E.S.E. HOSPITAL LOCAL CARTAGENA DE INDIAS

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

GESTIÓN TECNOLOGICA Y DE SISTEMAS DE INFORMACIÓN

OBJETIVOS

Objetivo General

Establecer los conceptos básicos y metodológicos para una adecuada administración de riesgos a partir de su identificación, manejo y seguimiento.

Objetivos Específicos

- ✓ Concientizar a todos los colaboradores, áreas, procesos, proveedores, externos en general sobre la necesidad e importancia de gestionar de manera adecuada, los riesgos inherentes a la gestión.
- ✓ Involucrar y comprometer a todos en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.
- ✓ Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.

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 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 Pagina 7 de 13

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.

AMBITO DE APLICACION

Los lineamientos definidos en esta guía, aplica para la gestión de los riesgos.

DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- ✓ **Acciones asociadas:** son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.
- ✓ **Administración de riesgos:** conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
- ✓ **Amenaza:** situación externa que no controla la entidad y que puede afectar su operación
- ✓ **Análisis del riesgo:** etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).
- ✓ **Asumir el riesgo:** opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.
- ✓ **Causa:** medios, circunstancias y/o agentes que generan riesgos.
- ✓ **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- ✓ **Compartir o transferir el riesgo:** opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.
- ✓ **Consecuencia:** efectos que se pueden presentar cuando un riesgo se materializa.
- ✓ **Contexto estratégico:** son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
- ✓ **Control:** acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
- ✓ **Control preventivo:** acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.
- ✓ **Control correctivo:** acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.

- ✓ **Debilidad:** situación interna que la entidad puede controlar y que puede afectar su operación.
- ✓ **Evaluación del riesgo:** resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.
- ✓ **Evitar el riesgo:** opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.
- ✓ **Frecuencia:** ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
- ✓ **Identificación del riesgo:** etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos
- ✓ **Impacto:** medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.
- ✓ **Mapa de riesgos:** documento que de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.
- ✓ **Materialización del riesgo:** ocurrencia del riesgo identificado
- ✓ **Opciones de manejo:** posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).
- ✓ **Plan de contingencia:** conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio
- ✓ **Probabilidad:** medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.
- ✓ **Procedimiento:** conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.
- ✓ **Proceso:** conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.
- ✓ **Riesgo:** eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.
- ✓ **Riesgo de corrupción:** posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.
- ✓ **Riesgo inherente:** es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.

- ✓ **Riesgo institucional**: Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:
  - Los riesgos que han sido clasificados como estratégicos: en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.
  - Los riesgos que se encuentran en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.
  - Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.
  - Los riesgos de corrupción: todos los riesgos identificados que hagan referencia a situaciones de corrupción, serán considerados como riesgos de tipo institucional.
- ✓ **Riesgo residual:** nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.
- ✓ **Valoración del riesgo:** establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.

MONITOREO Y REVISION DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACION

Los jefes de cada uno de los procesos realizaran el monitoreo anual o en el momento que se determine, de los mapas de riesgos con el apoyo de las áreas de Control Interno, Calidad y Gestión Tecnológica y Sistemas de Información con la finalidad de analizar con sus equipos de trabajo el estado de sus riesgos frente a los controles establecidos. Según el resultado de la administración del riesgo, el líder del proceso solicitará ajuste a los riesgos o controles y elaborará acciones de mejoramiento o correctivas en el Plan de Mejoramiento del proceso, para propender por un efectivo manejo de los Riesgos de Seguridad y Privacidad de la Información.

REFERENCIA Y DOCUMENTOS ASOCIADOS

El plan de tratamiento de riesgos de seguridad y privacidad de la información se articula con las siguientes referencias y documentos asociados:

- ✓ Plan modelo de seguridad y privacidad de la información – MSPI
- ✓ Modelo integrado de planeación y gestión. Departamento administrativo de planeación nacional.
- ✓ Estrategia de gobierno digital. Ministerio de las TIC
- ✓ Guía diligenciamiento del mapa de riesgos de seguridad y privacidad de la información.
- ✓ Política de administración de riesgos.
- ✓ Manual de políticas de seguridad de la información de la ESE Hospital Local Cartagena de Indias.

