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

En cumplimiento al Decreto 612 de 2018

1. Presentación

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información tiene como objetivo establecer los lineamientos necesarios para implementar y socializar las estrategias de seguridad en el marco del Gobierno en Línea, específicamente en la temática de seguridad y privacidad de la información. Este plan busca proteger la información sensible de los ciudadanos, garantizando su seguridad, privacidad y cumplimiento normativo, y salvaguardando los datos que el HOSPITAL LA BUENA ESPERANZA DE YUMBO custodia.

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**).

“Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944.” (Derechos de autor, **Ley 44 de 1993**).

“Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”. (**Ley 527 de 1999).**

“Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”. (**Ley 1273 de 2009).**

"Régimen común sobre derecho de autor y derechos conexos". CONPES 3854 de 2016 – Política de Seguridad Digital del Estado Colombiano. (**Decisión Andina 351 de 2015).**

Modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC. (**Decreto 1078 de 2015)**

Modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión MIPG. (**Decreto 1499 de 2017).**

3. Glosario de términos

Análisis: Fase del ciclo de vida de desarrollo software que consiste en la identificación de los elementos, estructura, funcionalidades, relaciones, etc. de los elementos que se quieren desarrollar.

Auditoría: Proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

Dato: Representación simbólica (numérica, alfabética, algorítmica etc.), un atributo o una característica de una entidad. Los datos son hechos que describen sucesos y entidades.

Entidad: Representa una "cosa" u "objeto" del mundo real con existencia independiente, es decir, se diferencia unívocamente de cualquier otro objeto o cosa, incluso siendo del mismo tipo, o una misma entidad.

Especificaciones: Conjunto de requisitos que deben ser cumplidos por un sistema software, tanto desde el punto de vista funcional como técnico.

Información: Conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Relación: Describe cierta dependencia entre entidades o permite la asociación de las mismas.

Trazabilidad: Conjunto de procedimientos preestablecidos y autosuficientes que permiten conocer el histórico y el estado de un sistema en un momento dado.

Planificación estratégica: Es una herramienta de gestión que permite establecer el que hacer y el camino que deben recorrer las organizaciones para alcanzar las metas previstas.

Marco de Referencia de AE: Marco de Referencia de Arquitectura Empresarial para la Gestión de TI del Estado.

AE: Arquitectura Empresarial definición relacionada con el desarrollo del proceso de TI y dominios de datos, aplicaciones, infraestructura, seguridad y procesos en una organización.

Confidencialidad: Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

4. Objetivos

➢ Objetivo General

Controlar, mitigar y minimizar los riesgos relacionados con la seguridad y privacidad de la información en HOSPITAL LA BUENA ESPERANZA DE YUMBO, con el fin de proteger los activos de información, gestionar el acceso adecuado a los sistemas y asegurar la confidencialidad de los datos tanto de pacientes (clientes externos) como de empleados (clientes internos).

➢ Objetivos específicos

- Elaborar un plan de trabajo específico para tratar los riesgos de seguridad y privacidad, validando los recursos y herramientas actuales del hospital.
- Establecer e implementar el Direccionamiento Estratégico de Tecnología de la Información, garantizando que las soluciones tecnológicas respondan a las necesidades presentes y futuras de la institución.
- Adquirir e implementar tecnologías avanzadas que apoyen la gestión de los procesos asistenciales, administrativos y misionales, asegurando la evolución tecnológica acorde con las mejores prácticas de seguridad y privacidad.

5. Diagnóstico

Actualmente, el HOSPITAL LA BUENA ESPERANZA DE YUMBO cuenta con un protocolo de seguridad que regula la custodia de los datos personales de los pacientes y empleados. Este protocolo está diseñado para proteger tanto la información sensible como los materiales de apoyo de la institución.

Sin embargo, existen algunas brechas tecnológicas que deben ser abordadas:

Renovación de equipos de cómputo y servidores: No se cuenta con una política de renovación tecnológica adecuada, lo que podría generar desactualización frente a los avances en infraestructura tecnológica y afectar la capacidad operativa del hospital.

Capacidad de la red de datos: La infraestructura de red no ha crecido de manera proporcional al aumento de los procesos digitalizados y las cargas operativas generadas por la digitalización de la información.

