PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

INTRODUCCIÓN

Para la Unidad de Salud de Ibagué la información es un activo que cobra importancia en la optimización de sus procesos que se refleja en la satisfacción de los pacientes, por ende se hace necesario definir el proceso necesario para colocar en marcha la implementación del Modelo de Seguridad de La Información expedido por el Ministerio de Tecnología y Comunicaciones del Estado Colombiano.

La estrategia de Gobierno en Línea - GEL, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente

En el Plan Nacional de Desarrollo 2018-2022 se reconoce la seguridad y privacidad de la información, como un factor fundamental para la apropiación de las TIC; así mismo plantea un marco de seguridad necesario, que permita garantizar la prestación de servicios a los ciudadanos a través de las TIC, y que debe estar respaldado por unos planes, políticas y procedimientos orientados a preservar y minimizar el impacto a los activos de información de la entidad por eventos como fallas de seguridad, perdida del servicio y disponibilidad del servicio.

El Plan de Seguridad y Privacidad de la Información y Continuidad de TI para estar acorde con las buenas prácticas de seguridad y continuidad deberá ser actualizado periódicamente; así mismo recoger los cambios técnicos de la norma, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

La seguridad de la información garantiza que los responsables de la información sean capaces de gestionar la información de forma segura, independientemente del formato o soporte en el que se encuentra. Mediante el proceso de Gestión de TI y el modelo de seguridad y privacidad de la información y de continuidad de TI, se

trabajará en el fortalecimiento de la seguridad de la información en la Unidad de Salud de Ibague, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación colombiana.

OBJETIVOS

GENERAL

Definir en el Plan de Seguridad y Privacidad de la Información, los lineamientos que respondan asertiva y oportunamente a eventos que afecten la seguridad de la información.

ESPECIFICOS:

- Definir las fases para diseñar, implementar y evaluar la Estrategia de Seguridad y privacidad de la Información.
- Contribuir a la disminución de incidentes y requerimientos relacionados con la seguridad de la información.
- Facilitar la implementación de los lineamientos del Marco de Referencia de Seguridad de la Información de Gobierno en Línea, relacionados con la seguridad de la información.

ALCANCE

Este documento contempla la estructura de gobierno y los lineamientos principales para la seguridad y privacidad de la información en la Unidad de Salud de Ibagué Los lineamientos definidos en este documento deben ser conocidos y cumplidos por empleados, contratistas y todos los terceros que tengan acceso, almacenen, procesen o trasmitan información de la institución o sus pacientes.

La estructura del Plan se basa en la metodología propuesta por MINTIC para el componente de Seguridad y Privacidad de la Información. El presente plan, aplican a todos los procesos soportados por el proceso de Apoyo Tecnológico de la Unidad de Salud de Ibagué.

ESTRUCTURA DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Unidad de Salud de Ibague ha estructurado el Plan de Seguridad y Privacidad de la Información en concordancia con los marcos legal y conceptuales del Estado relacionadas con la Seguridad y privacidad de la Información y garantizará la Confidencialidad, Integridad y Disponibilidad de la Información presentados anteriormente, que permita cumplir con el objetivo definido en dicho plan, para esto se definen las actividades que se describen a continuación:

FASE DE DIAGNOSTICO

En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información. Para esta fase tenemos como metas:

Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.

Determinar el nivel de madurez de los controles de seguridad de la información.

Identificar el avance de la implementación del ciclo de operación al interior de la entidad.

Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.

Identificación del uso de buenas prácticas en ciberseguridad.

Realizar el diagnóstico de las condiciones en que se encuentran los activos de información administrados por la entidad.

Para ello, utilizaremos las siguientes herramientas publicadas en http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html :

Herramienta de diagnostico

Instructivo para el diligenciamiento de la herramienta

Guía No 1 - Metodología de Pruebas de Efectividad

FASE DE PLANIFICACION

En esta fase se pretenderá cumplir con las siguientes metas:

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Se proyectará la Política de Seguridad y Privacidad de la información que estará contenida en un documento de alto nivel que incluye la voluntad de la Alta Dirección de la Unidad de Salud de Ibagué para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información.