5. VISION GENERAL DEL PROCESO DE RIESGOS DE SEGURIDAD DE LA INFORMACION

A continuación, se presenta el modelo de gestión de riesgos de seguridad de la información diseñado Y basado tanto en la norma ISO/IEC 31000 como en la ISO 27005 aprobado por la UPTC para la adecuada administración de riesgos en la seguridad de la información; los elementos que lo componen son:

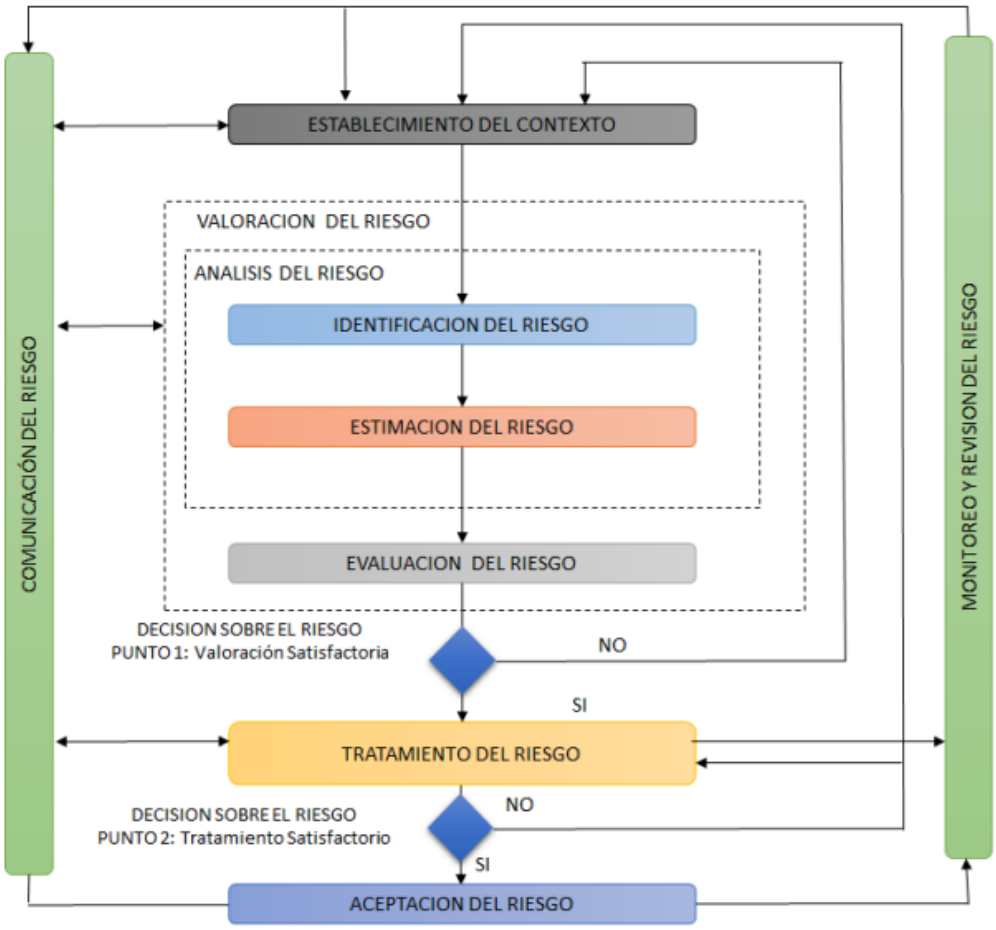


Imagen 1: VISION PROCESO DE RIESGOS DE SEGURIDAD

Tomado de la norma ISO/IEC 27005

CLASIFICACION DE LOS RIESGOS

Durante la etapa de identificación, se realiza una clasificación del riesgo, según sus características, con el fin de orientar la formulación de un tratamiento adecuado que posibilite la mitigación del riego mediante la definición de controles y planes de manejo:

