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

E.S.E. HOSPITAL SAGRADO CORAZON DE JESUS DE QUIMBAYA

2020

Cra. 4 Cll. 19 Esquina
PBX 7520200 – FAX 7520405
e-mail: hscj@ese-hscj.gov.co
Web: ese-hscj.gov.co

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

Tabla de Contenido

INTRODUCCIÓN 3
1. OBJETIVO 4
2. EJECUCIÓN DEL PLAN 4
2.1. ESTABLECER EL CONTEXTO PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 4
CRITERIOS DE EVALUACIÓN DEL RIESGO: 4
CRITERIOS DE IMPACTO 5
CRITERIOS DE ACEPTACIÓN DEL RIESGO 5
2.2. VALORACIÓN DEL RIESGO 6
IDENTIFICACIÓN DEL RIESGO 6
IDENTIFICACIÓN DE LOS ACTIVOS 6
IDENTIFICACIÓN DE LAS AMENAZAS 7
IDENTIFICACIÓN DE LAS VULNERABILIDADES 7
2.3. ANÁLISIS DE RIESGOS 8
Criterios para clasificar la probabilidad de ocurrencia del riesgo 8
Criterios para la calificación del impacto del riesgo 8
MAPA DE CALOR 10
2.4. EVALUACIÓN DE RIESGOS 11
Peso o participación de cada variable en el diseño del control para la mitigación del riesgo. 11
2.5. TRATAMIENTO DE RIESGOS 12
2.6. DECLARACIÓN DE APLICABILIDAD 13
3. COMUNICACIÓN Y CONSULTA 14
4. MONITOREO Y REVISIÓN 14
5. MECANISMOS DE SEGUIMIENTO Y VERIFICACIÓN 17
MAPA DE RIESGOS 18
FORMATO DE DESCRIPCION DEL RIESGO DE SEGURIDAD DIGITAL 18
FORMATO MAPA Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL 21
6. BIBLIOGRAFIA 24
7. SEGUIMIENTO, CONTROL Y MEJORA 24
8. MODIFICACIONES ..... **¡Error! Marcador no definido.**
9. APROBACIÓN 25

INTRODUCCIÓN

La información que genera constantemente la E.S.E. Hospital Sagrado Corazón de Jesús de Quimbaya es crucial para su correcto desempeño y cumplimiento de los objetivos organizacionales, es por ello que la seguridad y privacidad de la información se convierten en atributos indispensables para evitar cualquier posibilidad de alteración, mal uso, pérdida, entre otros eventos, que puedan significar una alteración para el normal desarrollo en la prestación de servicios de salud.

De acuerdo a lo mencionado anteriormente, dentro de Marco de Seguridad del Modelo de Seguridad y Privacidad de la información –MSPI-, un tema decisivo, es la Gestión de riesgos la cual es utilizada para la toma de decisiones. Es por esto que la E.S.E. Hospital Sagrado Corazón de Jesús de Quimbaya adopta la metodología “Guía de Riesgos” del Departamento Administrativo de la Función Púbica y como herramienta metodológica la utilizada por la Unidad Nacional para la Gestión del Riesgo de Desastres de la Presidencia de la República, además ha incorporado como referente la Norma ISO 31000 con el objetivo de generar buenas prácticas de gobierno corporativo y del mejoramiento continuo en la gestión de riesgos.

La E.S.E. Hospital Sagrado Corazón de Jesús de Quimbaya acoge la gestión de riesgos como un proceso sistemático de identificación, análisis, evaluación, valoración, y tratamiento de los riesgos; aplicando los controles necesarios para evitar, reducir, compartir, transferir o asumir el riesgo con medidas preventivas o correctivas que deberá generar como resultado minimizar pérdidas, maximizar rendimientos y cuidar la seguridad y privacidad de la información.

1. OBJETIVO

Vincular la identificación y análisis de Riesgos de la Entidad hacia los temas de la Seguridad de la Información con la Metodología de riesgos del DAFP.

2. EJECUCIÓN DEL PLAN

Para la realización del plan de tratamiento de riesgos de seguridad y privacidad de la información se utilizó la Guía para la Administración del riesgo y el diseño de controles en entidades públicas- Riesgos de gestión, corrupción y seguridad digital versión 4 del DAFP y el Anexo 4 Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas del Ministerio de tecnologías de la información y las comunicaciones.

