

E.S.E. HOSPITAL LOCAL CARTAGENA DE INDIAS

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

GESTIÓN TECNOLÓGICA 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 APLICACIÓN

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.

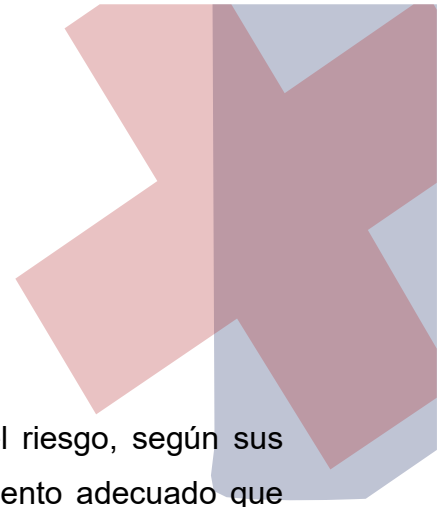
MONITOREO Y REVISION DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACION

Los jefes de cada uno de los procesos realizarán 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.



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 riesgo mediante la definición de controles y planes de manejo:

Clases de Riesgo	Definición
Estratégico	Son los riesgos relacionados con la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
Operativo	Relacionados con el funcionamiento y operatividad de los sistemas de información de la entidad: definición de procesos, estructura de la entidad, articulación entre dependencias.
Financieros	Relacionados con el manejo de los recursos de la entidad: ejecución presupuestal, elaboración estados financieros, pagos, manejos de excedentes de tesorería y manejo de los bienes.
Cumplimiento	Capacidad de cumplir requisitos legales, contractuales, ética pública y compromiso con la comunidad.
Tecnología	Capacidad para que la tecnología disponible satisfaga las necesidades actuales y futuras y el cumplimiento de la misión.
Imagen	Tienen que ver con la credibilidad, confianza y percepción de los usuarios de la entidad.

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.

CLASIFICACION DEL RIESGO	RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	CAUSA	CONSECUENCIA
ESTRATEGICO	Perdida, robo o fuga de información	Fallas en el proceso de copia de respaldo o de restauración de la información o pérdida de la misma	Afectación parcial o total de la operación Vulneración de los sistemas de seguridad Generación de consultas funcionalidades o reportes con Información sensible de la entidad y sus usuarios
		Falla en los análisis y socialización de las vulnerabilidades de la infraestructura de TI.	
		No contar con acuerdos de Confidencialidad con los empleados y terceros	
		Falta de autorización para la extracción de información generadas por requerimientos	
		Ingreso a la red y acceso a los activos de TI por parte de máquinas ajenas a la entidad	
		No contar con Antivirus actualizado	
		Habilitación de puertos USB en modulo lectura y escritura para medios de almacenamiento	
		Ataques cibernéticos internos y externos	
		Empleados no capacitados en los temas de riesgos informáticos	
		Desconocimiento del riesgo	
		Prestar los equipos informáticos a personal no autorizado	
		No cerrar sesión cuando se desplaza del puesto	
		Acceso no autorizado a las dependencias	
		Acceso a enlaces o páginas web no autorizados	
		Falta de implementación de la política de escritorio limpio	
Brechas de seguridad en proveedores y terceros			
OPERATIVO	Correos electrónicos con remitentes desconocidos o adjunto con ejecutables	Desconocimiento del riesgo	Cifrado de información captura de las pulsaciones del teclado, monitoreo de las actividades realizadas en el equipo, acceso remoto, robo de contraseñas, documentos y/ archivos, sistema con mal funcionamiento
		Empleados no capacitados en los temas de riesgos informáticos	
		falta de filtros en el firewall	
		acceso a correo o portales no autorizados	
	Daño en los equipos tecnológicos	Suplantación de correos electrónicos	Perdidas de información perdida de los equipos informáticos Indisponibilidad del servicio traumatismo en los procesos
		Manejo inadecuado de los equipos	
		Falta de mantenimiento o mala conexión de los mismos en las instalaciones eléctricas	
		Falta de protección de potenciación	
		Fallas por defectos de fabrica	
		Derrame de liquido	
		Falta de ambiente adecuado para los equipos	
		Falta de educación a los usuarios en el manejo de los equipos de computo	
		Cambios de voltaje en el fluido eléctrico	
		Infraestructura en mal estado (paredes, cielo raso, techo, divisiones)	
	Equipos en estado de obsolescencia		
	Perdida de conectividad	Daño externo del servicio de internet	Interrupción en la continuidad de las actividades y/o tareas que requieren del servicio de internet Realización de procesos administrativos y asistenciales de forma manual
		Robo de equipos	
		Fallas en los equipos de conectividad	
		fallas en el fluido eléctrico	
		No contar con redundancia de red	
		Daños en fibra óptica causados por factor humano y/o ambiental	
Obstrucción en la línea de vista del radio enlace			
No contar con redundancia eléctrica			
El no pago oportuno al proveedor del servicio			
Ataques informáticos	Espionaje	<ul style="list-style-type: none"> ✓ Denegación del servicio ✓ Daño a los equipos tecnológicos ✓ Indecentes en la confidencialidad, integridad y disponibilidad de la información ✓ Suplantación de identidad ✓ Destrucción de información 	
	Ánimo de lucro		
	Rebelión		
	Estafa o extorsión		
	Estimulo personal		

