PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ESTRUCTURA DE PLAN

En cumplimiento al Decreto 612 de 2018

1. Presentación

El Plan 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.

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

Atributos: Características que definen o identifican a una entidad, estas pueden ser muchas, y solo el diseñador utiliza o implementa las que considere más relevantes. Los atributos son las propiedades que describen a cada entidad en un conjunto de entidades.

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

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

Monitorización: Proceso por medio del cual, nos aseguramos que nuestro proceder está encaminado adecuada y eficazmente hacia un resultado final, evitando las posibles desviaciones que pudieran presentarse. La monitorización puede detectar las posibles interferencias que pudieran presentarse en el curso de alguna acción y puede dar lugar a corregir el procedimiento antes de llegar a un resultado final.

Perfil: Descripción detallada de las posibles transacciones que puede realizar un usuario en el sistema.

Privilegio: Permiso sobre una determinada funcionalidad que se le da a los usuarios.

Rol: Nombre que se le confiere al conjunto de perfiles que le son asignados al usuario para el ejercicio de sus funciones.

4. Objetivos

➢ Objetivo General

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

➢ Objetivos específicos

- 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.
- Incluir un Direccionamiento Estratégico de Tecnología de la información que justifiquen las necesidades actuales y futuras de la institución.
- Adquirir nuevas tecnologías que apoyen a los procesos funcionales y misionales de la institución.

5. Diagnóstico

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 empleados “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.

El hospital no cuenta con una política de renovación de equipos de cómputo y servidores que permita estar alineado con los avances tecnológicos en el término de 2 años, el aumento de la red de datos no ha tenido un crecimiento acorde a la implementación realizada

6. Lineamientos conceptuales

El presente plan fue propuesto dado que afecta de manera transversal toda la organización y de la misma manera aplica como riesgo de tipo alto dado la connotación del caso y más aún cuando se habla de seguridad y privacidad como principal componente para este plan se tiene presente el riesgo de la seguridad y privacidad de la información y de cómo custodiarla y como protegerla.

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 mismo 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 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.

8. Herramientas De Apoyo

Contamos con varias alternativas de control y autocontrol que aplican a la seguridad y la privacidad de la información.

9. Diseño de herramientas de recolección de información

Herramientas de respaldo automático para los equipos de cómputo.

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

10. Metodología (Métodos y técnicas para el desarrollo del Plan)

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 de pérdida de información, el ataque de posibles virus, daño de discos duros al finalizar su vida útil.

- **Propuesta y planificación del plan.**

  Contar con los respectivos protocolos de copias seguridad para todas las plataformas instaladas, como también protocolo de copias seguridad para la información relevante de cada estación de trabajo de igual forma que todos los equipos se encuentren protegidos con sus respectivos antivirus y el cumplimiento de los planes de mantenimiento preventivo a todas las máquinas de la institución. Lo anterior con el fin de mitigar los riesgos y no incursionar en reprocesos.

  Diseñar e implementar una estructura funcional que dimensione e integre el macro proceso gestión de la información (sistemas, estadística, comunicaciones y gestión documental, etc.) muchas funciones son Adhoc

- **Implementación y seguimiento.**

  Automatizar respaldo para las plataformas instaladas en la institución como también los respaldos para la información de las estaciones de trabajo más relevantes de la institución como son las estaciones de los líderes y funcionarios que consoliden y custodien información relevante para la institución, por otra parte realizar un respaldo semanal de la información a un repositorio externo; los seguimientos de la misma manera se encuentran automatizados por medio de correos electrónicos posterior a

cada proceso de las copias de seguridad y los respectivos soportes posterior a la custodia realizada externamente.

- **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.

11. Desarrollo del Plan:

Verificación automatización de los procesos de respaldo para los equipos de computo

Verificación automatización de los procesos de respaldo para los aplicativos o plataformas de información que hacen parte de la institución.

Soportes de extracción de las copias de seguridad semanales en sede o repositorio por fuera de la institución.

12. Indicadores

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

13. Cronograma de cumplimiento

Como el presente plan hace parte de un procedimiento institucional todo se encuentra descrito en el proceso de apoyo de gestión de la información no obstante se describe de manera general el cronograma

Actividad	Periodicidad
Backup (Respaldo) base de datos de manera incremental	Dos veces al día una al medio día y otro a la media noche siguiente a servidor NAS
Backup (Respaldo) estaciones de trabajo según nivel de información	Todos los martes son realizados automáticamente a servidor NAS