E.S.E. HOSPITAL UNIVERSITARIO
Julio Méndez Barreneche

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

SANTA MARTA 2022

Contenido

1. INTRODUCCIÓN

Para la ESE Hospital Universitario Julio Méndez Barreneche HUJMB, la administración de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

La información que hace parte del HUJMB es crucial para su correcto desempeño dentro de la política pública y su relación con el ciudadano, sin importar qué tipo de información se trate en la Entidad, ésta será parte primordial en el cumplimiento de sus Objetivos, es por ello que resguardar todo tipo de Información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos, puede significar un respaldo para el normal desarrollo de las actividades de una Entidad o de un Estado.

Todos los servidores públicos, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Por esa razón, el presente plan tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, sus fundamentos teóricos y da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y da lineamientos sencillos y claros para su adecuada gestión.

2. OBJETIVOS

2.1 GENERAL

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

2.2 ESPECIFICOS

- 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.

3. ALCANCE

Este plan proporciona adopta la metodología establecida por el HUJMB para la administración y gestión de los riesgos a nivel de actividades, funciones y procesos; orienta sobre las actividades a desarrollar desde la definición del contexto estratégico, la identificación de los riesgos, su análisis, valoración y la definición de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

4. AMBITO DE APLICACION

Los lineamientos definidos en este plan, aplica para la gestión de los riesgos de los procesos del HUJMB en lo correspondiente a la seguridad y privacidad de la información

5. 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.

6. RESPONSABLES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

El éxito de la administración del riesgo depende de la decidida participación de los directivos, servidores públicos y contratistas; por esto, es preciso identificar los actores que intervienen:

- ✓ Grupo de Trabajo de Seguridad de la Información
- ✓ Líderes de Procesos
- ✓ Subdirección Administrativa
- ✓ Subdirección Científica

✓ Gerencia

7. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

- Debe ser cultura del HUJMB que todo riesgo se gestione y se identifiquen acciones que permitan la minimización del impacto negativo de su materialización.

- Se debe tener un flujo de comunicación tanto interna como externa que contribuya al conocimiento de los riesgos por las partes involucradas.

8. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

A continuación, se presenta el proceso basado con la Gestión de Riesgo Institucional - CODIGO: PLAR5P, con el cual se realizará la gestión de riesgos de la seguridad y privacidad de la información, que serán actualizados para la vigencia 2021:

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLES
Establecimiento del contexto externo	La información de entrada para establecer el contexto externo de los riesgos de la organización se debe definir en un análisis estratégico que contenga como mínimo el comportamiento del sector, la reglamentación, el análisis financiero, la política y directrices del HUJMB. Este análisis estratégico debe ser revisado y actualizado mínimo una vez al año, debe ser socializado con las directivas y los responsables de proceso de la empresa.	Grupo de Trabajo de Seguridad de la Información

Establecimiento del contexto interno	Para definir el contexto interno cada responsable de proceso registrará en la matriz de riesgos, lo relativo a su proceso, para cual se apoyarán en la siguiente información de entrada: resultados de auditoria, evaluaciones de desempeño, no conformidades reportadas, resultados de indicadores de gestión, quejas de usuarios, encuestas de satisfacción, entre otras.	Grupo de Trabajo de Seguridad de la Información y Responsables de proceso
Identificación del riesgo	Cada proceso debe diligenciar el formato de identificación de riesgos PLAR1FV, el cual debe contener el nombre y el objetivo del proceso, las posibles causas, riesgos, una breve descripción del mismo y sus efectos o consecuencias. Los formatos de identificación de riesgos luego de tramitados deben ser socializados como mínimo con el equipo de planeación estratégica y las personas que intervienen en el proceso.	Grupo de Trabajo de Seguridad de la Información y Responsables de proceso
Análisis del riesgo	Una vez identificados los riesgos se procederá a calificar la probabilidad e impacto de los mismos teniendo en cuenta los niveles establecidos por la empresa en las tablas de calificación de probabilidad PLAR2FV y de la calificación del impacto PLAR3FV.	Grupo de Trabajo de Seguridad de la Información y Responsables de proceso
Evaluación del riesgo	Los resultados del análisis del riesgo se consolidarán en la matriz de calificación, evaluación, y respuesta a los riesgos PLAR4FV establecida por la empresa. La calificación del riesgo se obtiene de la multiplicación de la criticidad por el impacto. Se considerará un riesgo como: • Aceptable si su resultado es 5. • Tolerable si su resultado es 10.	Grupo de Trabajo de Seguridad de la Información y Responsables de proceso

