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

PLA-SIN-06

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado "Superintendencia Nacional de salud"

Contenido

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

OBJETIVO

Definir el Plan de Tratamiento de Riesgos de Seguridad de la Información en la ESE Hospital Geriátrico San Miguel para aplicar controles que buscan minimizar su impacto en la organización generando confianza en el manejo de la información institucional.

OBJETIVOS ESPECIFICOS

- 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 Entidad.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación.

ALCANCE

Inicia con la identificación de los riesgos de seguridad de la información y finaliza con los controles implementados.

CAMPO DE APLICACIÓN

Aplica para los procesos y servicios de la E.S.E. Hospital Geriátrico San Miguel. El Plan de Tratamiento de Riesgo considerará los riesgos de los niveles Alto y Extremo según los lineamientos definidos por el Ministerio TIC.

ACTUALIZACIÓN

El plan debe ser actualizado por lo menos una vez al año por mejoramiento continuo, cuando cambie la normatividad o se evidencien nuevas acciones que conlleven a la aplicación de nuevos controles.

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

DEFINICIONES

- **CONFIDENCIALIDAD:** Capacidad de no divulgar o publicar información sensible de una empresa a personas no autorizadas. Como ejemplo tenemos los accesos no autorizados, fugas y filtraciones de información. Al tener fallo en esa característica de la información, supone el incumplimiento de leyes y compromisos en relación con la custodia de datos, además que la organización evidenciaría que no es competente para el manejo de datos.
- **INTEGRIDAD:** Característica de mantener la información de manera intacta sin tener modificaciones. Al fallar este elemento afecta directamente el correcto funcionamiento de la organización.
- **DISPONIBILIDAD**: Consiste en tener los activos disponibles cuando se requiere su uso. La falta de este atributo evidencia una interrupción del servicio y afecta la productividad de la organización.
- **ACTIVOS DE LA INFORMACIÓN:** Elementos de valor que posee la empresa como son, datos, software, hardware, elementos de redes y comunicaciones, infraestructura y recursos humanos.
- **INFORMACIÓN:** Datos que maneja la empresa ya sea en forma digital o impresa. Riesgo: Aquella eventualidad que imposibilita el cumplimiento de un objetivo.
- **RIESGO:** Posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso.
- **AMENAZAS:** Cualquier situación que se puede presentar en la entidad dañando un activo de información, mediante la explotación de una vulnerabilidad.
- **VULNERABILIDAD:** Es toda debilidad del sistema informático que puede usarse para causar un daño. Corresponde a las ausencias o fallas en los controles para proteger un activo.
- **IMPACTO:** Es el alcance del daño que se produce en un activo cuando sucede una amenaza.
- **ANÁLISIS DE RIESGOS:** Es fundamental en el proceso de implantación de un SGSI, ya que en esta fase se cuantifica la importancia de los activos para la seguridad de la organización. Controles: Medida de protección que se implementa para minimizar los riesgos.
- **FUENTE DE RIESGO**: Elemento que, por sí solo o en combinación con otros, tiene el potencial de generar riesgo.
- **GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **INCERTIDUMBRE**: Es el desconocimiento si un hecho o situación ocurrirá
- **MECANISMOS DE PROTECCIÓN DE DATOS PERSONALES:** Lo constituyen las distintas alternativas con que cuentan las Entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimizarían o cifrado.
- **NIVEL DE RIESGO**: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser: Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

- **PLAN DE TRATAMIENTO DE RIESGOS:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000)
- **RIESGO DE 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. (ISO/IEC 27000).
- **TOLERANCIA DEL RIESGO:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad**.**
- **TRAZABILIDAD:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad. (ISO/IEC 27000)**.**

GENERALIDADES

De acuerdo con la norma ISO 27001, El riesgo está catalogado como la “Combinación de probabilidad de ocurrencia de un evento de seguridad de la información y su resultante consecuencia”, así mismo, se pueden establecer varias definiciones. Un ejemplo puede darse como “la posibilidad de sufrir daños o pérdidas.

La amenaza es un componente del riesgo y se puede considerar como: un agente de amenazas ya sea humano o no humano, toma alguna acción, como identificar y explotar una vulnerabilidad, que ofrece un resultado inesperado y no deseado. Dichos resultados generan impactos negativos en la empresa. Los impactos pueden incluir: pérdida de ingresos o clientes, pérdida de diferenciación de mercado, costos de respuesta y recuperación por el incidente y el costo de pagar multas o sanciones reguladoras.

