PLAN DE TRATAMIENTO DE LA SEGURIDAD EN LA INFORMACIONY TRATAMIENTO DE RIESGOS DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

VIGENCIA 2022

ENERO 29 DE 2022

ESE HOSPITAL SAN FRANCISCO DE ASIS PALERMO-HUILA

PLAN DE TRATAMIENTO DE RISGOS DE SEGURIDAD

Y PRIVACIDAD DE LA INFORMACION

VIGENCIA 2022

DRA. SARA ALEXANDRA YAGUAR JIMENEZ

ENERO 29 DE 2022

TABLA DE CONTENIDO

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

PRESENTACION GENERAL DE LA E.S.E

La E.S.E Hospital San Francisco de Asís del Municipio de Palermo Huila, es una institución prestadora de servicios de salud de baja complejidad que tiene como misión principal y por su naturaleza brindar servicios a los usuarios, contando para ello con personal idóneo y comprometido en cada uno de los procesos que se desarrollan, cumpliendo los objetivos institucionales que la E.S.E ha diseñado, a través de sus planes, políticas y estrategias, enmarcadas dentro de su Misión y Visión institucional.

La E.S.E Hospital San Francisco de Asís de Palermo-Huila, requiere avanzar dentro de la estrategia de Gobierno en línea, a través de las directrices exigidas por el Ministerio TIC, al cumplir con la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, a fin de contribuir dentro de la construcción de un Estado más eficiente, más transparente y participativo. La adopción de un plan de Seguridad y Privacidad de la Información para dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno en línea, permitirá un mejor aprovechamiento de las TIC, a lo cual se trabajará en el fortalecimiento de la seguridad de la información dentro de la institución, pues se hace más que necesario garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, acorde con lo expresado en la legislación Colombiana

DIRECIONAMIENTO ESTRAT|EGICO

MISIÒN

Somos una Empresa Social del Estado de atención primaria, que brinda servicios integrales en salud a la población.

VISION.

La ESE Hospital San Francisco de Asís de Palermo, en el año **2024** será una empresa con atención humanizada y con sostenibilidad social y financiera.

PRINCIPOS CORPORATIVOS:

- **HUMANIZACIÒN:** Atención integral y calidez humana para nuestros pacientes y personal.
- **SEGURIDAD**: Ambientes seguros y confortables que proporcionan mayor confiabilidad.
- **LIDERAZGO**: Nuestro compromiso fortalece la capacidad de liderazgo en elsector salud.
- **SOLIDARIDAD**: Servicio con enfoque humanizado que aumenta la solidaridad empresarial.
- **INTEGRIDAD**: Respetamos y fortalecemos el cuidado de la integridad de nuestros pacientes**.**
- **EQUIDAD:** La igualdad y el respeto por los derechos humanos son nuestro pilar empresarial.

NUESTRA POLITICAS INSTITUCIONALES

- **POLITICA DE CALIDAD.**
- **POLITICA SEGURIDAD DEL PACIENTE.**
- **POLITICA IAMII.**
- **POLITICA DE BIOSEGURIDAD.**

VALORES.

- **Respeto** a la dignidad humana: Se reconoce y tolera la diversidad de creencias, sentimientos y afinidades de cada uno de nuestros funcionarios y usuarios.
- **Integralidad:** Garantizar la atención del paciente en la promoción de la salud, detección temprana de la enfermedad y protección específica, tratamiento y rehabilitación de los usuarios de la institución.
- **Solidaridad** Adhesión o apoyo incondicional a causas o intereses ajenos, especialmente en situaciones comprometidas o difíciles.
- **Calidad** Conjunto de propiedades inherentes a una cosa que permite caracterizarla y valorarla con respecto a las restantes de su especie.
- **Equidad** Cualidad que consiste en no favorecer en el trato a una persona perjudicando a otra.

POLITICA DE CALIDAD:

Hacer parte de un hospital que hace amable la vida, nos compromete a enfocarnos por mejorar de manera permanente nuestros procesos de calidad, conforme a lanormatividad vigente , con talento humano calificado, atención humanizada, buscando siempre la satisfacción de los usuarios, su grupo familiar,funcionarios y demas participes del sistema de salud , sin descuidar la interacciónresponsable con el medio ambiente como legado a las futuras generaciones.

De esta manera garantizamos la atención integral al usuario, lo que nos permite satisfacer sus necesidades y expectativas; a través del cumplimiento de procesos, evaluación de indicadores, acciones de mejoramiento continuo, dirigidos a la promoción de la salid y prevención de la enfermedad.

