E.S.E. HOSPITAL
San Rafael
DE ITAGÜÍ

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

2024

CONTENIDO

1. JUSTIFICACIÓN

El principal objetivo es evaluar las posibles acciones cuyo fin es la mitigación de los riesgos existentes teniendo en cuenta los criterios de aceptación de los riesgos definidos por la ESE HOSPITAL SAN RAFAEL DE ITAGUI, estableciendo controles y medidas efectivas, viables y transversales, con el propósito de preservar la disponibilidad, integridad y confidencialidad de la información.

El plan se basa en una orientación estratégica que requiere del desarrollo de una cultura de carácter preventivo, que, al comprender el concepto de riesgo, así como el contexto, se planeen acciones que reduzcan la afectación a la ESE HSRI en caso de materialización, buscando desarrollar estrategias para su identificación, análisis, tratamiento, evaluación y monitoreo de los riesgos con gran objetividad.

El área de sistemas es conocedora de la importancia de un buen proceso para la 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. ENFOQUE DIFERENCIAL

El principio de enfoque diferencial reconoce que hay poblaciones con características particulares debido a su edad, género, raza, etnia, condición de discapacidad y víctimas de la violencia para las cuales el Sistema de Seguridad Social en Salud - SGSSS ofrecerá especiales garantías y esfuerzos encaminados a la eliminación de situaciones de discriminación y marginación. Para lo que la E.S.E Hospital San Rafael de Itagüí implementa el manual ‘’Atención en salud con enfoque diferencial’’ MN-04-AT.

Los riesgos derivados de las nuevas tecnologías y su incidencia en el teletrabajo traducidos como los nuevos riesgos psicosociales para la salud de los teletrabajadores. Tales riesgos que deben ser seriamente investigados por las consecuencias negativas que repercute en el teletrabajador son:

- "Síndrome de fatiga informativa" o "tecnoestrés".
- "Tecnoansiedad", es una sensación de tensión y malestar psicológico que se experimenta ante el uso presente o posible de algún tipo de tecnología
- "Tecnoadicción", El uso indiscriminado de la tecnología puede generar tecno adicción y además otras consecuencias más graves.
- Tecnofatiga", es un tipo de tecnoestrés que afecta negativamente a quien la padece, causando una sensación de malestar físico y mental muy desagradable como consecuencia de un uso excesivo de las tecnologías de la información y la comunicación (TIC).

- Tecnofobia". Asimismo, se explican las ventajas, desventajas, descripción, características, causas y consecuencias de cada uno de los riesgos derivados por el uso de las nuevas tecnologías.

3. OBJETIVO GENERAL

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación que el MINTIC pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

4. OBJETIVOS ESPECÍFICOS

- Aplicar una metodología adecuada y mantener el ciclo PHVA.
- Apoyar la planeación de controles para mantener los riesgos aceptables.
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.
- Gestionar riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de acuerdo con los contextos establecidos en la E S E HOSPITAL SAN RAFEL DE ITAGUI.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación.

5. RESPONSABLE(S) DEL PLAN

Área de Sistemas de Información de la E.S.E Hospital San Rafael de Itagüí.

6. DEFINICIONES

AMENAZA: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

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.

CONTROL O MEDIDA: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

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.

IMPACTO: son las consecuencias que genera un riesgo una vez se materialice.

MALWARE: Se llama programa malicioso, programa malévolo, programa malintencionado, es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas, 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.

PROBABILIDAD: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

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.

RIESGO: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

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 como son:

- **INTEGRIDAD:** Es una condición que garantiza que la información solo puede ser modificada por quien esté autorizado, esta debe ser consistente o coherente.
- **CONFIDENCIALIDAD**: La información solo debe ser visible por quien la requiera y esté autorizado, hace referencia a la privacidad de la información.
- **DISPONIBILIDAD:** Condición que garantiza que la información pueda ser accedida en cualquier momento que sea requerida. Está directamente relacionada con la continuidad del negocio.

SNIFFER: es una herramienta de software o hardware que permite al usuario supervisar su tráfico en Internet en tiempo real y capturar todo el tráfico de datos que entran y salen de su equipo.