ROLES Y RESPONSABILIDADES

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**: aprueba 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.
- **Sistema Integrado de Gestión**: Realiza acompañamiento para la aplicación de la metodología seleccionada para la administración del riesgo de la Entidad, coordina, lidera, capacita y asesora en su aplicación.
- **Responsables de los procesos y subprocesos**: Identifican, analizan, evalúan y valoran los riesgos de la entidad (por procesos e institucionales) al menos una vez al año. Si bien los Líderes 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

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

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. Las personas que trabajan en cada proceso mejor conocen los riesgos del desarrollo de sus actividades.

- **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.
- **Asesor de Control Interno**: Debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos.
- **Equipo de gestión de riesgos y de incidentes de seguridad de la información**: Las funciones de este equipo estarán dadas de la siguiente manera:

  - Detección de Incidentes de Seguridad: Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información.
  - Atención de Incidentes de Seguridad: Recibe y resuelve los incidentes de seguridad de acuerdo con los procedimientos establecidos.
  - Anuncios de Seguridad: Deben mantener informados a los funcionarios, contratistas o terceros sobre las nuevas vulnerabilidades, actualizaciones a las plataformas y recomendaciones de seguridad informática a través de algún medio de comunicación (Web, Intranet, Correo).
  - Auditoría y trazabilidad de Seguridad Informática: El equipo debe realizar verificaciones periódicas del estado de la plataforma para analizar nuevas vulnerabilidades y brechas de seguridad.
  - Clasificación y priorización de servicios expuestos: Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.
  - Investigación y Desarrollo: Deben realizar la búsqueda constante de nuevos productos en el mercado o desarrollo de nuevas herramientas de protección para combatir brechas de seguridad, y la proposición de nuevos proyectos de seguridad de la información.

Este grupo está conformado por:

- Encargado del proceso Planeación y Calidad o su delegado.
- Líder de Gestión de Talento Humano o su delegado.
- Encargado del proceso en Sistemas de Información. (Líder de grupo)
- Líder del proceso de Control Interno o su delegado.
- Líder del Proceso de Gestión Documental o su delegado.

METODOLOGIA

Para la realización del análisis de riesgos de seguridad informática se toma como metodología la “Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital” propuesta por el Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República y el Ministerio

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

de Tecnologías de la Información y Comunicaciones, brindando una seguridad razonable frente al logro de sus objetivos.

Al aplicar esta metodología permitirá cumplir con requisitos legales y reglamentarios, proteger los recursos del Estado, identificar y tratar los riesgos en todos los niveles de la entidad.

La administración del Riesgo comprende el conjunto de Elementos de Control y sus interrelaciones, para que la institución evalúe e intervenga aquellos eventos, tanto internos como externos, que puedan afectar de manera positiva o negativa el logro de sus objetivos institucionales. La administración del riesgo contribuye a que la entidad consolide su Sistema de Control Interno y a que se genere una cultura de Autocontrol y autoevaluación al interior de esta. (Tomado de Guía para la Administración del Riesgo)

Para la realización de la Gestión de Riesgos en Seguridad Digital se requiere realizar las siguientes actividades:

DESCRIPCIÓN

Actividad	Tarea	Responsable	Fecha Inicio	Fecha Fin
Mejoramiento	Identificación de oportunidad de mejora y diseño de controles en la matriz de riesgo	Equipo de Gestión de riesgos e incidentes de seguridad de la información	Marzo 2024	Mayo 2024
Monitoreo y revisión	Generación, presentación y reporte de riesgos identificados durante el año en curso.	Encargado del proceso en Sistemas de Información	Mayo 2024	Dic 2024
	Verificación del cumplimiento de los controles definidos en la matriz de riesgos	Equipo de Gestión de riesgos e incidentes de seguridad de la información	Marzo 2024	Dic 2024
Comunicación	Presentación a Comité de Gestión y Desempeño de avances en el cumplimiento de controles definidos en la matriz de riesgos	Encargado del proceso en Sistemas de Información	Abril 2024	Dic 2024
	Publicación de seguimiento a matriz de riesgos	Encargado del proceso en Sistemas de Información	Junio 2024	Junio 2024

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”

Actualizado por:	Revisado por:	Aprobado por:
ORIGINAL FIRMADO	ORIGINAL FIRMADO	ORIGINAL FIRMADO
Jhonny Torres **Sistemas e Información**	María del Mar Medina Osorio **Auxiliar Gestión y Mejora**	Carolina Osorio Gonzalez **Subgerente Administrativa y Financiera**
Fecha:22/01/2024	**Fecha:22/01/2024**	**Fecha:22/01/2024**

VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA DE VIGENCIA
01	Creación del plan	Enero 2023
02	Actualización Plan	Enero 2024

Nit 890.303.448-6
Carrera 70 No. 2A - 04 Cali – Colombia
PBX +57 (2) 339 0821
ancianatosanmiguel@sanmiguel.gov.co www.sanmiguel.gov.co
Vigilado “Superintendencia Nacional de salud”