PLAN DE TRATAMIENTO DEL RIESGO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | VIGENCIA 2022

KATHERINE CALABRO GALVIS
Gerente

TABLA DE CONTENIDO

1 INTRODUCCIÓN

El entorno digital es un escenario en el que globalmente se desarrollan cada vez más todo tipo de actividades socioeconómicas. Esto expone tanto a las personas como a las mismas organizaciones a amenazas cibernéticas por parte de delincuentes que aprovechan el creciente intercambio de información. Se debe apuntar a que existan las medidas suficientes, tanto en el fortalecimiento de la seguridad, como en la generación de la confianza digital, respecto a una adecuada anticipación, gestión de riesgos, atención oportuna y defensa ante las amenazas existentes en el entorno digital, dentro de un marco de gobernanza nacional eficiente, acorde con las necesidades actuales y en constante desarrollo, en el que se pueda materializar rápidamente la confianza y la seguridad digital ante la aparición de nuevas tecnologías.

2 OBJETIVO

Determinar las acciones de tratamiento de riesgos de seguridad y privacidad de la información, mediante la identificación, análisis, valoración y tratamiento de los riesgos de pérdida de confidencialidad, disponibilidad e integridad de la información, para prevenir su materialización y/o reducir los impactos negativos en la gestión institucional.

3 ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la ESE Hospital Regional Sur Oriental, para la vigencia 2022, está orientado a gestionar los riesgos de seguridad digital asociados a la plataforma tecnológica y servicios de tecnologías de información y comunicaciones, que apoyan el desarrollo de las diferentes actividades asociadas al modelo de operación por procesos adoptados en la entidad.

4 NORMATIVIDAD

Decreto 612 de 2018: Por el cual se fijan las directrices para la integración de los planes institucionales estratégicos al plan de acción por parte de las entidades del estado.

Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Ley 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se

preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Norma Técnica Colombiana NTC ISO 27001 Norma internacional de sistemas de gestión de seguridad y confidencialidad de la información.

Guía No. 7, MINTIC, Guía de gestión de riesgos, Seguridad y privacidad de la información

5 DEFINICIONES

Los siguientes términos son utilizados en el contexto de la gestión de la seguridad de la información y aplican para todas sus fases y momentos, incluyendo la gestión de riesgos.

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

(ISO/IEC 27000)

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la Organización.

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de

un riesgo se evaluada.

Control: Medida que modifica el riesgo. Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada

zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos inaceptables en el marco de la seguridad de la información e implantar los controles necesarios para proteger la misma.

Parte interesada (Stakeholder): Persona u organización que puede afectar a, ser afectada por, o percibirse a sí misma como afectada por una decisión o actividad.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proceso: Conjunto de actividades interrelacionadas que apuntan a un objetivo o que interactúan para transformar una entrada en salida.

Riesgo en la seguridad de la información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo: Aceptación de la pérdida o ganancia proveniente de un riesgo particular.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.

Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

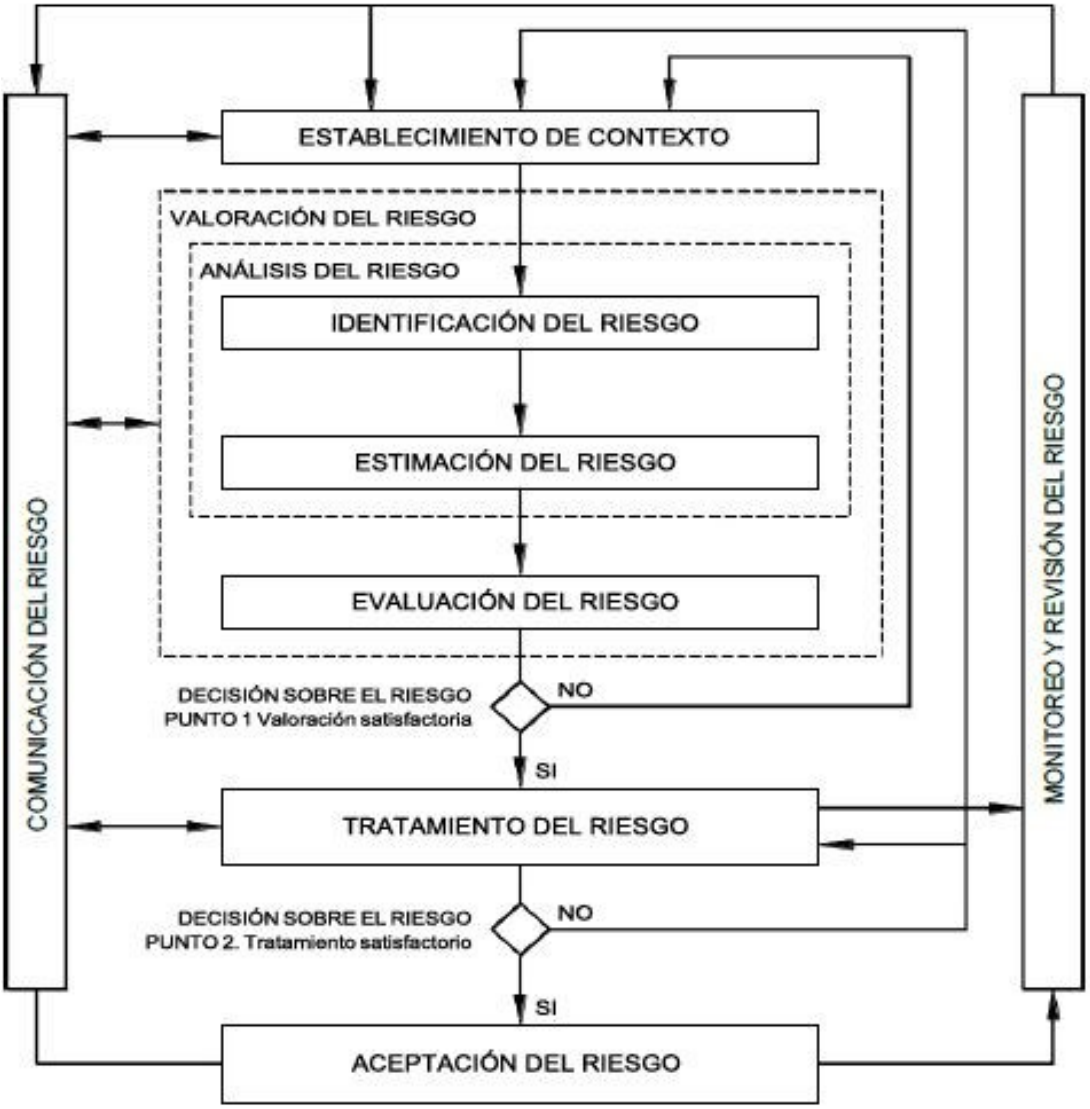
6 CONTENIDO DEL PLAN

El proceso de gestión de riesgo en la seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento.

La política de Administración del riesgo de la ESE se baja en las fases de la cartilla de administración del riesgo de la DAFP

- Contexto estratégico: determinar los factores externos e internos del riesgo.
- Identificación: identificación de causas, riesgo, consecuencias y clasificación del riesgo.
- Análisis: Calificación y evaluación del riesgo inherente.
- Valoración: identificación y evaluación de controles; incluye la determinación del riesgo residual.
- Manejo: determinar, si es necesario, acciones para el fortalecimiento de los controles.
- Seguimiento: evaluación integral de los riesgos.

Así el proceso para administración de los riesgos en seguridad de la información es el siguiente



Como lo ilustro imagen el proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o el tratamiento del mismo.

El contexto se establece como primera medida, luego se realiza la valoración del riesgo y si esta suministra información suficiente para determinar de manera eficaz las acciones que se necesitan para modificar los riesgos a un nivel aceptable entonces la labor está terminada y sigue el tratamiento del riesgo. Si la información no es suficiente, se llevará a cabo otra iteración de la valoración del riesgo con un contexto revisado (por ejemplo, los criterios de evaluación del riesgo los criterios para aceptar el riesgo o los criterios de impacto).

La eficacia del tratamiento de tratamiento del riesgo depende de los resultados de la valoración del riesgo. Es posible que el tratamiento del riesgo no produzca inmediatamente un nivel aceptable de riesgo residual en esta situación, si es necesaria, se puede requerir otra iteración de la valoración del riesgo con cambios en los parámetros del contexto (por ejemplo, criterios para la valoración del riesgo, de aceptación o de impacto del riesgo). La actividad de aceptación del riesgo debe asegurar que los riesgos residuales son aceptados explícitamente por los directores de la entidad. Esto es especialmente importante en una situación en la que la implementación de los controles se omite o se pospone, por ejemplo, por costos.

La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del MSPI

ETAPAS DEL MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDADDE LA INFORMACION
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

Tabla 3. Etapas de la Gestión del Riesgo a lo Largo del MSPI

Por lo tanto, La gestión del riesgo se realiza según lo descrito en la política de administración del riesgo de la E.S.E. Hospital Regional Sur Oriental

7 PLAN DE ACCIÓN

PLAN	COMPONENTE	N°	ACTIVIDAD	INDICADOR	SOPORTE	RESPONSABLE	FECHA INICIO - FIN
PLAN DE TRATAMIENTO DEL RIESGO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2022	Planificación	1	Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información	Alcance del Plan	Publicación del Plan	Sistemas	Enero 2022- enero 2022
PLAN DE TRATAMIENTO DEL RIESGO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2022	Identificación	2	Identificación de Amenazas y Vulnerabilidades	Identificación y valoración de nuevos Riesgos asociados a cada Categoría frente a Ciberamenazas.	Entrega de informe	Sistemas	Febrero 2022- Abril 2022
PLAN DE TRATAMIENTO DEL RIESGO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2022	Identificación	3	Determinación de riesgos	Asegurar que los riesgos identificados son monitoreados de acuerdo con la política de administración de riesgos, por parte de los cargos que lideran de manera transversal temas estratégicos de gestión (tales como jefes de planeación, financieros, contratación, TI, servicio al ciudadano, líderes de otros	Entrega de informe	Sistemas	Mayo 2022- junio 2022

				sistemas de gestión, comités de riesgos).			
PLAN DE TRATAMIENTO DEL RIESGO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2022	Evaluación	4	Monitoreo y revisión continua de riesgos	Seguimiento a los controles de la matriz de riesgos	Entrega de informe	Sistemas	Julio 2022- Agosto 2022
PLAN DE TRATAMIENTO DEL RIESGO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2022	Mejora Continua	5	Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información	proceso al día	Entrega de informe	Sistemas	septiembre 2022- diciembre 2022