TABLA DE CONTENIDO

ELABORACIÒN	REVISIÓN	APROBACIÓN
Mary González Tirado **MARY YISSETH GONZÁLEZ TIRADO** Profesional de Apoyo al área de Sistemas	Isai Ruiz **ISAI MANUEL RUIZ ROMERO** Profesional de Apoyo al área de Planeación	**FARIEL EMIRO MEDINA DUQUE** Gerente (E)
Fecha: 20/01/2023	Fecha: 20/01/2023	Fecha: 30/01/2023

1. INTRODUCCIÓN

En la actualidad en toda entidad, institución u organización se está dando mayor prioridad a salvar, proteger y custodiar el activo de la información, debido a que los sistemas de información y los avances tecnológicos están siendo implementados en todas las empresas del mundo.

La ESE Hospital Regional de II Nivel de San Marcos, sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno en Línea que viene impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información dando cumplimiento al Decreto 1078 de 2015.

Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las empresas. Una entidad sin un plan de gestión de riesgos está expuesta a perder su información.

Todas las organizaciones deberían implementar planes para gestionar los riesgos que afectan a los sistemas de información, tecnologías de información y activos informáticos, considerando que en la actualidad los riesgos más comunes son generados por ataques dirigidos al software empresarial, afectando la disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación.

Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres, ya que cuando el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad de la entidad tras sufrir alguna pérdida o daño en la información de la misma.

Considerando la situación actual de la ESE Hospital Regional de II Nivel de San Marcos, para reducir los niveles de riesgo, es indispensable diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

2. OBJETIVO

Desarrollar un plan de gestión de seguridad y privacidad que permita minimizar los riesgos de pérdida de activos de la información en la ESE Hospital Regional de II Nivel de San Marcos

2.1. OBJETIVOS ESPECIFICOS

- Identificar las potenciales amenazas o vulnerabilidades asociadas a los activos de información.
- 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.
- Proteger los activos de información para disminuir los impactos generados ante posibles amenazas.
- Definir estrategias de seguridad que establezca planes para la clasificación de los activos de información.
- Realizar acciones de mejora para los activos clasificados como altamente críticos.
- Mejorar el nivel de exposición de los activos de información para eliminar o minimizar el riesgo dentro de la institución.
- Evaluar y comparar el nivel de riesgo actual con el impacto generado después de implementar el plan de gestión de seguridad de la información.
- Involucrar y comprometer a todos en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.

3. ALCANCE

Logar la concientización del personal de la ESE Hospital Regional de II Nivel de San Marcos en cuanto a los grandes riesgos de la seguridad de la información y la ciudadanía en general que tengan acceso a la información de la institución

4. DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- **Activos de información**: Los activos de información son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones **funcionen y consigan los objetivos** que se han propuesto por la alta dirección.

- **Alcance del SGSI**: Ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).

- **Análisis del riesgo:** Uso sistemático de la información para identificar las fuentes y estimar el riesgo. (Guía ISO/IEC 73:2002)

- **Confidencialidad**: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. (NTC 5411-1:2006)

- **Evaluación de riesgos**: Proceso de comparar el riesgo estimado contra el criterio de riesgo dado con el objeto de determinar la importancia del riesgo. (ISO/IEC Guía 73:2002)

- **Evento de seguridad de la información**: presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. (ISO/IEC TR 18044:2004)

- **Enfoque de evaluación de riesgos:** descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades,

probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables. (www.ISO27000.es)

- **Gestión del riesgo**: actividades coordinadas para dirigir y controlar una organización en relación con el riesgo. (Guía ISO/IEC 73:2002)

- **Incidente de seguridad de la información**: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. (ISO/IEC TR 18044:2004)

- **Informe de evaluación de riesgos:** estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización. (www.ISO27000.es)

- **Integridad propiedad:** Salvaguardar la exactitud y estado completo de los activos. (NTC 5411-1:2006)

- **ISO/IEC 27001:** ISO/IEC 27001 es un reconocido marco internacional de las mejores prácticas para un sistema de gestión de seguridad de la información. Le ayuda a identificar los riesgos para su información importante y pone en su lugar los controles apropiados para ayudarle a reducir el riesgo. (ISO/IEC 27001)