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Criterios para definir el nivel de probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

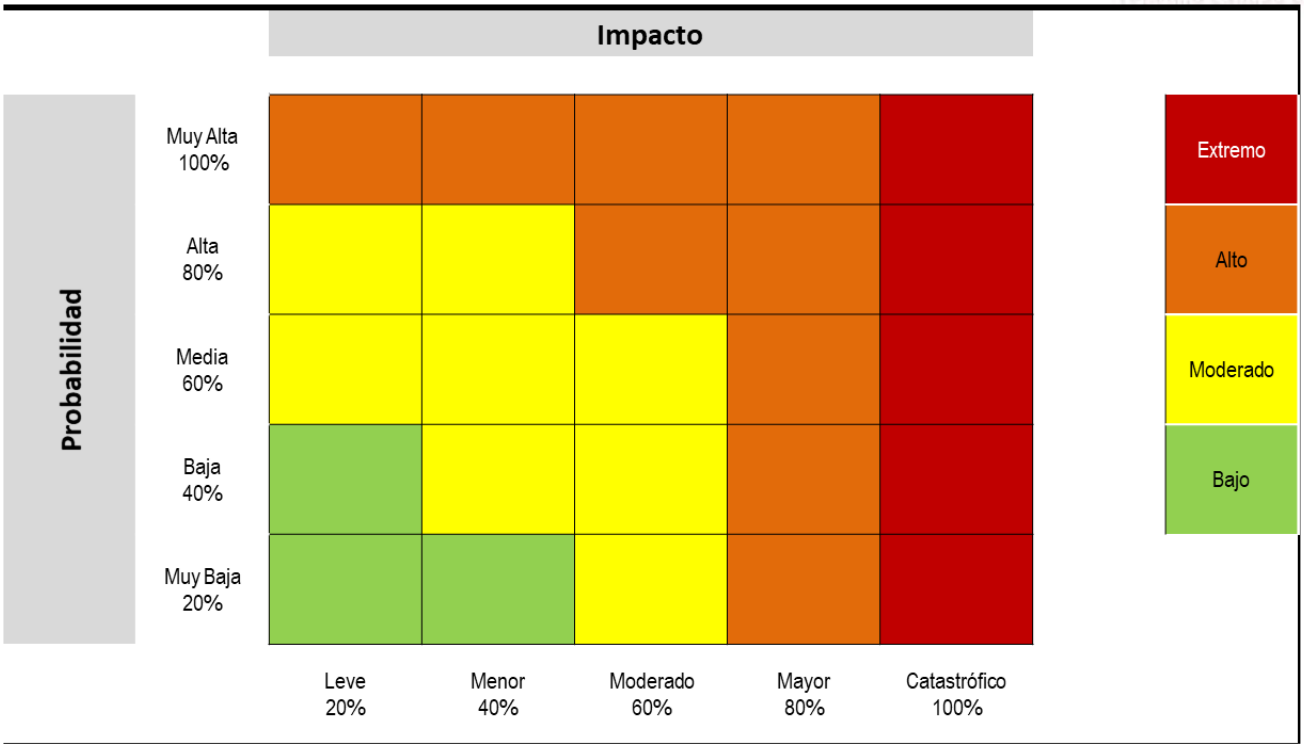
Criterios para definir el nivel de impacto

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Evaluación de riesgos: a partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

3.2.1 Análisis preliminar (riesgo inherente): se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor

Matriz de calor (niveles de severidad del riesgo)



IDENTIFICACIÓN DE RIESGOS

Normalmente se identifican los riesgos como eventos o situaciones no deseadas que se pretenden evitar, por tal razón la identificación de riesgos inicia con términos como: Ausencia, No adherencia, Inadecuada, No suficiencia, entre otros. Una vez se identifique el riesgo, debe complementarse para obtener el contexto del riesgo, ya que éste puede presentarse en un área, en un horario, por parte de un grupo de colaboradores, o en unas circunstancias específicas que ayudarán más adelante a determinar las acciones a tomar.

