PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

EMPRESA SOCIAL DEL ESTADO

HOSPITAL SAN JUAN DE DIOS

ITUANGO

2024

INTRODUCCION

El Modelo de Seguridad y Privacidad de la Información, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos.

Mediante el aprovechamiento de las TIC y el modelo de seguridad y privacidad de la información, se trabaja en el fortalecimiento de la seguridad de la información, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad.

MARCO LEGAL

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).

1. 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).

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

2. Datos Personales Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012).

3. Datos Personales Públicos Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

1. OBJETIVO

Generar un documento de lineamientos de buenas prácticas en Seguridad y Privacidad para las entidades del Estado.

1.1 OBJETIVOS ESPECIFICOS

Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.

Revisar los roles relacionados con la privacidad y seguridad de la información al interior de la entidad para optimizar su articulación.

2. DIAGNOSTICO

Actualmente la ESE Hospital San Juan de Dios de Ituango cuenta con un protocolo de seguridad de información en la custodia de todos los datos tanto para los usuarios “clientes externos” como también nuestros empelados “clientes internos” de la misma forma la custodia y respaldo de todo el material de apoyo y de trabajo de cada una de las dependencias que cuenta la institución.

3. REPONSABLE

Líderes de Procesos, todos los usuarios o funcionarios de la institución

4. FORMULACION DEL PLAN

La ESE Hospital San Juan de Dios de Ituango en su modelo de gestión de calidad tiene incorporado en el proceso de apoyo sistemas de información y la comunicación mecanismos para la seguridad y la privacidad de la información contemplado como contingencia el cual aporta las herramientas necesarias que aportan al presente plan en todo lo relacionado con la seguridad y privacidad.

Herramientas de apoyo

Contamos con varias alternativas de control y autocontrol que aplican a la seguridad y la privacidad de la información entre ellos:

Respaldo externo de la institución de la información de la institución. Herramientas de respaldo automático para los equipos de cómputo.

Servidor de respaldo para la copia de seguridad de todas las aplicaciones y plataformas instaladas en la institución.

5. ACTIVIDADES

- Realizar actividades preventivas de respaldo
- Verificar automatización de los procesos de respaldo para los equipos de cómputo
- Verificar automatización de los procesos de respaldo para los aplicativos o plataformas de información que hacen parte de la institución.

6. SEGUIMIENTO E IMPLEMENTACION

Según lo mencionado anteriormente se describe a continuación las etapas que se desarrollaran y los tiempos esperados para alcanzar el presente plan:

Revisión y/o Modificación plan de Seguridad y privacidad. Revisión del Control de acceso.

7. CRONOGRAMA

ACTIVIDADES	2024
Verificar Protocolos de seguridad	Enero y febrero 2024
Iniciar Plan	Marzo 2024
Realizar seguimiento y mejora	Octubre 2024