OBJETIVOS

OBJETIVO GENERALES

Crear y gestionar un plan que permita controlar y minimizar los riesgos de seguridad y privacidad de la información, relacionados a los procesos TIC existentes, en la ESE San Francisco de Asís del Municipio de Palermo Huila.

OBJETIVOS ESPECIFICOS

- Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.
- Aplicar las metodologías del DAFP e ISO respectivamente en seguridad y riesgo de la información, para la ESE San Francisco de Asís del Municipio de Palermo Huila.
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo.
- Definir los principales activos a proteger en la ESE.
- Evaluar y comparar el nivel de riesgo actual con el impacto generado después de implementar el plan de gestión de seguridad de la información

RESPONSABLES

GERENCIA

JEFES DE AREA

LIDERES DE PROCESOS Y PROCEDIMIENTOS.

LIDER DE LAS Tics

ADMINISTRADORES DE INFORMACION

CONCEPTOS BASICOS

Administradores de la Información

Todos aquellos servidores públicos, sin interesar su vinculación laboral que administren, accedan, manejen y/o entreguen información de la ESE San Francisco de Asís de Palermo Huila.

Acceso a la Información Pública

Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información

En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.

Archivo

Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Amenazas

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría

Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Autorización

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales

Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

Ciberseguridad

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio.

Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura (Ley 594 de 2000, artic 13).

Datos Personales Sensibles

Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

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).

Información Pública Clasificada.

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Información Pública Reservada

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Plan de continuidad del negocio

Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC

27000).

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).

Privacidad
En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Responsabilidad Demostrada
Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos
Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

Riesgo
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).

Seguridad de la información
Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI
Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Titulares de la información
Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

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).

ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

El éxito de la administración del riesgo depende de diversos factores, aun así, la participación de la alta dirección en este caso Gerente, Asesores, Jefes de Áreas, Lideres de Procesos, Administradores de Información, permite que el proceso se desarrolle con mayor fluidez y efectividad, es por ello que en la identificación de los roles no solo se observa el equipo técnico que hará las labores de análisis y tratamiento del riesgo, sino que se involucran todos los servidores públicos de la entidad.

RESPONSABLES

- LIDERES DE PROCESOS Y PROCEDIMIENTOS.
- LIDER DE LAS Tics
- ADMINISTRADORES DE LA INFORMACION

s

Metodología de evaluación del riesgo

Es el primer paso en su viaje hacia la gestión de riesgos. Necesita definir las reglas para llevar a cabo la gestión de riesgo, ya que querrá que toda la empresa lo haga de la misma forma, el principal problema del plan de tratamiento de riesgos de seguridad de la información es que la organización lo ejecute de diferente forma en distintas partes de la organización.

Usted necesita definir si quiere una evaluación cualitativa o cuantitativa del riesgo, cuáles son las escalas que se utiliza durante la evaluación cualitativa, conocer cuál será el nivel aceptable de riesgo, etc.

Implantación de la evaluación del riesgo

Una vez que se conocen las reglas, se puede comenzar localizando los problemas potenciales que pueden ocurrir. Es necesario realizar un listado de todos los recursos, de las amenazas y vulnerabilidades que se relacionan con los recursos, evaluar el impacto y la probabilidad de ocurrencia para finalmente calcular el nivel de riesgo.

Implementar el tratamiento del riesgo

No todos los riesgos tienen el mismo origen, se debe enfocar en los más importantes, los llamados riesgos no aceptables. Existen cuatro opciones que puedeescoger para mitigar el riesgo no aceptable.

Aplicar controles de seguridad para disminuir el riesgo.

- Transferir el riesgo a otras personas, es decir, comprando un seguro con una compañía aseguradora.

- Evitar riegos al detener la ejecución de la actividad que genera un elevado riesgo, o al hacerla de forma diferente.
- Aceptar el riesgo, por ejemplo, si el costo de atenuación es mayor que el daño en sí mismo.

Identificación de controles

Es crucial para la implementación adecuada de un SGSI la aplicación de controles existentes según la norma ISO 27001. Estos salen como resultado del análisis de riesgo efectuado en la etapa inicial (plain), en la mayoría de los casos para la aplicación de los controles es necesario personal experto en diversas áreas pues si bien es cierto que la implantación de un sistema de seguridad de la información está ligada al personal encargado de TI según la norma se trabaja sobre los dominios existentes los cuales incluyen desde recursos humanos hasta la legislación.