A continuación podemos observar los riesgos generales a los que la entidad podría estar expuesta

IDENTIFICACIÓN DEL RIESGO				
IMPACTO	**DESCRIPCIÓN DEL RIESGO**	**CAUSA RAIZ**	**CONSECUENCIAS**	**CLASIFICACIÓN DEL RIESGO**
Reputacional	Daño en equipos tecnologicos e interrupción de servicios a cargo del área TIC por factores electricos en la sede administrativa y centros de salud de la entidad	Corte de energia electrica, fluctuaciones de tensión, ruido electrico, interrupciones, mantenimiento de los equipos y las redes electricas.	Interrupción del servicio	Fallas Tecnológicas
Económico	Daño en equipos tecnologicos e interrupción de servicios a cargo del área TIC a causa del manejo indebido de equipos tecnologicos	Inexistencia de manuales de procedimiento s para administrar la infraestructura tecnologica	Baja eficiencia en la prestación del servicio, reclamo e insatisfacción de los usuarios, perdida de credibilidad e imagen d ela entidad	Usuarios, Productos y Prácticas
Reputacional	Interrupción del servicio de internet por fallos en la provisión del servicio	Inconvenientes de configuración y direccionamien to, mantenimiento de las redes y equipos, suspensión del servicio, ruido, actualizaciones	Interrupción del servicio, reclamos e insatisfaccione s y perdida de credibilidad e imagende la entidad	Fallas Tecnológicas

IDENTIFICACIÓN DEL RIESGO				
IMPACTO	**DESCRIPCIÓN DEL RIESGO**	**CAUSA RAIZ**	**CONSECUENCIAS**	**CLASIFICACIÓN DEL RIESGO**
Reputacional	Interrupción del servicio TI causados por daños en la infraestructura tecnologica por causas desconocidas	Defectos de fabrica, implementación e instalación incorrecta, factores tecnologicos desconocidos	Interrupción del servicio, daños, bloqueos o desconfiguración de los equipos.	Fallas Tecnológicas
Reputacional	Robo, alteración y/o perdida de información de la entidad por acceso indebido a sistemas de información	Acceso abusivo a un sistema informatico, obstaculización ilegitima del sistema informatico o red de telecomunicaciones, interceptación de datos informaticos, uso de software malicioso, violación de datos, suplantación de sitios web	Interrupción del servicio y perdidas economicas	Usuarios, Productos y Prácticas
Reputacional	Robo, alteración y/o perdida de información de la entidad por robo informatico	Hurto por medio informaticos y semejantes, transferencia no consentida de activos	Perdida de información, vulnerabilidad de la información	Daños a Activos Fijos

IDENTIFICACIÓN DEL RIESGO				
IMPACTO	**DESCRIPCIÓN DEL RIESGO**	**CAUSA RAIZ**	**CONSECUENCIAS**	**CLASIFICACIÓN DEL RIESGO**
Reputacional	Desactualización y obsolencias tecnologica a causa de actualizaciones	Evolución y mejora continua de la tecnologia en cuanto a hardaware y software	Obsolencia tecnologica, indisponibilidad del servicio y cambios de normatividad	Ejecución y administración de Procesos
Reputacional	Ineficiencia administrativa por desconocimiento o falta de formación TI	Falta de presupuesto para llevar a cabo capacitaciones al personal suministrado.	Desconocimiento de la normatividad Sanciones a la entidad	Ejecución y administración de Procesos
Reputacional	Perdida de información por virus informatico	No se tiene un software actualizado que detecte virus informáticos	Perdida de información. Daño en equipos. Perdida de tiempo para poder entregar información oportunamente.	Daños a Activos Fijos
Reputacional	No se cuenta con los recursos para la ejecución total del PETI- Plan Estrategico de Tecnologia de Información	Falta de presupuesto	Obsolencia tecnologica. Poca adaptación a los cambios del entorno.	Fallas Tecnológicas