La política contendrá una declaración general por parte de la Alta Dirección, donde se especifique sus objetivos, alcance, nivel de cumplimiento. La política será sometida a aprobación y será divulgada al interior Unidad de Salud de Ibagué. Se tomará de base la Guía 2 - Política General MSPI del Modelo de Seguridad y privacidad de la Información de MinTic.

La actualización de la política debe realizarse al menos una vez al año o cuando se evidencie que nuevas amenazas pueden afectar la Seguridad de la Información en HUFT, todos los cambios que surtan en la política debe ser aprobado y divulgado al interior de la entidad.

POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Se desarrollará un manual de políticas, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior Unidad de Salud de Ibagué; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información

En el manual de políticas de la entidad, se debe explicar de manera general, las políticas, los principios de seguridad y la normatividad pertinente. De la Unidad de Salud de Ibagué deberá evaluar los requerimientos necesarios para ser ajustados o desarrollados en la elaboración de las políticas de seguridad y privacidad, así como en la implementación.

POLITICA DE SEGURIDAD DE LA INFORMACION

1. Responsabilidad del Personal. Todas las personas internas o externas que laboran para la Unidad de Salud de Ibagué, son responsables de sus actos, del cumplimiento de las políticas, normas, procedimientos y estándares vigentes, sobre la seguridad de la plataforma tecnológica.

2. Responsabilidad de manejo de la Información. Es responsabilidad de todos los empleados de la **UNIDAD DE SALUD DE IBAGUE**, el velar por la veracidad de los datos y que la información sea generada, manipulada, modificada, almacenada, conservada, transportada, accedida, divulgada y destruida de acuerdo con las normas que se establezcan. Los contratistas que tengan acceso a la información del **UNIDAD DE SALUD DE IBAGUE** tendrán igual responsabilidad.

3. Responsabilidad sobre la identificación de usuarios. Todos los usuarios deben tener una identificación única e intransferible para hacer uso de la información y de los recursos tecnológicos en cada una de las plataformas. La identificación puede ser requerida si la norma lo especifica. La persona dueña de la Identificación es responsable de esta y del uso que se haga de la misma. Los datos concernientes a los usuarios que han intentado o realizado accesos sobre los recursos o la información pueden ser registrados, consultados, mantenidos y divulgados si la entidad lo ve necesario y/o si la norma lo especifica.

4. Propiedad de la Información. Toda la información generada, adquirida o administrada por las personas que laboran en la UNIDAD **DE SALUD DE IBAGUE** es propiedad de la Entidad y como tal no debe ser empleada para usos que no le generen beneficios a a la misma. De igual forma, toda la información generada, adquirida o administrada por terceros en virtud de la ejecución de procesos de la institucion y de la prestación de servicios, también se considera propiedad del **UNIDAD DE SALUD DE IBAGUE**

5. Privacidad de la información. La información de la **UNIDAD DE SALUD DE IBAGUE** podrá ser clasificada según el grado de privacidad y confidencialidad requerido. Los usuarios de la información podrán tener restricciones para el acceso a la información, según las clasificaciones establecidas y según la norma lo especifique. Las normas y procedimientos que se determinen podrán restringir el acceso a la información para los diversos tipos de usuarios, pero en virtud de la obligatoriedad establecida por normas superiores sobre el suministro de información a instancias legales, no podrán permitir el ocultamiento definitivo de información.

