E.S.E. HOSPITAL REGIONAL SUR ORIENTAL

PLAN DE TRATAMIENTO DEL RIESGO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TABLA DE CONTENDO

1 INTRODUCCIÓN

En la actualidad, la seguridad en la información es una de las preocupaciones más grandes que puede llegar a tener una compañía, ya que se refiere a garantizar la calidad, disponibilidad, veracidad y confidencialidad de su activo más preciado: la información.

El presente plan se elabora con el fin de dar a conocer como se realizará la implementación y socialización del componente de Gobierno en línea en el Eje Temática de la Estrategia en seguridad y privacidad de la información, el cual busca guardar los datos de los ciudadanos como un tesoro, garantizando la seguridad de la información.

2 OBJETIVOS

Establecer los criterios para la identificación, análisis, valoración, acciones y seguimientos a los riesgos potenciales que afecten la confiabilidad, disponibilidad e integridad de la información de la E.S.E. HRSO

2.1 OBJETIVOS ESPECÍFICOS

- Realizar el plan de trabajo específico validando los recursos con los que se cuentan actualmente la ESE HRSO para tener un plan de tratamiento de riesgo de seguridad y privacidad de la información.

- Aplicar las metodologías del DAPF e ISO respectivamente en seguridad y riesgo de la información

3 ALCANCE

Las políticas definidas el presente documento aplican a todos los procesos de la E.S.E. Hospital Regional Sur Oriental.

4 TÉRMINOS Y DEFINICIONES

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

Riesgo en la seguridad de la información: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo. [ISO/IEC Guía 73:2002]

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo. [ISO/IEC Guía 73:2002]

Reducción del riesgo: Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.[ISO/IEC Guía 73:2002]

Retención del riesgo: Aceptación de la pérdida o ganancia proveniente de un riesgo particular. [ISO/IEC Guía 73:2002]

Transferencia del riesgo: Compartir con otra de las partes la pérdida o la ganancia de un riesgo.[ISO/IEC Guía 73:2002]

Confidencialidad: La información debe ser clara sólo para los extremos autorizados.

Integridad: La información no debe ser alterada durante el transporte por las redes inseguras.

Continuidad: La información debe estar disponible para los usuarios auténticos.

Host: Un servidor, PC, estación de trabajo o dispositivo móvil que en algún momento posee una dirección de capa de red de la pila de protocolos TCP/IP.

5 NORMATIVIDAD VIGENTE

Norma NTC-ISO-IEC 27001

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

6 GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

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 del riesgos en seguridad de la información es el siguiente

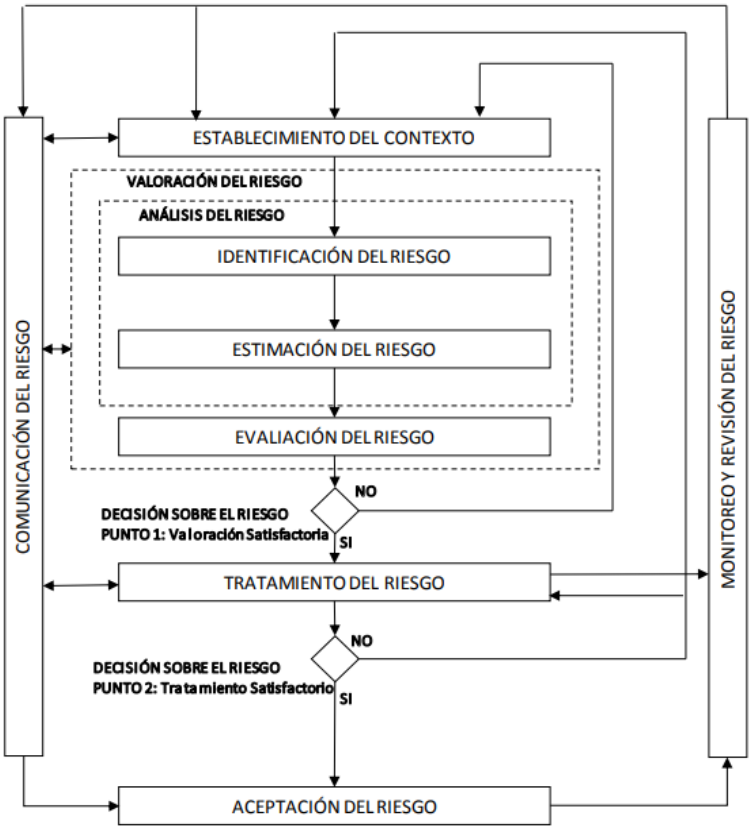

Imagen 2. Tomado de la NTC-ISO/IEC 27005

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 IMPLEMENTACIÓN

COMPONENTE	ACTIVIDADES	RESPONSABLE	META / ENTREGABLE	Fecha
PLANIFICACIÓN	Establecer el contexto estratégico de la ESE	Ingeniero de Sistemas	Diagnostico	Agosto 2020
	Socialización de la política de administración el riesgo a los líderes de procesos	Planeación	Acta de socialización	Septiembre 2020
	Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información	Ingeniero de Sistemas	Alcance del Plan	Agosto 2020
IMPLEMENTACIÓN	Realizar la Identificación de los Riesgos con los líderes del Proceso.	Lideres de procesos	Matriz de riesgos de seguridad de la información	Octubre 2020
EVALUACIÓN DEL DESEMPEÑO	Monitoreo y revisión continua de riesgos	Ingeniero de Sistemas	Seguimiento a los controles de la matriz de riesgos	Diciembre 2020
MEJORA CONTINUA	Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información	Ingeniero de Sistemas	proceso actualizado	Diciembre 2020

8 SEGUIMIENTO Y EVALUACIÓN

Es importante llevar el registro de acciones de seguimiento para cada uno de los controles implementados en el Plan de tratamiento, con el fin de evaluar la eficacia en su implementación, adelantando verificaciones como mínimo semestralmente o cuando se considere necesario, evidenciando todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones de tratamiento.

El monitoreo semestral debe estar a cargo de los responsables de los procesos, la Oficina de Control Interno y la Oficina de Tecnologías de la Información, aplicando y sugiriendo los correctivos y ajustes necesarios para propender por un efectivo manejo del riesgo de seguridad y privacidad de la información.