HOSPITAL LA BUENA ESPERANZA

E.S.E.

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

2018-2020

1. INTRODUCCION

El presente plan se elabora con el fin de dar a conocer como se realizará la implementación y socialización del componente de Gobierno en línea en el Eje Temática de la **Estrategia en seguridad y privacidad de la información**, el cual busca guardar los datos de los ciudadanos como un tesoro, garantizando la seguridad de la información que custodia el HOSPITAL LA BUENA ESPERANZA DE YUMBO.

2. MARCO NORMATIVO

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

3. OBJETIVO

Desarrollar un plan de gestión para controlar los riesgos asociados a los procesos tecnológicos existentes, en el HOSPITAL LA BUENA ESPERANZA DE YUMBO con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

3.1 OBJETIVO ESPECIFICO

- Realizar el plan de trabajo específico validando los recursos con los que se cuentan actualmente en el HOSPITAL LA BUENA ESPERANZA DE YUMBO para tener un plan de tratamiento de riesgo de seguridad y privacidad de la información.

4. DIAGNOSTICO

Actualmente el HOSPITAL LA BUENA ESPERANZA DE YUMBO cuenta con un protocolo de seguridad de información en la custodia de todos los datos tanto para los pacientes "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.

5. RESPONSABLE

- Líderes de Procesos
- Todos los usuarios o funcionarios de la institución.

6. FORMULACION DEL PLAN

El HOSPITAL LA BUENA ESPERANZA DE YUMBO en su modelo de gestión de calidad tiene incorporado en el proceso de apoyo sistemas de información y la comunicación mecanismos para mitigar y prevenir los riesgos sobre la seguridad y la privacidad de la información descrito en sus procedimientos

HERRAMIENTAS DE APOYO

Contamos con varias alternativas para mitigar los riesgos de seguridad y privacidad de la información aplicado a cada usuario que interactúan con una herramienta tecnológica o para consultar algún tipo de información entre ellos:

- ✓ Usuarios con roles y perfiles según su grado de responsabilidad.
- ✓ Equipos de computo en un entorno de dominio.
- ✓ Aplicaciones en ambiente cliente servidor para garantizar el almacenamiento de los datos.
- ✓ Contamos con un servidor proxy para mitigar posibles accesos externos de personas mal intencionadas
- ✓ Contamos con un paquete administrativo ara el control de virus.
- ✓ Todos los equipos cuentan con una clave propia de seguridad por

7. ACTIVIDADES

Realizar la Identificación de los Riesgos con los líderes del Proceso.

- Entrevistar con los líderes del Proceso
- Plantear al plan de tratamiento de riego aprobado por los lideres

8. 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 de la actual Política de Seguridad.
- Seguridad Ligada a los recursos humanos
- Revisión del Control de acceso
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio.

9. CRONOGRAMA

Actividades	2018	2019	2020
Identificar riesgos	31/10/2018		
Definir y ejecutar plan tratamiento	01/11/2018		
Realizar seguimiento y mejora	Permanente	15/06/2019	15/06/2020

CLAUDIA JIMENA SÁNCHEZ ALCALDE

Gerente