MAPA DE RIESGO INSTITUCIONAL 2022

Codigo: FTO- PLN-MRIN-11
Versión: 2
Fecha: 21/01/2022

PROCESO	OBJETIVO DEL PROCESO	IDENTIFICACIÓN DEL No. DEL RIESGO	IDENTIFICACIÓN DEL RIESGO					Análisis del riesgo inherente		ZONA DE RIESGO INHERENTE	CONTROLES		Evaluación del riesgo - Nivel del riesgo residual		NUEVA VALORACIÓN ZONA DE RIESGO (RESIDUAL)	Responsable	OPCIONES MANEJO	ACCIONES PREVENTIVAS	META	INDICADOR
			IMPACTO	DESCRIPCIÓN DEL RIESGO	CAUSA RAIZ	CONSECUENCIAS	CLASIFICACIÓN DEL RIESGO	PROBABILIDAD	IMPACTO		DESCRIPCIÓN CONTROL	Tipo Control	PROBABILIDAD	IMPACTO						
			Reputacional	Daño en equipos tecnologicos e interrupción de servicios a cargo del área TIC por factores electricos en la sede administrativa y centros de salud de la entidad	Corte de energia electrica, fluctuaciones de tensión, ruido electrico, interrupciones, mantenimiento de los equipos y las redes electricas.	Interrupción del servicio	Fallas Tecnológicas	Media	Menor	Moderado	Informar a la gerencia de la entidad y a la coordinación de del área de mantenimiento por medio de un informe las fallas electricas que se presenten en las sede administrativa y diferentes centros de salud en la infraestructura de telecomunicaciones	Control Correctivo-Automático	Baja	Menor	Moderado	SISTEMAS	Reducir-Mitigar	Revisar y notificar que hallan tomado las medidas necesarias para dar solución a lo planteado en el informe acerca de fallas electricas presentadas.	12	# de informes entregados / # de informes programados
			Económico	Daño en equipos tecnologicos e interrupción de servicios a cargo del área TIC a causa del manejo indebido de equipos tecnologicos	linexistencia de manuales de procedimiento s para administrar la infraestructura tecnologica	Baja eficiencia en la prestación del servicio, reclamo e insatisfacción de los usuarios, perdida de credibilidad e imagen d ela entidad	Usuarios, Productos y Prácticas	Media	Menor	Moderado	Entrega de actas de compromiso y responsabilidad sobre los equipos asignados a los funcionarios de la sede administrativa y centros de salud de la entidad	Control Correctivo-Manual	Baja	Menor	Moderado	SISTEMAS	Evitar	Se relacionan informes de los equipos dañados y se pasan al área de almacén para darles de baja	4	# de informes entregados / # de informes programados
			Reputacional	Interrupción del servicio de internet por fallas en la provisión del servicio	Inconvenientes de configuración y direccionamien to, mantenimiento de las redes y equipos, suspensión del servicio, ruido, actualizaciones	Interrupción del servicio, reclamos e insatisfaccione s y perdida de credibilidad e imagende la entidad	Fallas Tecnológicas	Media	Leve	Moderado	Contar con un canal de respaldo que garantice la continuidad del servicio. Configurar aplicaciones que monitoren los consumos y disponibilidad del servicio, dejarlo por sentado por medio de informes. Solicitar al contratista que cuente con canales de respaldo Solicitar al contratista acceso a las herramientas de monitoreo que permitan la generación de informes sobre los consumos y prestación del	Control Preventivo-Automático	Baja	Leve	Bajo	SISTEMAS	Reducir-Mitigar	Contratar canales de backup y soporte de servicio	1	# servicios contratados / # de servicios programados a contratar
			Reputacional	Interrupción del servicio TI causados por daños en la infraestructura tecnologica por causas desconocidas	Defectos de fabrica, implementació n e instalación incorrecta, factores tecnologicos desconocidos	Interrupción del servicio, daños, bloqueos o desconfiguraci ón de los equipos.	Fallas Tecnológicas	Media	Menor	Moderado	Reemplazar recursos tecnologicos que tengan un alto indice de obsolencia y promover procesos de compra de infraestructura tecnologica moderna.	Control Correctivo-Manual	Media	Menor	Moderado	SISTEMAS	Reducir-Mitigar	Reportando nuevas adquisiciones y necesidades en los informes de gestión entregados por el área TIC	12	# de informes entregados / # de informes programados