Para cada uno de los dominios existen controles que deberán ser aplicados para la mitigación del riesgo depende de la clasificación inicial.

- **Estructuralmente la ESE Hospital San Francisco de Asís de Palermo Huila, manejara los riesgos identificados de la siguiente manera:**

Controles de clase técnica
Estos controles se basan prácticamente en la gestión operativa y de aseguramiento, de zonas físicas, accesos, manipulación de hardware y software, accesos a sitios web, manejo de la información, etc.

Controles de clase documental

En esta fase los controles son dirigidos a reglamentar, aplicar, sensibilizar a todo el personal que labora en las organizaciones además son los controles más complicados pues con base en ello es que se les informa y distribuye el respectivo funcionamiento a los demás trabajadores.

Usualmente estas políticas, instructivos, reglamentos no son muy tenidos en cuenta por los trabajadores dejando de forma incompleta la implantación del sistema de gestión de seguridad. Es aquí donde los planes de capacitación y sensibilización deben ser planificados de la mejor manera para tener la mayor aceptación en cada uno de los trabajadores de la compañía para dar el máximo cumplimiento y sacar el máximo de efectividad con la aplicación de controles técnicos.

Implementar programas de capacitación y sensibilización

Es ideal que se programen las fechas desde el inicio y las respectivas capacitaciones y sensibilizaciones, pues de esto depende en gran parte el éxito de la implementación del sistema. Al aplicar algunos controles se deberá realizar el debido seguimiento para verificar y cuantificar la funcionalidad del mismo, sin embargo, esto no aplica para todos los controles; Es ahí donde la sensibilización entra a jugar un papel fundamental en la compañía pues por desconocimiento los trabajadores pueden interferir o estropear el funcionamiento real del control, pues si bien es cierto que el sistema puede ser estable los usuarios son parte fundamental del éxito de cada uno.

Implementación de procedimiento de manejo de incidentes de seguridad

Cuando se habla de incidente informático, se hace referencia a un suceso que se presentó o que tiene una gran posibilidad de darse en un momento determinado.

Este suceso puede ser llevado a cabo a voluntad o accidental. Dependiendo de la gravedad de la situación este puede afectar el funcionamiento normal de la organización. Por lo general el manejo del incidente implica que este se debe solucionar en el menor tiempo posible para evitar una afectación mayor y se debe buscar documentar cada uno de los eventos presentados y el tiempo que transcurrió entre cada uno de ellos, con el fin de poderlo analizar posteriormente y aplicar correcciones del caso para que en un futuro este no se vuelva a presentar o al menos su impacto sea lo menor posible. Para ello, se pueden seguir los seis pasos ideales para mantener el orden adecuado.

Erradicación y Recuperación

Con base en la información tomada en la detección y contención es necesario tomar las medidas del caso para que no se vuelvan a presentar. Es posible que la ESE Hospital San Francisco de Asís de Palermo, tenga que invertir en elementos de protección adicionales. Pero esta decisión debe ser fundamentada en hechos y datos, ser lo más objetivos posibles. En el proceso de recuperación puede ser necesario restaurar las copias de respaldo, cambio de contraseñas, cambios de direcciones IP.

Reporte y cierre

Se hace necesario llevar a cabo un informe en el cual se documente los procesos realizados, siendo muy claros en los pasos llevados a cabo. Esta información puede servir más adelante para resolver nuevos impases o determinar si las decisiones tomadas fueron acordes al incidente.

Se debe generar un documento de lecciones aprendidas el cual debe estar redactado por el equipo que afronto el incidente, estas lecciones aprendidas se analizaran posteriormente por la alta dirección la cual se informara y hará los aportes para prevenir futuras situaciones. Por último, dar a conocer las recomendaciones del caso y llevar a cabo las implementaciones a que haya lugar. Es bueno, volver a hacer una revisión periódica tanto a las decisiones tomadas como las inversiones hechas por la ESE. Con ello evitamos que una solución planteada hoy mañana sea obsoleta y se nos presente un incidente nuevamente.

TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Administración de riesgos es un método sistemático que permite establecer a las entidades sean públicas o privadas, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos en función de la tecnología, equipos, infraestructura etc., asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades

Para la ESE Hospital San Francisco de Asís de Palermo Huila, es de suma importancia que su información sea protegida, es por ello que emprenderá acciones tendientes a preservar, conservar y asegurar sus datos y documentos a fin de mantener protegida toda su información. Para lograrlo la ESE, con su grupo técnico identificará previamente los posibles riesgos y propondrá acciones correspondientes para su mitigación

Una vez que la ESE Hospital San Francisco de Asís de Palermo Huila, ha identificado los riesgos, sus causas y sus eventuales daños, se hace necesario adoptar medidas preventivas y correctivas a fin de minimizar los posibles efectos y los daños que finalmente se puedan ocasionar a la información

Para mitigar y lograr los menores daños posibles es necesario mejorar los controles existentes y asignar recursos humanos, presupuestales y tecnológicos que permitan asegurar la información

A continuación, se presenta un cuadro de riesgos identificados, sus causas y las acciones preventivas y correctivas que serán implementadas en la institución.

(ORIGINAL FIRMADO)
SARA ALEXANDRA YAGUAR JIMENEZ
Gerente

MATRIZ DE RIESGOS

RIESGO	EVALUACION RIESGO	CONTROLES	NUEVA EVALUACION	OPCIONES DE MANEJO	ACCIONES	RESPUESTA	INDICADOR
Daño en equipos tecnológicos e interrupción de servicios a cargo de la Oficina de sistemas por factores eléctricos	Zona de Riesgo Extrema	La Oficina sistemas cuenta con 1 UPS con capacidad de 10 KvA y las cuales brindan respaldo aproximadamente a un 50 % de la infraestructura tecnológica de la ESE.	Zona de Riesgo Alta	Reducir el riesgo, evitar, compartir o transferir	Informar a la GERENCIA el riesgo y sugerir la elaboración de un estudio técnico que permita establecer posibles soluciones para reducir la interrupción del servicio por fallas eléctricas.	Jefe de la Oficina sistemas	Informe entregado a la Gerencia a fin de sugerir estudio técnico para mitigar el riesgo.
Interrupción del servicio de Internet por fallos en la	Zona de Riesgo Extrema	El servicio de internet es monitoreado de forma diaria por	Zona de Riesgo Moderada	Asumir el riesgo, reducir el riesgo	Mantener y/o mejorar el canal de Internet dedicado al	Jefe de la	Número de canales de Internet

RIESGO	EVALU ACION RIESGO	CONTR OLES	NUEVA EVALU ACION	OPCION ES DE MANEJ O	ACCION ES	RESPU ESTA	INDICA DOR
Daño en equipos tecnológicos e interrupción de servicios a cargo de la Oficina de sistemas por factores eléctricos	Zona de Riesgo Extrem a	La Oficina sistemas cuenta con 1 UPS con capacidad de 10 KvA y las cuales brindan respaldo aproximadament e a un 50 % de la infraestructura tecnológica de la ESE.	Zona de Riesgo Alta	Reducir el riesgo, evitar, compartir o transferir	Informar a la GERENCIA el riesgo y sugerir la elaboración de un estudio técnico que permita establecer posibles soluciones para reducir la interrupción del servicio por fallas eléctricas.	Jefe de la Oficina sistemas	Informe entregado a la Gerencia a fin de sugerir estudio técnico para mitigar el riesgo.
Interrupción del servicio de Internet por fallos en la	Zona de Riesgo Extrem a	El servicio de internet es monitoreado de forma diaria por	Zona de Riesgo Moderad a	Asumir el riesgo, reducir el riesgo	Mantener y/o mejorar el canal de Intenet dedicado al	Jefe de la	Número de canales de Internet

provisión del servicio	parte del contratista quien provee el servicio de internet ala ESE.	servicio de la ese y un servicio de Backup	Oficina sistemas	contratados y de backup
Robo, alteración y/o perdida de Información de la Entidad por acceso indebido a sistemas de información	LA Oficina Sistemas establece dentro del manual la periodicidad en la realización de copias de seguridad}.	Realizar diagnóstico de Sistema de seguridad de la información, incluyendo el mejoramiento de los programas de protección de virus y ataques informáticos	Jefe de la Oficina sistemas	Numero de mejoramientos en el sistema de seguridad de la información al interior de la entidad
Robo, alteración y/o perdida de Información de la Entidad por robo informático	No se cuenta con ningún control o herramienta que permita mitigar este riesgo.	Realizar diagnóstico de Sistema de seguridad de la información, incluyendo el mejoramiento de los programas	Jefe de la Oficina sistemas	Numero de mejoramientos en el sistema de seguridad de la información al interior de la entidad