6. Lineamientos conceptuales

Este plan abarca todos los procesos organizacionales del hospital, asegurando que la seguridad y privacidad de la información se gestionen de manera integral. Los riesgos son tratados desde un enfoque basado en los pilares de la gestión de calidad y el modelo de arquitectura empresarial. La implementación se realizará en un contexto de mejora continua, buscando la adaptabilidad y sostenibilidad de las soluciones tecnológicas adoptadas.

Los lineamientos principales son los siguientes:

Evaluación continua de riesgos: Identificación y evaluación periódica de riesgos asociados a la seguridad de la información, considerando las amenazas emergentes y los cambios en la normativa.

Definición de roles y responsabilidades: Establecimiento claro de las funciones de cada miembro del personal en cuanto a la protección de la información, incluyendo la gestión de accesos y permisos.

Implementación de medidas de control: Desarrollo de medidas de control preventivas y correctivas para mitigar los riesgos, tales como el cifrado de datos, la autenticación multifactor y los sistemas de detección de intrusos.

Auditorías y revisiones periódicas: Realización de auditorías internas y externas para evaluar el cumplimiento de los procedimientos de seguridad y privacidad, asegurando la eficacia del plan.

Capacitación continua: Entrenamiento regular a todo el personal sobre las políticas de seguridad, mejores prácticas en manejo de datos personales y gestión de accesos.

Como se representa gráficamente nuestros componentes están relacionados de manera transversal a nivel institucional donde cada uno de ellos juega un papel importante desde el tratamiento de la información, su custodia y privacidad y como también los resultados de los mismos, teniendo siempre presente la estructura organizacional y cumpliendo con todas las etapas del modelo de gestión de calidad institucional.

7. Formulación 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 descrita en sus procedimientos

8. Diseño de herramientas de recolección de información

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

- Usuarios con roles y perfiles según su grado de responsabilidad.
- Los usuarios tienen acceso restringido a cada equipo para no poder realizar alteraciones y/o adiciones de software.
- Cada equipo de cómputo cuenta con dos cuentas protegidas por usuario y contraseña (una administradora controlada por el área de sistemas, otra de usuario que va de acuerdo a cada dependencia donde se encuentre ubicado el equipo).
- Equipos de cómputo 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.

9. Metodología

Uno de los principales problemas para el presente plan es la seguridad y la privacidad de la información dado el entorno como entidad pública donde cada vez es más importante el cuidado y la privacidad de la información.

- **Análisis de las posibles causas que han provocado problemas en el tiempo.**

  Una de las principales causas del presente plan es el alto riesgo en cuanto al tratamiento de la información desde su procesamiento hasta su etapa final.

- **Propuesta y planificación del plan.**

  Identificar con cada uno de los lideres todos los posibles riesgos en cuanto a la recopilación consolidación y etapa final de la información el cual a su vez obedece a todo el ciclo PHVA con el que cuenta la institución.

- **Implementación y seguimiento.**

  Definir en cada una de las plataformas los respectivos roles y perfiles para cada profesional con el fin de llevar control de la información y de esta manera minimizar todos los posibles riesgos en cuanto al tratamiento de riesgos de seguridad y privacidad de la información.

- **Evaluación**

  Se realizará informe trimestral sobre el plan indicando las ventajas y desventajas como también de los resultados obtenidos y de los posibles riesgos materializados. Adicional a eso existe un proceso de estancamiento en el crecimiento de la tecnología informática y los sistemas de información Redes y Centro de Cómputo y servidor de contingencia en la nube o propio

10. Desarrollo del Plan:

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

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

11. Indicadores

Informe trimestral sobre el plan indicando las ventajas y desventajas como también de los resultados obtenidos y de los posibles riesgos materializados

12. Cronograma de cumplimiento

Actividades	2018	2019	2020	2021	2022	2023
Identificar riesgos	31/10/18					
Definir y ejecutar plan tratamiento	01/11/18					
Realizar seguimiento y mejora		23/04/19	15/06/20	15/09/21	28/10/22	10-01-2023

Actividades	2024	2025				
Identificar riesgos						
Definir y ejecutar plan tratamiento						
Realizar seguimiento y mejora	19-01-2024	22-01-2025				