- **Manual de seguridad**: por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI. (www.ISO27000.es)

- **Procedimientos:** documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información. (www.ISO27000.es)

- **Riesgo residual:** nivel restante de riesgo después del tratamiento del riesgo. [Guía ISO/IEC 73:2002]

- **Seguridad de la información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad. (NTC-ISO/IEC 17799:2006)

- **SGSI**: Es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. (WWW.ISO27000.es)

- **Tratamiento del riesgo:** proceso de selección e implementación de medidas para modificar el riesgo. (Guía ISO/IEC 73:2002)

5. ROLES Y RESPONSABLES

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:

- **Alta Dirección**: aprueban las directrices para la administración del riesgo en la Entidad. La Alta Dirección es la responsable del fortalecimiento de la política de administración del riesgo.

- **Proceso Administración del Sistema Integrado de Gestión:** Genera la metodología para la administración del riesgo de la Entidad, coordina, lidera, capacita y asesora en su aplicación.

- **Responsables de los procesos:** Identifican, analizan, evalúan y valoran los riesgos de la entidad (por procesos e institucionales) al menos una vez al año. Si bien los Líderes SIG apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos, esto no quiere decir que el proceso de administración de riesgos este solo bajo su responsabilidad. Al contrario, cada responsable de proceso se encarga de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada funcionario que trabaja en dicho proceso.

• **Servidores públicos y contratistas:** Ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.

• **Control Interno:** Debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos

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

La ESE Hospital Regional de II Nivel de San Marcos, mediante el plan de tratamiento de riesgos de seguridad y privacidad de la información buscará identificar y evaluar los riesgos e incidentes que puedan afectar a la institución. Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios, en la ESE Hospital Regional de II Nivel de San Marcos se encontraron otras amenazas e impactos como los siguientes:

- Los puntos de red ubicados en cada oficina no son suficientes y se debe realizar estudio de necesidad para mejorar. No existe una estructura o protocolo fijo y establecido para la infraestructura física del hospital.
- Algunos cables de energía están sueltos, no están cerca a los escritorios o no son suficientes para la cantidad de equipos que tiene cada oficina, existe riesgo de pérdida de información en el caso que sean desconectados por accidente.
- Bebidas y alimentos cerca a los equipos de cómputo, poniendo en riesgo todos los equipos y sufrir un corto circuito.
- Existe un riesgo de pérdida de información por falta de equipos en algunas áreas.
- La información es llevada en memorias o discos duros portátiles personales, por ende, la información sale de la entidad corriendo riesgo de pérdida de información.
- Los documentos físicos que se manejan en la entidad no se han digitalizado por lo tanto están expuestos a perdidas y daños físicos debido a que los sitios de almacenamiento en las oficinas no son los adecuados.

7. MEDICIÓN DE RIESGO

Según la siguiente escala se busca hacer la medición de los riegos

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.

8. PROPUESTA DE SEGURIDAD

- Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias de las oficinas.
- Establecer políticas de seguridad y privacidad de la información como también las políticas de seguridad informática.
- Implementar y socializar las políticas de seguridad y privacidad de la información con el personal del hospital.
- Implementar el sistema de documentación digital en el hospital para reducir riesgos de pérdida de información física.
- Socializar con los empleados de la ESE la importancia del Plan de Continuidad de Negocio, para hacer frente a incidentes graves de seguridad en la Entidad, resumiendo de forma clara y sencilla cada una de las actividades a desarrollar dentro del plan.

9. PLAN SEGURO PARA EL ACOPIO DE COPIAS DE SEGURIDAD

Elaborar un procedimiento de la realización de los backups diarios.

Realizar diario Backups del sistema de información para mitigar el riesgo de pérdida de información, ante un daño de software o hardware.

Guardar en un equipo periférico los Backups.

Dejar en custodia equipo periférico donde se almacena el Backups.

Almacenar un Backups por lo menos una vez en la semana en una nube.

Contar con un plan alternativo que asegure la continuidad de la actividad del negocio en caso que ocurran incidentes graves.

