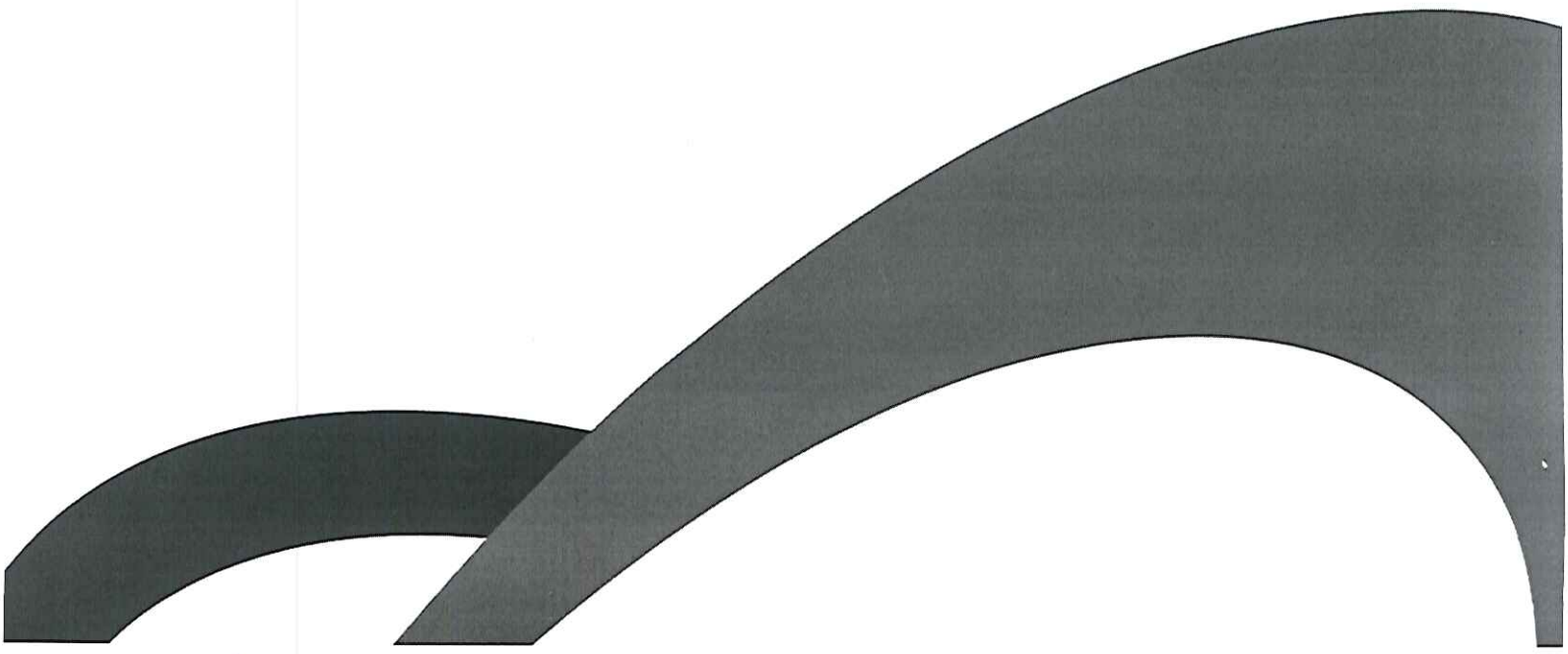
E.S.E. HOSPITAL
San Rafael
DE ITAGÜÍ

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



CONTENIDO

1. JUSTIFICACIÓN 3
2. OBJETIVO GENERAL 3
3. OBJETIVOS ESPECÍFICOS 3
4. RESPONSABLE(S) DEL PLAN 3
5. DEFINICIONES 3
6. META 5
7. DESARROLLO DEL PLAN 5
7.1 DESCRIPCIÓN 7
7.2 PROGRAMACIÓN DE ESTRATEGIAS Y ACTIVIDADES 11
8. PRESUPUESTO 11
9. EVALUACIÓN 11
10. DOCUMENTOS DE REFERENCIA 13
11. CONTROL DE DIVULGACIÓN 13
12. CONTROL DE CAMBIOS 13
13. ANEXOS 14

1. JUSTIFICACIÓN

La gestión del riesgo informático en una organización tiene como principal objetivo construir bases muy sólidas para alcanzar la misión, proteger la información y todos los activos informáticos. En el caso se la E.S.E Hospital San Rafael de Itagüí gran parte del procesamiento de información se hace con ayudas tecnológicas para brindar apoyo a la misión de la Institución, por lo tanto, es importante realizar una buena gestión del riesgo para proteger los activos de información.