6. Gestión de la plataforma tecnológica. La plataforma tecnológica debe ser diseñada, adquirida, modificada, operada, controlada y respaldada siguiendo practicas que garanticen las siguientes características de seguridad: confidencialidad, control de acceso (autenticidad), integridad, disponibilidad y la no repudiación de la información y las operaciones que se realicen sobre la plataforma. Los mecanismos que se empleen para proveer dichas características podrán estar en uno solo de los componentes de la plataforma o en varios de ellos, según el nivel de seguridad que se requiera. Ante eventos que atenten contra las características de seguridad podrá restringirse o detenerse completamente la operación. La plataforma tecnológica esta compuesta por: los equipos y

enlaces de red de telecomunicaciones, los equipos de computación o procesamiento de datos o de información, las aplicaciones y programas de software, los repositorios de datos y los datos.

7. Legalización de la plataforma tecnológica. Todos los componentes de la plataforma tecnológica que la **UNIDAD DE SALUD DE IBAGUE** utilice, deben estar debidamente legalizados de acuerdo con las normas colombianas establecidas para ello.

8. Proveedores. Todo proveedor que tenga una relación contractual con la **UNIDAD DE SALUD DE IBAGUE** debe cumplir las políticas, normas y procedimientos definidos por la institución, Los contratos que se firmen con terceros, deben contener una cláusula, que los obligue a cumplirlas junto con un acuerdo de confidencialidad establecido por la Entidad

9. Cumplimiento de las políticas. Es responsabilidad de la oficina de Sistemas, velar por el cumplimiento de las políticas y normas de seguridad Informática. Esta dependencia debe apoyar esta función y servirá para dirimir los posibles conflictos que se presenten en la aplicación de las políticas, normas y procedimientos.

10. Confidencialidad. Toda la información que se genere y que tenga relación con seguridad informática debe ser custodiada y mantenida con todas las normas de seguridad física y de la información y solo puede ser manipulada por las personas designadas por la **UNIDAD DE SALUD DE IBAGUE**

11. Acceso a áreas criticas: El acceso de personal a áreas críticas se llevará acabo de acuerdo a las normas y procedimientos que se establezcan en concordancia con las políticas de la entidad. Se debe proveer de la infraestructura de seguridad requerida con base en los requerimientos específicos de cada área.

12. Seguridad de Equipamiento: Todo el equipo de cómputo (computadoras, estaciones de trabajo, equipo accesorio y de telecomunicaciones), que esté o sea conectado a la Red, o aquel que en forma autónoma se tenga y que sea propiedad de la entidad debe sujetarse a las normas y procedimientos de instalación, actualización, mantenimiento preventivo y correctivo, acceso, reubicación, reasignación, y todo aquello que implique movimientos en su ubicación, de adjudicación, sistema y misión. Se debe tener un registro de todos los equipos que sean propiedad de la entidad. Todos y cada uno de los equipos deben ser asignados a un responsable. El equipo de la institución que sea de propósito específico y tenga una misión crítica asignada, requiere estar ubicado en un área que

cumpla con los requerimientos de: seguridad física, las condiciones ambientales y de alimentación eléctrica establecidos en las normas.

13. Ambiente de trabajo: El ambiente de trabajo debe reunir condiciones que permitan y faciliten el buen desempeño de los usuarios, además de brindar medidas de protección en sus labores diarias.

14. El no cumplimiento de las políticas, normas y procedimientos establecidos por la Política de Seguridad Informática ameritara una sanción de acuerdo al reglamento interno de la **UNIDAD DE SALUD DE IBAGUE**

PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN.

Se desarrollarán y formalizarán los procedimientos que permitan gestionar la seguridad y privacidad de la información en cada uno de los procesos definidos en la Unidad de Salud de Ibague.

ROLES Y RESPONSABILIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La entidad debe definir mediante un acto administrativo (Resolución) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos de la Entidad.

INVENTARIO DE ACTIVOS DE INFORMACIÓN.

Realizar el Inventario de los activos de información por parte de cada proceso, siendo el proceso de Apoyo Tecnológico quien recopila la información generando un solo documento con todos los activos de la entidad, con el fin de definir la criticidad, sus propietarios, custodios y usuarios.