			Reputacional	Robo, alteración y/o perdida de infomación de la entidad por acceso indebido a sistemas de información	Acceso abusivo a un sistema informatico, obstaculización ilegitima del sistema informatico o red de telecomunicaci ones, interceptación de datos informaticos, uso de software malicioso, violación de datos, suplantación de sitios web	Interrupción del servicio y pertidas economicas	Usuarios, Productos y Prácticas	Baja	Leve	Bajo	Revisar consumo banda ancha, verificar servicios de nuestros canales.	Control Preventivo-Automático	Baja	Leve	Bajo	SISTEMAS	Evitar	Reporte a Control interno y disciplinario	12	# de reportes entregados / # de reportes programados
			Reputacional	Robo, alteración y/o perdida de infomación de la entidad por robo informatico	Hurto por medio informaticos y semejantes, transferencia no consentida de activos	Perdida de información, vulnerabilidad de la información	Daños a Activos Fijos	Baja	Leve	Bajo	Renovación de servicio de backup en la nube	Control Preventivo-Automático	Muy Baja	Leve	Bajo	SISTEMAS	Evitar	Reporte a Control interno y disciplinario	4	# de informes entregados / # de informes programados
			Reputacional	Desactualización y obsolencias tecnologica a causa de actualizaciones	Evolución y mejora continua de la tecnologia en cuanto a hardaware y software	Obsolencia tecnologica, indisponibilida d del servicio y cambios de normatividad	Ejecución y administració n de Procesos	Baja	Moderado	Moderado	Suministro de partes y piezas para optimizar el funcionamiento de la infraestructura tecnologica. Recepción de solicitudes mediante el formato solicitud, cambios, ajustes y/o creación de nuevos modulos sobre los sistemas de información de la entidad.	Control Detectivo-Manual	Muy Baja	Moderado	Moderado	SISTEMAS	Reducir-Mitigar	Contratar servicios de suministros de piezas	1	# servicios contratados / # de servicios programados a contratar
			Reputacional	Ineficiencia administrativa por desconocimiento o falta de formación TI	Falta de presupuesto para llevar a cabo capacitaciones al personal suministrado.	Desconocimien to de la normatividad Sanciones a la entidad	Ejecución y administració n de Procesos	Baja	Leve	Bajo	Solicitud de capacitaciones a la subgerencia administrativa	Control Detectivo-Manual	Muy Baja	Leve	Bajo	SISTEMAS	Reducir-Transferir	Capacitaciones de plataformas para administrar TI	1	# capacitaciones realizadas / # de capacitaciones programados
			Reputacional	Perdida de información por virus informatico	No se tiene un software actualizado que detecte virus informáticos	Perdida de información. Daño en equipos. Perdida de tiempo para poder entregar información oportunament e.	Daños a Activos Fijos	Media	Moderado	Moderado	Instalacion y configuracion de antivirus gratuito	Control Preventivo-Automático	Muy Baja	Moderado	Moderado	SISTEMAS	Reducir-Mitigar	Backup de la información	12	# backup realizados / # de backup programados
			Reputacional	No se cuenta con los recursos para la ejecución total del PETI- Plan Estrategico de Tecnologia de Información	Falta de presupuesto	Obsolencia tecnologica. Poca adaptación a los cambios del entorno.	Fallas Tecnológicas	Baja	Leve	Bajo	Solicitar a la Gerencia y Subgerencia administrativa el presupuesto para llevar a cabo los proyectos plasmados en el PETI	Control Preventivo-Automático	Muy Baja	Leve	Bajo	SISTEMAS	Reducir-Mitigar	Implementar herramientas gratuitas hasta donde sea posible.	1	# servicios contratados / # de servicios programados a contratar