Desde el área de sistemas sabemos la importancia de un buen proceso de gestión del riesgo como agregado fundamental de la seguridad de TI, motivo por el cual se crea la necesidad de gestionarlos ofreciendo una metodología, que permita planificar y mantener el riesgo bajo control, con un sistema de auditoría y evaluación.

2. OBJETIVO GENERAL

Concientizar a todos los responsables de los sistemas informáticos sobre la existencia de los riesgos y su obligación de mitigarlos.

3. OBJETIVOS ESPECÍFICOS

- Aplicar una metodología adecuada y mantener el ciclo PHVA.
- Apoyar la planeación de controles para mantener los riesgos aceptables.

4. RESPONSABLE(S) DEL PLAN

Plan a cargo del área de Sistemas de Información.

5. DEFINICIONES

Seguridad informática: Se entiende por riesgo de seguridad informática toda amenaza que explote alguna vulnerabilidad de uno o varios activos y pueda afectar el funcionamiento de un sistema, teniendo en cuenta la probabilidad que ocurra el evento y el impacto en

caso de materializarse, en alguna de las tres características principales de la seguridad informática las cuales se describen a continuación.

a) **Integridad:** Es una condición que garantiza que la información solo puede ser modificada por quien esté autorizado, esta debe ser consistente o coherente.

b) **Confidencialidad:** La información solo debe ser visible por quien la requiera y esté autorizado, hace referencia a la privacidad de la información.

c) **Disponibilidad:** Condición que garantiza que la información pueda ser accedida en cualquier momento que sea requerida. Está directamente relacionada con la continuidad del negocio.

Ciclo PHVA: El PHVA es un enfoque de gestión simple e iterativo para probar cambios en procesos o soluciones a problemas, e impulsar su optimización continua a través del tiempo.

DDoS: En seguridad informática, un ataque de denegación de servicio, llamado también ataque DoS, es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Malware: Se llama programa malicioso, programa malévolo, programa malintencionado, en inglés malware, badware o código maligno, a cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

Ransomware: Un ransomware o 'secuestro de datos' en español, es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción.

Cortafuegos: El cortafuegos o firewall en inglés, en el mundo de la informática es un sistema de seguridad para bloquear accesos no autorizados a un ordenador mientras sigue permitiendo la comunicación de tu ordenador con otros servicios autorizados.

6. META

Cumplir con el 90% de control en la gestión del riesgo informático de la E.S.E Hospital San Rafael de Itagüí para diciembre 15 del 2022.

7. DESARROLLO DEL PLAN

Componentes de la gestión de riesgos informáticos

las pautas de seguridad y correcta gestión del riesgo deben empezar desde la alta gerencia, concientizando a toda la institución de su importancia y el buen papel que desempeña cada uno de los integrantes. Algunas de las áreas en que habitualmente ha incursionado la seguridad se pueden definir así:

- Seguridad física.
- Control de accesos.
- Protección de los datos.
- Seguridad en las redes.

Pasos para mitigación de riesgos

1. **Sistema de caracterización:** En este paso determinamos el alcance de la evaluación de los riesgos, debe realizar la identificación de los activos a tener en cuenta: Hardware, software, la información, personas que apoyan y utilizan el sistema de TI, diagnóstico de los sistemas, sensibilidad de los datos y controles actuales entre otros. Para poder obtener esta información se hace necesario contar con un instrumento de recolección de datos en la E.S.E Hospital San Rafael de Itagüí.
2. **Identificación de las amenazas:** Identificamos las posibles ocurrencias en los diferentes eventos o sitios sobre los sistemas o activos tecnológicos que pertenecen al hospital, una vez identificadas dichas amenazas se investigan sobre el historial de este tipo de amenazas, y se busca una posible solución que mitigue el riesgo; estas amenazas pueden ser de diferente índole, como ataques externos, desastres naturales o errores humanos.

- **Ataques externos:** Los ciberdelincuentes siempre tienen en su punto de mira a las empresas y sus sistemas, con el objetivo de robar información (bancaria o de otra índole comercial o personal), tirar sus sistemas o utilizar sus recursos. Dos de las mayores amenazas que reciben las empresas hoy en día son ataques de denegación de servicio DDoS (inutilizan los sistemas informáticos de la Institución) o ataques con malware de tipo ransomware (encriptan los datos de la empresa, solicitando un rescate económico en criptomonedas para liberarlos).

- **Errores humanos:** La intervención humana en los procesos informáticos siempre está expuesta a que se cometan errores (intencionados o no intencionados). Por ejemplo, un colaborador del hospital sin los conocimientos suficientes, o con privilegios superiores a los de su función, puede realizar acciones que comprometan los datos o produzcan un malfuncionamiento en los sistemas la E.S.E Hospital San Rafael de Itagüí.
- **Desastres naturales:** Es posible que se den situaciones que pongan en peligro los activos informáticos de la empresa como inundaciones o sobrecargas en la red eléctrica.