2.1. ESTABLECER EL CONTEXTO PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Corresponde a una visión general de los riesgos que pueden afectar el cumplimiento de los objetivos en este caso para la seguridad y privacidad de la información se analiza información de la estructura organizacional, del modelo de operación por procesos, del cumplimiento de planes y programas, de los recursos físicos y tecnológicos, entre otros.

Para establecer el contexto para la gestión del riesgo es necesario definir los criterios de riesgo de seguridad y privacidad de la información:

CRITERIOS DE EVALUACIÓN DEL RIESGO:

Para la evaluación del riesgo con el fin de determinar el riesgo en la seguridad de la información de la organización se tienen en cuenta los siguientes aspectos

- El valor estratégico del proceso de información para la entidad

- La criticidad de los activos de información involucrados en el proceso

- Los requisitos legales y reglamentarios, así como las obligaciones contractuales

- La importancia de la disponibilidad de la confidencialidad, e integridad de la información para las operaciones de la entidad
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación de la entidad.

CRITERIOS DE IMPACTO

Los criterios de impacto del riesgo se especifican en términos de afectación a la población, afectación del presupuesto anual de la entidad y afectación medio ambiental, estos criterios de impacto son cuantitativos y en términos cualitativos se mide en cuanto al nivel de la integridad, disponibilidad y confidencialidad, los cuales pueden ser: Sin afectación, afectación leve, afectación moderada, afectación grave y afectación muy grave en cada uno de ellos.

CRITERIOS DE ACEPTACIÓN DEL RIESGO

La E.S.E. Hospital Sagrado Corazón de Jesús de Quimbaya cuenta con los siguientes criterios:

Tipo de riesgo	Zona de riesgo	Nivel de aceptación
Riesgos de seguridad digital	Baja	Se **ASUMIRÁ** el riesgo y se administra por medio de las actividades propias del proceso asociado y se realiza en el reporte **semestral** de su desempeño.
	Moderada	Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo, se hace seguimiento **SEMESTRALMENTE** y se registra en el formato establecido.
	Alta y Extrema	Se debe incluir el riesgo tanto en el Mapa de riesgo del Proceso como en el Mapa de Riesgo Institucional y se establecen acciones de Control Preventivas que permitan **MITIGAR** la materialización del riesgo. Se monitorea **TRIMESTRALMENTE** y se registra en el formato establecido.

2.2. VALORACIÓN DEL RIESGO

La valoración del riesgo consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

Para realizar la valoración del riesgo hay que tener en cuenta el análisis del riesgo y la evaluación del riesgo.

Para los riesgos de seguridad y privacidad se debe tener en cuenta:

IDENTIFICACIÓN DEL RIESGO

Para efectos del presente modelo se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad digital:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles **amenazas** y **vulnerabilidades** que podrían causar su materialización.

La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza **puede** no requerir la implementación de un control.

IDENTIFICACIÓN DE LOS ACTIVOS

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital son activos elementos tales como aplicaciones de la entidad pública, servicios Web, redes, información física o digital, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-) que utiliza la organización para su funcionamiento.

Para la identificación de activos de deben tener en cuenta los siguientes pasos:

Paso 1: Listar activos por cada proceso
Paso 2: Identificar el dueño de los activos
Paso 3: Clasificar los activos
Paso 4: Clasificar la información
Paso 5: Determinar la criticidad del activo
Paso 6: Identificar si existen infraestructuras críticas Cibernétcias

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 (ej. Acciones no autorizadas, daño físico, fallas técnicas) Algunas amenazas pueden afectar a más de un activo y en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

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. Se pueden identificar vulnerabilidades en las siguientes áreas:

Organización.
Procesos y procedimientos.
Rutinas de gestión.
Personal
Ambiente físico
Configuración del sistema de información.
Hardware, software y equipos de comunicaciones.
Dependencia de partes externas.