VULNERABILIDAD: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

7. META

Cumplir el 90% de las actividades propuestas el plan durante la vigencia.

8. 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.

8.1. ETAPAS

El primer paso para proteger la empresa contra las amenazas es comprender dónde se encuentran sus vulnerabilidades, los tipos de datos que controla y dónde y cómo se almacenan.

La siguiente etapa consiste en analizar dónde se encuentran los riesgos en sí. Al analizar los riesgos de las áreas vulnerables y comprender el impacto que pueden tener en las operaciones, se estará mejor preparado para encontrar soluciones que mitiguen el riesgo para el negocio.

Es necesario clasificar los riesgos, algunos son peores que otros. Es necesario determinar cómo se superpone cada uno de ellos y cómo repercute en el potencial de ataque de un actor malicioso. La mejor manera de hacerlo es calcular.

Nivel de riesgo = Probabilidad de una violación de datos X Impacto financiero de una violación de datos. Por ejemplo, en caso de un accidente es probable que la información personal y los secretos comerciales tengan prioridad.

Fijar una tolerancia al riesgo y establecer estrategias de gestión de riesgos informáticos (TI). Establecer tolerancia significa decidir si aceptar, transferir, mitigar o rechazar el riesgo. La estrategia de gestión de riesgos informáticos consiste en que se asegure de que tanto el líder de sistemas como los equipos de trabajo saben con quién deben ponerse en contacto y qué deben hacer en caso de desastre. Debe asegurarse de que los datos tienen una copia de seguridad y de tener un Plan de Recuperación de Desastres para que los sistemas puedan volver a estar en línea de la forma más rápida y eficiente posible.

Mitigar el riesgo. El almacenamiento en la nube puede convertirse en una solución segura, proporcionando tanto la seguridad como la accesibilidad que su empresa necesita. Otras formas de mitigar el riesgo incluyen la subcontratación de la gestión de riesgos de TI, que no sólo puede

proporcionar servicios de TI, sino que otorga acceso a funciones de seguridad avanzadas y equipos de vigilancia las 24 horas del día.

Identificar las vulnerabilidades. El riesgo es una amenaza que debe reevaluarse constantemente para garantizar la protección de su empresa, sus sistemas y sus datos.

8.2. METODOLOGIA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información.

ACTIVIDAD	TAREA	RESPONSABLE	FECHA DE INICIO	FECHA DE FINALIZACIÓN
Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	Equipo de gestión de riesgos	01/01/2024	31/12/2024
Sensibilización	Socialización guía y herramienta.	Equipo de gestión de riesgos	01/03/2024	16/03/2024
Identificación de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	Gestión de riesgos de seguridad y privacidad de la información, seguridad Digital y continuidad de la operación.	Equipo de gestión de riesgos	01/01/2024	31/12/2024
	Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Equipo de gestión de riesgos	Trimestral	Trimestral
Aceptación de riesgos identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	Equipo de gestión de riesgos	Trimestral	Trimestral
Publicación	Publicación matriz de Riesgos (SIMIG)	Equipo de gestión de riesgos	Semestral	Semestral
Seguimiento fase de tratamiento	Seguimiento, estado planes de tratamiento de riesgos identificados y verificación de evidencia.	Equipo de gestión de riesgos	01/01/2024	31/12/2024

ACTIVIDAD	TAREA	RESPONSABLE	FECHA DE INICIO	FECHA DE FINALIZACIÓN
Evaluación de riesgos residuales	Evaluación de riesgos residuales	Equipo de gestión de riesgos	Trimestral	Trimestral
Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Equipo de gestión de riesgos	Semestral	Semestral
	Actualización guía Gestión de riesgos seguridad de la información de acuerdo con los cambios solicitados	Equipo de gestión de riesgos	Semestral	Semestral
Monitoreo y revisión	Generación, presentación y reporte de indicadores	Equipo de gestión de riesgos	Semestral	Semestral

8.3. PASOS PARA MITIGACIÓN DE RIESGOS

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.