3. **Detectar vulnerabilidades:** Las vulnerabilidades se presentan en activos informáticos y presentan un riesgo para la información. Estas debilidades pueden aparecer en cualquiera de los activos informáticos, esta identificación se realiza por medio de unas pruebas de seguridad y una lista de verificación de acuerdo con el sistema o activo evaluado, estas vulnerabilidades están contempladas a detalle en la política de seguridad de la información de la E.S.E Hospital San Rafael de Itagüí.
4. **Medidas de prevención y control:** Una vez se tengan identificadas las amenazas y vulnerabilidades de los sistemas de la E.S.E Hospital San Rafael de Itagüí y se tengan definidos todos los riesgos y sus consecuencias, deben establecerse una serie de medidas y tratamientos de riesgo con dos objetivos claros:
    - Evitar que se produzca el riesgo.
    - Minimizar su impacto en caso de que llegue a producirse.

Medidas para evitar y mitigar riesgos informáticos

a. Instalación de software de seguridad y cortafuegos (por software o hardware).
b. Implementación de sistemas de seguridad en la nube automatizados.
c. Añadir protocolos de seguridad para reforzar la seguridad de las contraseñas.
d. Revisión de los roles y privilegios de los usuarios (con especial cuidado en la asignación de los roles con mayores privilegios, como los administradores).
e. Contratación de un seguro que cubra los daños ocasionados.
f. Implementación de sistemas alternativos o duplicados para asegurar la disponibilidad del sistema (high availability).

Clasificación de los riesgos

- **Alto:** Si una observación o hallazgo se evalúa como de alto riesgo, hay una fuerte necesidad de medidas correctivas. Un sistema existente no puede continuar operando sino hay un plan de acción correctivo que debe ponerse en marcha tan pronto como sea posible.
- **Medio:** Si una observación está clasificada como de riesgo medio, las acciones correctivas son necesaria y un plan debe ser desarrollado para incorporar estas acciones dentro de un período razonable de tiempo.
- **Bajo:** Si una observación es descrita como de bajo riesgo, el sistema debe determinar si aún se requieren acciones correctivas o deciden aceptar el riesgo.

Matriz de riesgo: Se debe generar la matriz del riesgo a cada uno de los activos, se debe categorizar de una manera organizada con el fin de sacar los reportes, de acuerdo con la probabilidad de que se materialice el riesgo y el impacto que puede ocasionar, no solo económico también de imagen, prestigio perdida de clientela entre otros, la matriz se puede realizan de manera cualitativa o cuantitativa.

7.1 DESCRIPCIÓN

Gobierno de seguridad

Un buen gobierno de seguridad tiene su base en una excelente estructura organizacional alineada a la política de gestión de la calidad de la institución, esta estructura es un organismo dinámico que puede cambiar según la estructura y las necesidades de la institución. En todo momento debe ser clarificada con el fin de que se conozca la cadena de

toma de decisión de cada uno de los temas necesarios para la gestión de la seguridad de la información.

Por tal motivo se hace necesario la creación de una matriz RACI donde las actividades están responsabilizadas por un rol. Los tipos de responsabilidades usados son los siguientes:

Tipo de responsabilidad		Descripción
R	Responsable	Este rol corresponde a quien efectivamente realiza la tarea. Lo más habitual es que exista sólo un encargado (R) por cada tarea.
A	Técnico	Este rol se responsabiliza de que la tarea se realice y es quien debe rendir cuentas sobre su ejecución. Sólo puede existir una persona que deba rendir cuentas (A) de que la tarea sea ejecutada por su responsable (R).
C	Consultado	Este rol posee alguna información o capacidad necesaria para realizar la tarea. Se le informa y se le consulta información (comunicación bidireccional)
I	Informado	Este rol debe ser informado sobre el avance y los resultados de la ejecución de la tarea. A diferencia del consultado (C), la comunicación es unidireccional.

Esta es la estructura de la E.S.E Hospital San Rafael de Itagüí

Estructura de roles

Rol	Objetivo

Comité de Gerencia de la información	• El comité de gerencia de la información toma las responsabilidades en la E.S.E Hospital San Rafael de Itagüí del Comité de seguridad de la información. • Como objetivo principal para la seguridad de la información este comité realiza la aprobación de lineamientos estratégicos en cuanto a seguridad de la información, garantiza los recursos y la toma de decisiones orientadas al cumplimiento de la estrategia por ellos definida.
Agente de seguridad de información.	• Tiene la responsabilidad de guiar y realizar el seguimiento de la implementación de los planes de seguridad definidos.
Administrador de seguridad de la información	• Tienen la responsabilidad de la gestión de los esfuerzos de seguridad de la información, encargado de labores específicas de seguridad.
Líderes de procesos	• Tienen la responsabilidad de dar la cobertura de los lineamientos de seguridad a cada uno de sus procesos operacionales.