Cra. 4 Cll. 19 Esquina
PBX 7520200 – FAX 7520405
e-mail: hscj@ese-hscj.gov.co
Web: ese-hscj.gov.co

2.3. ANÁLISIS DE RIESGOS

Determinar probabilidad: Por PROBABILIDAD se entiende la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad

Criterios para clasificar la probabilidad de ocurrencia del riesgo

NIVEL	DESCRIPTOR	DESCRIPCION	FRECUENCIA
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

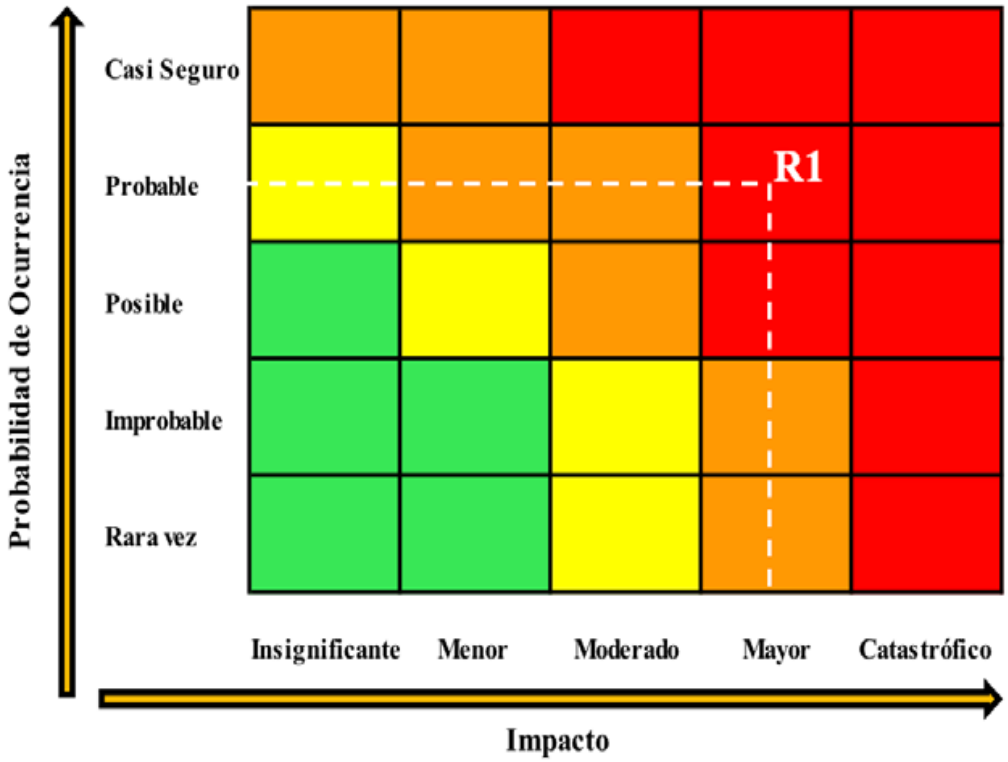
Determinar las consecuencias o nivel de impacto: Por IMPACTO se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Criterios para la calificación del impacto del riesgo

NIVEL	VALOR DEL IMPACTO	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
INSIGNIFICANTE	1	. Afectación ≥0.5% de la población. . Afectación ≥0.5% del presupuesto anual de la entidad. No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.
MENOR	2	. Afectación ≥1% de la población • Afectación ≥1% del presupuesto anual de la entidad	. Afectación leve de la integridad • Afectación leve de la disponibilidad • Afectación leve de la

		• Afectación leve del Medio Ambiente requiere de 0 (cero) días de recuperación	confidencialidad
MODERADO	3	. Afectación ≥2% de la población • Afectación ≥5% del presupuesto anual de la entidad • Afectación leve del Medio Ambiente requiere 0 (cero) semanas de recuperación	. Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros • Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros • Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros
MAYOR	4	. Afectación ≥5% de la población • Afectación ≥10% del presupuesto anual de la entidad • Afectación importante del Medio Ambiente que requiere de 0 (cero) meses de recuperación	Afectación leve de la integridad • Afectación leve de la disponibilidad • Afectación leve de la confidencialidad
CATASTROFICO	5	Afectación ≥10% de la población • Afectación ≥20% del presupuesto anual de la entidad • Afectación muy grave del Medio Ambiente que requiere de 0 (cero) año de recuperación	. Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros • Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros • Afectación muy grave confidencialidad de la información debido al interés particular de los empleados y terceros

MAPA DE CALOR



2.4. EVALUACIÓN DE RIESGOS

Esta última etapa es la valoración del riesgo y se realiza de manera tal que permita establecer la probabilidad de su ocurrencia y el impacto sobre la operación de la E.S.E.