10. MARCO LEGAL

Decreto 612 de 4 abril de 2018, “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado”.

Decreto 1008 de 14 de junio de 2018, “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital”.

Ley 594 de 14 de julio 2000, “Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”.

Decreto 1078 del 26 de mayo 2015, “Por medio del cual se expide el Decreto único reglamentario del sector de tecnologías de la información y las comunicaciones”.

Acuerdo 003 del 17 de febrero de 2015, “Por el cual se establecen lineamientos generales para las entidades del Estado en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el capítulo IV del Decreto 2609 de 2012".

Decreto 1083 del 26 de mayo 2015, “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”.

Ley 1474 del 12 de julio de 2011, “Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.”

11. REQUISITOS TÉCNICOS

Norma técnica colombiana NTC-ISO/IEC 27000 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. (SGSI). Visión General y Vocabulario

Norma técnica colombiana NTC-ISO/IEC 27001 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la seguridad de la información (SGSI). Requisitos

Guía 7 gestión de riesgos. Modelo de seguridad y privacidad de la información. Ministerio de Tecnologías de la información y las Comunicaciones, estrategias 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, estrategias de Gobierno en Línea.

Guía para la administración de riesgos en seguridad de la información. DNP. Departamento Nacional de Planeación.

12. SEGUIMIENTO Y EVALUACIÓN

Periódicamente deben revisarse los activos, impactos, amenazas, vulnerabilidades, cambios, que exijan valoración de los riesgos de seguridad de la información.

Es necesaria una supervisión activa que permita detectar nuevas amenazas, nuevas vulnerabilidades, nuevos impactos, mediante esquemas de seguimiento y medición al sistema de gestión y seguridad de la información.

13. CRONOGRAMA

	HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS	Codigo FR-PDI-01	Version 1	Pagina 1 de 1
	FORMATO FORMULACION DE PLANES DE TRABAJO		Fecha de Vigencia 09-11-2021	

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información

PERIODO: AÑO 2023

OBJETIVO	METAS	ACTIVIDAD	RESPONSABLE O LÍDER	CRONOGRAMA DE ACTIVIDADES	INDICADOR DE ESTRUCTURA, PROCESO Y RESULTADO	NIVEL DE CUMPLIMIENTO
Elaborar el diagnostico de tratamiento por area	Realizar auditoria del manejo que le dan a la información en cada una de las areas	Capacitar a cada lider de proceso sobre la importancia del tratamiento de la información	Lider de sistemas		No. De personal liderer asistente/ No. De total de personal *100	90%
Elaborar el alcance del plan por areas	Establecer cada una de la metas por areas especificas	Capacitar a cada lider de proceso sobre la importancia de la privacidad de la informacion	Lider de sistemas		No. De personal liderer asistente/ No. De total de personal *100	90%
Identificar los riesgos de seguridad y vulnerabilidad de la informacion por cada usuario que utiliza el sistema de informacion	Identificar, controlar, proteger los activos de la informacion definiendo, realizando y mejorando acciones para minimizar o eliminar el riesgo dentro de la institucion	Elaborar diagnostico de tratamiento	Lider de sistemas		No de riesgos subsanados/ No de riesgos encontrados	60%
Elaborar mapa de calor donde se encuentre los puntos de mayor riesgo de la informacion	Establecer cada uno de los puntos criticos donde exista riesgo de perdida de información	Mapa de calor con cada lineamiento	Lider de sistemas		cuadro de calor establecidos en los lineamientos de MINTIC	60%
Seguimiento y control actividades	Tener control sobre cada actividad de la institución	elaborar una bitacora de seguimiento	Lider de sistemas		informe final	80%

Elaboró	Revisó	Aprobó
MARY YISSETH GONZÁLEZ TIRADO Profesional de Apoyo al área de Sistemas	ISAI MANUEL RUIZ ROMERO Profesional de Apoyo al área de Planeación	FARIEL EMIRO MEDINA DUQUE Gerente (E)

14. CONTROL DE LOS CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO
10-01-2022	2	Con base a la ley 612 – 2018 se realizar Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información para la vigencia 2022.
30-01-2023	3	Con base a la ley 612 – 2018 se realizar Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información para la vigencia 2023.