Comité de gerencia de la información

Objetivo	• Aprobar los lineamientos estratégicos en cuanto a seguridad de la información y garantizar los recursos para su cumplimiento.
Principios de operación	• El comité se debe reunir de forma mensual o cuando una eventualidad lo requiera. El número de miembros del comité se limita a un grupo relativamente pequeño de líderes estratégicos y tácticos para asegurar la comunicación y toma de decisiones apropiado.

Responsabilidades	• El comité es el responsable de que las decisiones de seguridad de la información estén orientadas al apoyo de las decisiones estratégicas.

7.2 PROGRAMACIÓN DE ESTRATEGIAS Y ACTIVIDADES

ESTRATEGIAS	ACTIVIDADES	RESPONSABLES	PLAZOS	MEDIOS DE VERIFICACIÓN
CAPACITACIONES	Capacitación de manejo de equipos tecnológicos en los puestos de trabajo del personal administrativo	Área de sistemas	Mayo 2-6	Formato de lista de asistencia
	Capacitación de uso correcto de artefactos tecnológicos externos al personal administrativo del hospital	Área de sistemas	Julio 11-15	Formato de lista de asistencia

8. PRESUPUESTO

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
No aplica	No aplica	No aplica	No aplica
		TOTAL	No aplica

9. EVALUACIÓN

INDICADOR 01 - ATAQUES INFORMÁTICOS A LA ENTIDAD.	
IDENTIFICADOR	SGIN01
DEFINICIÓN	
Porcentaje de ataques informáticos recibidos en la entidad que impidieron la prestación de alguno de sus servicios.	
OBJETIVO	
Busca conocer el número de ataques informáticos que recibe la entidad	
TIPO DE INDICADOR	
Indicador de Cumplimiento	

DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
VSI01: ¿Cuántos ataques informáticos recibió la entidad en el último año?	VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Herramientas de Monitoreo/Usuarios Internos.
VSI02: ¿Cuántos ataques recibió la entidad en el último año que impidieron la prestación de algunos de los servicios que la entidad ofrece a los ciudadanos y empresas?		Herramientas de Monitoreo/Usuarios Internos.

METAS			
CUMPLE	1	NO CUMPLE	0
OBSERVACIONES			
N/A			

INDICADOR 02 - POLÍTICAS DE DISPONIBILIDAD DEL SERVICIO Y LA INFORMACIÓN		
IDENTIFICADOR	SGIN02	
DEFINICIÓN		
Grado de cumplimiento de las políticas de disponibilidad del servicio y la información.		
OBJETIVO		
Busca identificar el nivel de implementación de políticas de disponibilidad del servicio y la información.		
TIPO DE INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	FORMULA	FUENTE DE INFORMACIÓN
VSI02: ¿La entidad verifica que los lineamientos, normas y/o estándares orientados a la continuidad en la prestación de los servicios se cumplan?	VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Usuarios Internos
VSI02: ¿La entidad ha		Usuarios Internos

implementado mecanismos para que los servicios de Gobierno en línea tengan altos índices de disponibilidad?			
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			
N/A			

10. DOCUMENTOS DE REFERENCIA

CÓDIGO	NOMBRE
NTC ISO/IEC 27001	sistema de gestión de seguridad de información
ISO 27004	Evaluación de la Seguridad de la Información

11. CONTROL DE DIVULGACIÓN

PROCESO- SERVICIO/ÁREA	ESTRATEGIA DE DIVULGACIÓN
Gerencia, Asesores de Gerencia, Coordinadores, Lideres, jefes de Áreas.	Se realizará una presentación concisa de los principales componentes del PETI, partiendo del diagnóstico inicial, explicando claramente las estrategias y proyectos como resultado del trabajo de análisis realizado.
Funcionarios de la E.S.E Hospital San Rafael de Itagüí.	Su divulgación se realizará a través de la realización de presentaciones sobre el impacto del PETI en la organización. Haciendo uso de: • Página WEB • Correo electrónico Institucional • Intranet • Circulares Internas

12. CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCIPCIÓN DEL CAMBIO	SOLICITANTE

2022-01-22	01.	Creación de documentación	Samuel Guevara Mejía Líder Sistemas

13. ANEXOS

CÓDIGO	NOMBRE
NA	NA

Elaboró/actualizó:	Revisó:	Aprobó:
Samuel Guevara Mejía Líder Sistemas	Jony Sneider Rojas Chavarría Jefe Oficina Asesora Planeación y Calidad Luis Fernando Cadavid Tejada Jefe Oficina Asesora Jurídica	Diego León Muñoz Zapata Gerente
Firma:	Firma:	Firma:
Fecha: 2022-01-20	Fecha: 2022-01-21	Fecha: 2022-01-22