Antes y después de controles: Al momento de definir las actividades de control por parte de la primera línea de defensa, es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitigan las causas que hacen que el riesgo se materialice.

Riesgos antes de controles: Se identifican los riesgos inherentes o subyacentes que pueden afectar el cumplimiento de los objetivos estratégicos y de proceso.

Riesgos después de controles: Evaluar si los controles están bien diseñados para mitigar el riesgo y si estos se ejecutan como fueron diseñados.

Pasos para diseñar un control:
Paso 1: Debe tener definido el responsable de llevar a cabo la actividad de control.
Paso 2: Debe tener una periodicidad definida para su ejecución.
Paso 3: Debe indicar cuál es el propósito del control.
Paso 4: Debe establecer el cómo se realiza la actividad de control.
Paso 5: Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.
Paso 6: Debe dejar evidencia de la ejecución del control.

Peso o participación de cada variable en el diseño del control para la mitigación del riesgo.

CRITERIO DE EVALUACION	OPCION DE RESPUESTA AL CRITERIO EVALUACION	PESO EN LA EVALUACION DEL DISEÑO DEL CONTROL
Asignación del responsable	Asignado	15
	No asignado	0
Segregación y autoridad del responsable	Adecuado	15
	Inadecuado	0
Periodicidad	Oportuna	15
	Inoportuna	0
Propósito	Prevenir	15

	Detectar	10
	onfiable	15
	o confiable	0
	e investigan y resuelven oportunamente	15
	o se investigan y resuelven oportunamente	0
	ompleta	10
	ıcompleta	5
	o existe	0

2.5. TRATAMIENTO DE RIESGOS

Para el manejo de los riesgos se deben analizar las posibles acciones a emprender, las cuales deben ser factibles y efectivas, tales como: la implementación de las políticas, definición de estándares, optimización de procesos y procedimientos y cambios físicos entre otros. El tratamiento de riesgos implica tomar decisiones basadas en los resultados de la identificación de riesgos y su análisis.

La política de gestión de riesgos está determinada por las siguientes opciones de tratamiento:

Tipo de riesgo	Zona de riesgo	Nivel de aceptación
Riesgos de seguridad digital	Baja	Se **ASUMIRÁ** el riesgo y se administra por medio de las actividades propias del proceso asociado y se realiza en el reporte **semestral** de su desempeño.
	Moderada	Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo, se hace seguimiento **SEMESTRALMENTE** y se registra en el formato establecido.
	Alta y Extrema	Se debe incluir el riesgo tanto en el Mapa de riesgo del Proceso como en el Mapa de Riesgo Institucional y se establecen acciones de Control Preventivas que permitan **MITIGAR** la materialización del riesgo. Se monitorea **TRIMESTRALMENTE** y se registra en el formato establecido.

La gestión del riesgo está alineada con el modelo de mejoramiento institucional y es una de las fuentes de mejora. Para el tratamiento de los riesgos se implementan planes de mejoramiento, especialmente en los casos que se identifican nuevos riesgos, cuando es necesario rediseñar los controles existentes o definir unos nuevos controles.

2.6. DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad, por sus siglas en ingles Statement of Applicability (SoA), es un elemento fundamental para la implementación del Modelo de Seguridad y Privacidad de la Información.

La declaración de aplicabilidad se debe realizar luego del tratamiento de riesgos, y a su vez es la actividad posterior a la evaluación de riesgos.

La declaración de aplicabilidad debe indicar si los objetivos de control y los controles se encuentran implementados y en operación, los que se hayan descartado, de igual manera se debe justificar por qué algunas medidas han sido excluidas (las innecesarias y la razón del por qué no son requerías por la Entidad).

		Objetivo de control o control seleccionado Si/No	Razón de la Selección	Objetivo de control o control Implementado Si/No	Justificación de exclusión	Referencia	Aprobado por la alta dirección Firma director de la entidad
Dominio	A.5 Políticas de seguridad de la información						
Objetivo de control	A. 5.1 Directrices establecidas por la dirección para la seguridad de la información						
Control	A. 5.1.1 Políticas para la seguridad de la información						
Control	A. 5.1.2 Revisión de las políticas para seguridad de la información						

3. COMUNICACIÓN Y CONSULTA

La comunicación es muy importante porque permite que todas las partes interesadas emitan su propio juicio sobre los riesgos; es importante tener en cuenta que las percepciones variarán en cuanto a los valores, necesidades, suposiciones, conceptos y preocupaciones de los interesados.