	• Moderado si su resultado es 15 y 20. • Importante cuando sea de 30 y 40. Inaceptable si su resultado es 60.	
Tratamiento de los riesgos	Las acciones a implementar dependerán del resultado de la evaluación del riesgo, así, si e l riesgo es: **Aceptable:** la decisión será asumirlo lo que significa aceptar la perdida y elaborar planes de contingencia para manejarlo. **Tolerable**: la decisión será asumirlo y reducirlo, habrá que implementar medidas preventivas para disminuir la probabilidad y el impacto. **Moderado**: la decisión será evitar el riesgo, se tomarán las medidas necesarias para prevenir que se materialicen estos riesgos. **Importante**: las acciones serán: reducir el riesgo, evitarlo, compartirlo o transferirlo con las puertas involucradas. **Inaceptable**: las acciones serán: evitar el riesgo, reducirlo, compartirlo o transferirlos.	Grupo de Trabajo de Seguridad de la Información
Monitoreo de los riesgos	Se debe elaborar un mapa de riesgo por proceso en el formato PLAR6FV en el cual se detallarán el riesgo, su impacto, probabilidad, evaluación, controles, la valoración del riesgo, las acciones a seguir con sus responsables, y el parámetro de seguimiento asignado. El responsable del proceso debe diligenciar el formato de tratamiento del riesgo, el cual será revisado por el responsable del sistema con periodicidad semestral.	Oficial de Seguridad de la información Control Interno
Reevaluación del riesgo	Los riesgos identificados en los diferentes procesos deben ser reevaluados anualmente a fin de garantizar su adecuada gestión. Cuando se identifiquen nuevas amenazas o vulnerabilidades se debe proceder a la revaluación de los riesgos. Toda revaluación de riesgo debe generar un	Grupo de Trabajo de Seguridad de la Información

	registro que detalle las decisiones tomadas (Inclusión o retiro de un riesgo, Modificaciones en la valoración, cambio de controles, cambio de actividades, responsables, etc.).	

9. MAPA DE RIESGOS

Una vez se tenga toda la información relacionada en los numerales anteriores, se documentará la información en el formato Mapa de riesgos de Seguridad de la Información como la siguiente:

IDENTIFICACION DEL RIESGO			ANALISIS					VALORACION				TRATAMIENTO		
RIESGO, EVENTO, FALLA O SITUACION PELIGROSA	**GENERADO POR/ CAUSADO POR / FUENTE**	**POSIBLE CONSECUENCIA / EFECTO NO DESEADO**	**PROBABILIDAD (De 1 a 5)**	**CONSECUENCIA (De 1 a 5)**	**Resultado**	**NIVEL DEL RIESGO INHERENTE (Probabilidad x Consecuencia)**	**CONVERSIÓN**	**CONTROLES ACTUALES** (Controles de ingeniería, señalización/ advertencias o controles administrativos o EPP)	**EFICACIA DEL CONTROL (De 1 a 5)**	**Resultado**	**NIVEL DEL RIESGO RESIDUAL (Eficacia x Conversión Nivel**	**PLAN DE ACCIÓN O TRATAMIENTO** (Se puede considerar la eliminación o sustitución, mediante un plan de acción concreto/ Indispensable cumplimiento de requisito legal aplicable)		
												ACCION	**RESPONSABLE**	**FECHA DE EJECUCION**
Interrupción de servicios informáticos como: acceso a internet, correo electrónico, servicios de los sistemas de información.	Sobre carga en el canal de internet Uso indebido de internet para ocio en horario laboral Cambios en los niveles de voltaje o corriente Daños en la tecnología por mala manipulación	1. Interrupción parcial o total de los servicios informáticos. 2. Denegación de servicios informáticos 3. Pérdidas económicas. 4. Insatisfacción en el usuario 5. Mala imagen institucional 6. Sanciones legales y administrativas	3	4	12	Alto	4	1. Mantenimiento de equipos tecnológicos 2. Control interno sobre red general	2	8	De Alerta	Limitar el acceso a páginas web de ocio en horario laboral Capacitar al personal sobre el buen uso de las herramientas tecnológicas	Oficina de sistemas	Trimestral
Desactualización tecnológica o alto grado de obsolescencia en TICS	Poca disponibilidad Presupuestal Incumplimiento de contratos Falta de cultura hacia la seguridad informática	1. Perdida de información. 2. información inconsistente 3. Pérdidas económicas. 4. Retraso o imposibilidad en la prestación del servicio. 5, Insatisfacción en el usuario interno y externo. 6 Mala imagen institucional 7. Sanciones legales y administrativas	5	4	20	Muy Alto	5	1. Solicitud de insumos 2. Estudio de necesidades tecnológicas 3. Mantenimiento preventivo y/o correctivo	5	25	No Aceptable	Realización de plan de compras y actualización de equipos Aplicar políticas de renovación de equipos Aumentar el valor presupuestado para actualización de equipos	Oficina de sistemas Oficina de financiera Subgerencia administrativa	ANUAL