SE ANEXA MAPA DE RIESGO TIC

ESTRATEGIA DE COMUNICACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Periódicamente se revisara el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

Los riesgos son dinámicos como la misma entidad por tanto cambiar de forma o manera radical sin previo aviso. Por ello es necesario una supervisión continua que detecte:

- Nuevos activos o modificaciones en el valor de los activos
- Nuevas amenazas
- Cambios o aparición de nuevas vulnerabilidades
- Aumento de las consecuencias o impactos
- Incidentes de seguridad de la información

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión y de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.

Para llevar acabo la implementación del modelo de seguridad y privacidad de la información, se toma como base la metodología PHVA (planear, hacer, verificar y actuar) y los lineamientos emitidos por el ministerio de tecnología de la información y las comunicaciones – Min Tic, a través de lo derechos emitidos. De acuerdo con esto, se definen las siguientes fases de implementación del MSPI: 1. Diagnosticar 2. Planear 3. Hacer 4. Verificar 5. Actuar

Cronograma	Enero				Febrero				Marzo				Abril				Mayo				Junio			
	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
Valoración de Activos				X				X				X				X				X				X
Realizar la identificación de los riesgos		X				X				X				X				X				X		
Diseño del plan del tratamiento del riesgo		X				X				X				X				X				X		
Desarrollo, ejecución de actividades definidas en plan de tratamiento de riesgo	X				X				X				X				X				X			
Valorar del riesgo residual								X								X								X
Informe de riesgo a la gerencia	X				X				X				X				X				X			

Cronograma	Julio				Agosto				Septiembre				Octubre				Noviembre				Diciembre			
	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
Valoración de Activos				X				X				X				X				X				X
Realizar la identificación de los riesgos		X				X				X				X				X				X		
Diseño del plan del tratamiento del riesgo		X				X				X				X				X				X		
Desarrollo, ejecución de actividades definidas en plan de tratamiento de riesgo	X				X				X				X				X				X			
Valorar del riesgo residual								X								X								X
Informe de riesgo a la gerencia	X				X				X				X				X				X			

Como estrategia de comunicación y divulgación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se realizara a través de inducciones generales y página web institucional www.esecartagenadeindias.gov.co para ser conocido por los funcionarios, usuarios y/o colaboradores

Elaborado por:

EDWIN LÓPEZ
Coordinador Área Gestión Tecnológica y de Sistemas de Información

CARLOS FUENTES
P.A. Área Gestión Tecnológica y de Sistemas de Información

Aprobado por:

Miembros de comité institucional de gestión y desempeño:

JORGE SUAREZ
Gerente

AURA MORENO
Subgerente Administrativo

EMPERATRIZ CARDOZO
Subgerente Científico

LUZ MERY CIFUENTES CALIFA
Profesional Universitario

MONICA ESTHER ACOSTA CHIMA
Profesional Universitario

Dando cumplimiento con el Decreto 612 del 4 de abril de 2018, "...las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión (MIPG), al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año. El área de Gestión Tecnológica y de Sistemas de Información de la ESE Hospital Local Cartagena de Indias, publica el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información correspondiente a la vigencia 2021-2023.

Enero de 2022