4. MONITOREO Y REVISIÓN

Línea de defensa	Responsable	Responsabilidad frente al riesgo
Estratégica	Alta Dirección y Comité Institucional de Control Interno	• Establecer y aprobar las políticas de administración del riesgo. • Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles • Hacer seguimiento en el Comité Institucional y de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna. • Realizar seguimiento y análisis periódico (Semestralmente) a los riesgos institucionales • Retroalimentar al Comité institucional de gestión y desempeño sobre los ajustes que se deban hacer frente a la gestión del riesgo.
Primera Línea de Defensa	Líderes de los procesos	• Identificar y valorar los riesgos que pueden afectar los planes y procesos a su cargo y actualizarlo cuando se requiera. • Definir, aplicar y hacer seguimiento a los

		controles para mitigar el riesgo identificado alineado con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. • Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles • Informar a la oficina de planeación (segunda línea) sobre los riesgos materializados en los planes y procesos a su cargo. • Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.
Segunda línea de defensa	Oficina de planeación	• Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo • Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos. • Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad.

Cra. 4 Cll. 19 Esquina
PBX 7520200 – FAX 7520405
e-mail: hscj@ese-hscj.gov.co
Web: ese-hscj.gov.co

		• Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos. • Consolidar el Mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el Comité de Gestión y Desempeño Institucional. • Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo • Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos • Supervisar que la primera línea identifique, evalué y gestione los riesgos y controles para que se generen acciones correctivas. • Evaluar que los riesgos sean consistentes con la presente política de la entidad y que sean monitoreados por la primera línea de defensa. • Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles
Tercera línea de defensa	Oficina de Control Interno	• Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. • Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, incluyendo los riesgos de corrupción.

		• Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la Primer Línea de Defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos. • Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas. • Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa • Asesorar de forma coordinada con la Oficina de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles • Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al Comité Institucional de Control Interno. • Recomendar mejoras a la política de administración del riesgo.

5. MECANISMOS DE SEGUIMIENTO Y VERIFICACIÓN

Los atributos establecidos para valorar el desempeño de la gestión de riesgos es una parte de la evaluación global de la institución y de la medición del desempeño de las áreas y de las personas.

Las valoraciones integrales de toda la institución y particulares por proceso, proyecto o estrategia correspondiente a la disminución del nivel de vulnerabilidad, por lo que se tiene el siguiente indicador:

Índice de riesgo residual por proceso: Expresado como proporción o porcentaje de la reducción de los valores estimados de probabilidad e impacto, luego de aplicar las medidas de gestión de riesgos para cada proceso o proyecto.

Formula:

RIESGO INHERENTE – EFECTIVIDAD GESTIÓN DEL RIESGO = RIESGO RESIDUAL

RIESGO CONTROLADO

Meta: Índice de riesgo residual por proceso: Menor de 25

Por lo menos cada semestre, cada responsable de proceso realizará una autoevaluación a la gestión del riesgo, determinando la efectividad de sus controles para minimizar el riesgo, a su vez la Oficina de Control Interno realizará su propio informe de evaluación de riesgos y controles de segundo orden.

MAPA DE RIESGOS

Esta herramienta es utilizada para capturar y evaluar las prácticas de riesgos de la E.S.E. y proporcionar realimentación en forma de una calificación de Madurez de la Gestión de Riesgos.

FORMATO DE DESCRIPCION DEL RIESGO DE SEGURIDAD DIGITAL

RIESGO	ACTIVO	DESCRIPCION DEL RIESGO	AMENAZA	TIPO	CAUSAS / VULNERABILIDADES	CONSECUENCIAS
BASE DE DATOS SOFTWARE CORPORATI	DINAMICA GERENCIAL HOSPITALA	La falta de políticas de seguridad	Modificación no autorizad	Seguridad Digital	Falta de políticas de seguridad digital	Posibles consecuencias que pueda

VO	RIA	digital, ausencia de políticas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, antivirus vulnerable a ataques cibernéticos nuevos. pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos	a		Ausencia de políticas de control de acceso Contraseñas sin protección Autenticación débil	enfrentar la entidad o el proceso a causa de la materialización del riesgo(legales, económicas, sociales, reputacionales, confianza en el ciudadano).