ESCALA PARA CALIFICAR EL IMPACTO DEL RIESGO							
Tipos de efecto o impacto		a) Estratégico	b) Operativo	c) Financieros	d) Cumplimiento	e) Tecnología	f) Imagen
INSIGNIFICANTE	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos o bajos sobre la institución	Afecta el cumplimiento de algunas actividades	Genera ajustes a una actividad concreta	La pérdida financiera no afecta la operación normal de la institución	Genera un requerimiento	Afecta a una persona o una actividad del proceso	Afecta a un grupo de servidores del proceso
MENOR	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la institución	Afecta el cumplimiento de las metas del proceso	Genera ajustes en los procedimientos	La pérdida financiera afecta algunos servicios administrativos de la institución	Genera investigaciones disciplinarias, y/o fiscales y/o penales	Afecta el proceso	Afecta a los servidores del proceso
MODERADO	Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la Institución	Afecta el cumplimiento de las metas de un grupo de procesos	Genera ajustes o cambios en los procesos	La pérdida financiera afecta considerablemente la prestación del servicio	Genera interrupciones en la prestación del bien o servicio	Afecta varios procesos de la institución	Afecta a todos los servidores de la institución
MAYOR	Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la institución	Afecta el cumplimiento de las metas de la institución	Genera intermitencia en el servicio	La pérdida financiera afecta considerablemente el presupuesto de la institución	Genera sanciones	Afecta a toda la entidad	Afecta el sector
CATASTRÓFICO	Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos sobre la institución	Afecta el cumplimiento de las metas del sector y del gobierno	Genera paro total de la institución	Afecta al presupuesto de otras entidades o a de la del departamento	Genera cierre definitivo de la institución	Afecta al Departamento	Afecta al Departamento, Gobierno, Todos los usuarios de la institución

CALIFICACION DEL RIESGO

Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo. La primera representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse, y la segunda se refiere a la magnitud de sus efectos. Para la determinación de la calificación del riesgo, con base en la probabilidad y el impacto se debe tener en cuenta las siguientes tablas:

ESCALA PARA CALIFICAR LA PROBABILIDAD DEL RIESGO		
Nivel	Concepto	Frecuencia
Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
Improbable	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 5 años.
Moderado	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en el último año.
Casi certeza	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

SE ANEXA MAPA DE RIESGO TIC

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

Como estrategia de comunicación y divulgación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se realizará 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 JAVIER LÓPEZ CORRALES

Jefe de Oficina de IT

JOSÉ PÉREZ

Profesional Administrativo

Aprobado por:

Miembros de comité institucional de gestión y desempeño:

JULIO PIÑEROS

Gerente

LUIS SANDOVAL

Subgerente Administrativo

EMPERATRIZ CARDOZO MEZA

Subgerente Científico

LUZ MERY CIFUENTES CALIFA

Profesional Universitario

JOSE PAZ

Director Financiero

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 2019.

Enero 29 de 2025