Fallas en los equipos informáticos	Falta de seguimiento y ejecución al Plan de Mantenimiento preventivo de servidores, equipos y redes. Fallas en el control de stock de partes más usadas. Fallas en el control de stock de elementos de mantenimiento. Falta de herramientas necesarias para realizar mantenimientos preventivos y/o correctivos	1. Información inconsistente. 2. Demora en la ejecución de las actividades. 4. Insatisfacción en el usuario interno y externo. 4. Retraso o imposibilidad en la prestación del servicio.	3	3	9	Medio	3	1. Inventario de equipos tecnológicos 2. Plan de mantenimiento de equipos 3. documento informe de control de mantenimiento 4. hojas de vida de equipos tecnológicos 5. capacitaciones a personal	1	3	Aceptable	Continuar controles	Oficina de sistemas	Trimestral
Ataque cibernético a la infraestructura de red	Actor externo Fallas en software de seguridad Fallas humanas al descargar archivos infectados o en parametrizaciones de redes	Perdida o alteración de información Perdidas económicas Afectación de la prestación de servicios Afectación de trabajo en áreas administrativas Afectación de reputación de la institución	2	5	10	Medio	3	1. Software de seguridad 2. Revisión constate de equipos de red 3. Capacitación al usuario	1	3	Aceptable	Continuar controles	Oficina de sistemas	Cuatrimestral

Perdida, Alteración y/o manipulación de información	Actor externo Fallas en sistemas de información Fallas humanas Inafectación de virus de equipos Incendios Robos Fenómenos naturales	Perdida o alteración de información Perdidas económicas Afectación de la prestación de servicios Afectación de trabajo en áreas administrativas Afectación de reputación de la institución	2	5	10	Medio	3	1. Autenticación por doble criptografía 2. Restricción en acceso físico 3. Restricción de usuarios al acceso de información 4. Definición de roles para manejo de base de datos 5. Auditoria de acceso a bases de datos 6. Realización constante de copias de seguridad 7. Plan de contingencia 8. Base de datos de equipos 9. Circuito de vigilancia	1	3	Aceptable	Continuar controles	Oficina de sistemas	Mensual
Uso inapropiado de los equipos, sistemas de información, servicios de Internet y correo electrónico	Deficiente cultura del personal en el cumplimiento de Políticas de Seguridad	Daño en los equipos de cómputo; retraso en labores por retiro de equipos	4	4	16	Alto	4	1. Política de seguridad y privacidad de la información 2. Firewall de seguridad 3. Auditorias de trafico de red 4. Mantenimiento preventivo 5. Capacitación de usuarios 6. Restricción de accesos a equipos	2	8	De Alerta	Actualización de softwares de seguridad Sanciones o atestaciones a los usuarios Capacitación sobre el buen uso de la tecnología	Oficina de sistemas	Trimestral

Alteración y manipulación de información manejada por el proceso por parte de funcionarios o terceros.	Intereses particulares en la sustracción de datos confidenciales. Falta de controles en la gestión documental falta de herramientas tecnológicas para el manejo de la información.	Perdida de confidencialidad de información sensible Perjuicios económicos, técnicos y operativos.	5	4	20	Muy Alto	5	Claves de acceso Responsabilidades asignadas a líderes de procesos Política de Seguridad informática	2	10	De Alerta	1. Socialización y medición de la Política de Seguridad de la información 2. Creación de usuarios de acceso a la información con definición de perfiles y responsabilidades 3. Desarrollar los procedimientos que definan los criterios para el manejo de la información.	P/E Gestión de la Calidad	TRIMESTRAL

CONTROL DE CAMBIOS

Versión	Fecha	Cambios
1.0	Febrero 2021	Versión Inicial
2.0	Enero 2022	Actualización de Actividades - Responsables