PERDIDA DE INTEGRIDAD Y DISPONIBILIDAD	DINAMICA GERENCIAL HOSPITALARIA	Personal no calificado	Manipulación no autorizada - Falta de experticia - Error involuntario	Seguridad Digital	Inadecuada administración en la base de datos Inadecuada administración del hardware del centro de datos	Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo (legales, económicas, sociales, reputacionales, confianza en el ciudadano).

FORMATO MAPA Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

RIESGO	ACTIVO	TIPO	AMENAZAS	TIPO	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCION DE TRATAMIENTO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
BASE DE DATOS SOFTWARE CORPORATIVO	DINAMICA GERENCIAL HOSPITALARIA	Seguridad digital	Modificación no autorizada	No aplicabilidad de las políticas de control de acceso	2	2		Reducir	Mensualmente el técnico operativo de sistemas de la entidad es aplicara una lista de chequeo para realizar seguimiento a la aplicación de los siguientes controles: Claves de acceso, roles, implementación contraseñas seguras, antivirus actualizados,	Lista de chequeo	Técnico operativo-sistemas	Mensualmente	EFICACIA: No. de actividades verificadas en la lista de chequeo /No. de actividades a verificar

									inactivación de usuarios por retiro, copias de seguridad con periodicidad mínima. Para mejorar la seguridad de la información. Si se presenta alguna desviación se realizara informe que se presentara al Comité de Sistemas de la ESE.				
PERDIDA DE INTEGRIDAD Y DISPONIBILIDAD	DINAMICA GERENCIAL HOSPITALARIA	Seguridad digital	Manipulación no autorizada - Falta de experticia - Error involuntario	Falta de políticas de acceso	2	3		Reducir	Cada vez que se requiera el responsable de cada área realiza el estudio previo para la contratación del personal idóneo. El área de	Estudio	Técnico operativo-sistemas	Agosto de 2019	EFICACIA No. de actividades de control implementadas

									sistemas realizara el estudio para implementación de un mecanismo electrónico de seguridad en el cuarto de sistemas de la ESE. Cada vez que requiera el áreas de sistemas realizara informe a Gerencia sobre el mal estado de las instalaciones físicas y eléctricas, Cada vez que se requiera el área de sistemas realizara inducción y reinducción al personal de acuerdo a la necesidad. Mejorando así el control de acceso y las competencias de los funcionarios con acceso al sistema				

6. BIBLIOGRAFIA

Guía 7 gestiones de riegos. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia de Gobierno en Línea.

Guía 8 controles de seguridad y privacidad de la información. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia de Gobierno en Línea.

Guía para la administración del riesgo y el diseño de controles en entidades públicas- riesgos de gestión, corrupción y seguridad digital, versión 4.0 Dirección e gestión y desempeño institucional.

Anexo 4 lineamientos para la gestión de riesgos de seguridad digital en entidades públicas- Ministerio de tecnologías de la información y las comunicaciones.

7. SEGUIMIENTO, CONTROL Y MEJORA

- Según la periodicidad definida para cada riesgo, verifique las acciones preventivas. Tenga en cuenta la fecha Inicio y fecha fin establecida para su implementación.
- Analice los resultados del seguimiento y establezca acciones inmediatas ante cualquier desviación.
- Comunique al líder del proceso las desviaciones del riesgo según el nivel de aceptación del riesgo.
- Documente las acciones de corrección o prevención en el plan de mejoramiento.
- Revise y actualice el mapa de riesgo cuando se modifique las acciones o ubicación del riesgo.

8. APROBACIÓN

ELABORO	REVISO	APROBO
NOMBRE: MARTHA LILIANA ARROYAVE DE LA PAVA	NOMBRE: Comité Gerencia de Sistemas de información y gestión tecnológica	NOMBRE: DIANA MARCELA CARDONA BARRERA
Cargo: Técnica Operativa / Coordinadora de Sistemas	Cargo:	Cargo: Gerente

VIGENTE A PARTIR DEL: 31/01/2020