuentan con un Equipo MECI y se articulará este plan con este equipo.

Etapas propuestas para la Generación del análisis de riesgos de las Entidades, basadas la norma ISO27005

ETAPA 1: IDENTIFICACIÓN DEL RIESGO: El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida, las siguientes etapas deberían recolectar datos de entrada para esta actividad.

ETAPA 2: IDENTIFICACIÓN DE LOS ACTIVOS: Según la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección. La identificación de activos se debería llevar acabo con un nivel

8. METODOLOGÍA PARA LA IMPLEMENTACIÓN

adecuado de detalle que proporcione información suficiente para la valoración del riesgo. Para realizar esta identificación es necesario revisar la guía de gestión de activos adjunta al MSPI.

ETAPA 3: IDENTIFICACIÓN DE LAS AMENAZAS: Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo.

ETAPA 4: IDENTIFICACIÓN DE CONTROLES EXISTENTES: Se debe realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, por ejemplo, la duplicidad de controles, además de esto mientras se identifican los controles

ETAPA 5: IDENTIFICACIÓN DE LAS VULNERABILIDADES: Para realizar una correcta identificación de vulnerabilidades es necesario conocer la lista de amenazas comunes, la lista de inventario de activos y el listado de controles existentes.

ETAPA 6: MÉTODOS PARA LA VALORACIÓN DE LAS VULNERABILIDADES TÉCNICAS
ETAPA 7: IDENTIFICACIÓN DE LAS CONSECUENCIAS: Para la identificación de las consecuencias es necesario tener: Lista de activos de información y su relación con cada proceso de la entidad y Lista de las amenazas y vulnerabilidades con respecto a los activos y su pertinencia.

9. LÍNES ESTRATÉGICAS DEL PLAN

Minimizar los riesgos asociados a los procesos tecnológicos existentes, con el fin de salvaguardar los activos de 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

10. PLAN DE SEGUIMIENTO

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.

11. CRONOGRAMA DE EJECUCIÓN

Ver Anexo Cronograma

9. 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	Numeral 9	Actualización del Plan