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 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.

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.

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

- Instalación de software de seguridad y cortafuegos (por software o hardware).
- Implementación de sistemas de seguridad en la nube automatizados.
- Añadir protocolos de seguridad para reforzar la seguridad de las contraseñas.
- Revisión de los roles y privilegios de los usuarios (con especial cuidado en la
- Asignación de los roles con mayores privilegios, como los administradores).
- Contratación de un seguro que cubra los daños ocasionados.
- 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 generar reportes de acuerdo con la probabilidad de que se materialice el riesgo y el impacto que puede ocasionar no solo económico, sino también de imagen, prestigio, perdida de clientela entre otros, la matriz se puede realizan de manera cualitativa o cuantitativa.

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		DESCRIPCION
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	**TECNICO**	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.

- **ESTRUCTURA DE ROLES**

ROL	OBJETIVO
COMITE DE DESEMPEÑO INSTITUCIONAL	El comité de Desempeño Institucional es el que opera el Sistema Integrado de Gestión donde se encuentra el Proceso de Sistemas de 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 INFORMACION	Tiene la responsabilidad de guiar y realizar el seguimiento de la implementación de los planes de seguridad definidos.
ADMINISTRADOR DE SEGURIDAD DE LA INFORMACION	Tienen la responsabilidad de la gestión de los esfuerzos de seguridad de la información, encargado de labores específicas de seguridad.
LIDERES 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.

8.4. PROGRAMACIÓN DE ESTRATEGIAS Y ACTIVIDADES

ESTRATEGIAS	ACTIVIDADES	RESPONSABLES	PLAZOS	MEDIOS DE VERIFICACION
CAPACITACIONES	Capacitación de manejo de equipos tecnológicos en los puestos de trabajo del personal administrativo y asistencial.	Área de sistemas	Trimestralmente	Formato de lista de asistencia
	Capacitación de uso correcto de artefactos tecnológicos externos al personal administrativo del hospital.	Área de sistemas	Trimestralmente	Formato de lista de asistencia

9. PRESUPUESTO

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
N/A	N/A	N/A	N/A
		TOTAL	**N/A**

10. EVALUACIÓN

INDICADOR 01 - ATAQUES INFORMÁTICOS A LA ENTIDAD.		
IDENTIFICADOR	SGIN01	
DEFINICIÓN		
Porcentaje de peticiones denegadas de tráfico malicioso de red.		
OBJETIVO		
Busca conocer el número de peticiones maliciosas que recibe la entidad		
TIPO DE INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENTE DE INFORMACIÓN**

INDICADOR 01 - ATAQUES INFORMÁTICOS A LA ENTIDAD.		
VSI01: ¿Cuántos peticiones recibió la entidad en el último año?	VSI01/ VSIO2 * 100%	Herramientas de Monitoreo/Usuarios Internos.
VSI02: ¿Cuántos peticiones maliciosas 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 implementado mecanismos para que los servicios de Gobierno en línea tengan altos índices de disponibilidad?		Usuarios Internos

11. 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

12. 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 Plan, 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 Plan en la organización. Haciendo uso de: • Página WEB • Correo electrónico Institucional • Intranet • Circulares Internas

13. CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCIPCIÓN DEL CAMBIO	SOLICITANTE
2022-01-17	1	Formulación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2022	Samuel Guevara Mejía Líder Sistemas
2023-01-30	2	Formulación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2023	Samuel Guevara Mejía Líder Sistemas
2024-01-26	3	Formulación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024	Henry González S. Líder Sistemas

14. ANEXOS

CÓDIGO	NOMBRE
N/A	N/A

Elaboró/actualizó: Henry González Sosa Líder Sistemas	Revisó: Jony Sneider Rojas Chavarría Jefe Oficina Asesora Planeación y Calidad Luis Fernando Cadavid Tejada Jefe Oficina Asesora Jurídica	Aprobó: Diego León Muñoz Zapata Gerente
Firma:	Firma:	Firma:
Fecha: 2024-01-24	Fecha: 2024-01-25	Fecha: 2024-01-26