

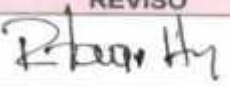
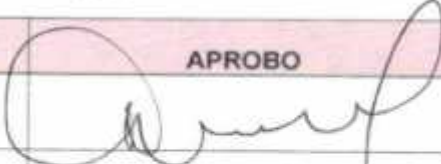



|  |  |                      |
|--|--|----------------------|
|  | <b>PROCESO GESTIÓN TECNOLÓGICA E INFORMÁTICA.</b>                                  | <b>GTI-SIS-PI-02</b> |
|  | <i>Plan de tratamiento de riesgos de seguridad y privacidad de la información.</i> | <b>Ver. 03</b>       |

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



| ELABORO   | REVISO  | APROBO   |
|---|---|--|
| <br>ANDREA CAROLINA VALDERRAMA QUIJANO | <br>RICARDO TOVAR HERNADEZ | <br>LIBIA SOTO SÁNCHEZ |
| Ingeniera de sistemas   | MECI-CALIDAD  | Representante de alta Dirección ante SGC.  |




|   |   |                      |
|---|---|----------------------|
|  | <b>PROCESO GESTIÓN TECNOLÓGICA E<br/>INFORMÁTICA.</b>   | <b>GTI-SIS-PI-03</b> |
|   | <i><b>Plan de tratamiento de riesgos de seguridad<br/>y privacidad de la información.</b></i> | <b>Ver. 03</b>       |

### Tabla de contenido.

|   |    |
|---|----|
| 1. PRESENTACIÓN.....  | 4  |
| 2. TERMINOS .....   | 4  |
| 3. OBJETIVOS .....  | 8  |
| 4. RECURSOS.....  | 9  |
| 5. RESPONSABLES .....   | 9  |
| 6. METODOLOGÍA DE IMPLEMENTACIÓN.....   | 9  |
| 6. PLAN DE TRATAMIENTO DE SEGURIDAD Y PRIVACIDAD DE LA<br>INFORMACIÓN ACTIVIDADES ..... | 10 |
| 7. CUMPLIMIENTO DE IMPLEMENTACIÓN.....  | 11 |
| 8. CRONOGRAMA.....  | 11 |
| 9. SEGUIMIENTO Y EVALUACIÓN.....  | 12 |
| 10. DIAGNOSTICO E IDENTIFICACION DE RIESGOS .....                                       | 12 |



|   |   |                      |
|---|---|----------------------|
|  | <b>PROCESO GESTIÓN TECNOLÓGICA E<br/>INFORMÁTICA.</b>   | <b>GTI-SIS-PI-03</b> |
|   | <b><i>Plan de tratamiento de riesgos de seguridad<br/>y privacidad de la información.</i></b> | <b>Ver. 03</b>       |

## 1. PRESENTACIÓN

La institución en su quehacer diario utiliza TIC en cuanto a captura, procesamiento y reporte de información tanto internamente como externamente para comunicarse con los diferentes actores del sistema de salud, lo cual implica que la institución sea vulnerable a ataques mal intencionados o mala manipulación de la información lo que acarrea problemas económicos, legales, y administrativos.

Por lo cual este documento busca establecer una línea de trabajo que permita a la entidad sortear los riesgos que lo rodean, busca guardar los datos de los usuarios, y lograr que su información este segura.

## 2. TERMINOS


) 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).

) Activo de Información En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.

) 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).



|   |   |                      |
|---|---|----------------------|
|  | <b>PROCESO GESTIÓN TECNOLÓGICA E<br/>INFORMÁTICA.</b>   | <b>GTI-SIS-PI-03</b> |
|   | <b><i>Plan de tratamiento de riesgos de seguridad<br/>y privacidad de la información.</i></b> | <b>Ver. 03</b>       |

) Amenazas Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000). Análisis de Riesgo Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

) Auditoría Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

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

) Bases de Datos Personales Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

) Ciberseguridad Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701). ) Ciberespacio Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).


) Control Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

) Datos Abiertos Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

) 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



|   |   |                      |
|---|---|----------------------|
|  | <b>PROCESO GESTIÓN TECNOLÓGICA E<br/>INFORMÁTICA.</b>   | <b>GTI-SIS-PI-03</b> |
|   | <b><i>Plan de tratamiento de riesgos de seguridad<br/>y privacidad de la información.</i></b> | <b>Ver. 03</b>       |

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).

) Datos Personales Privados Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

) Datos Personales Mixtos Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

) Datos Personales Sensibles Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).


) Declaración de aplicabilidad Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

) Derecho a la Intimidad Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

) Encargado del Tratamiento de Datos Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

) Gestión de incidentes de seguridad de la información Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).



|   |   |                      |
|---|---|----------------------|
|  | <b>PROCESO GESTIÓN TECNOLÓGICA E<br/>INFORMÁTICA.</b>   | <b>GTI-SIS-PI-03</b> |
|   | <b><i>Plan de tratamiento de riesgos de seguridad<br/>y privacidad de la información.</i></b> | <b>Ver. 03</b>       |

) Información Pública Clasificada Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

) Información Pública Reservada Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

) Plan de continuidad del negocio Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

) Plan de tratamiento de riesgos Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

) Privacidad En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.


) Responsabilidad Demostrada Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

) Responsable del Tratamiento de Datos Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

) Riesgo Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele





|   |   |                      |
|---|---|----------------------|
|  | <b>PROCESO GESTIÓN TECNOLÓGICA E<br/>INFORMÁTICA.</b>   | <b>GTI-SIS-PI-03</b> |
|   | <i><b>Plan de tratamiento de riesgos de seguridad<br/>y privacidad de la información.</b></i> | <b>Ver. 03</b>       |

considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

) Seguridad de la información Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

) Sistema de Gestión de Seguridad de la Información SGSI Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

) Titulares de la información Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

) Trazabilidad Calidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

## 3. OBJETIVOS

### 3.1. Objetivo General


Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en el HOSPITAL MALVINAS HECTOR OROZCO OROZCO con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

### 3.2. Objetivos Específicos

Realizar el plan de trabajo específico validando los recursos con los que se cuentan actualmente en el HOSPITAL MALVINAS HECTOR OROZCO OROZCO para tener un plan de tratamiento de riesgo de seguridad y privacidad de la información.

) Promover el uso de mejores prácticas de seguridad de la información.



|   |   |                      |
|---|---|----------------------|
|  | <b>PROCESO GESTIÓN TECNOLÓGICA E<br/>INFORMÁTICA.</b>   | <b>GTI-SIS-PI-03</b> |
|   | <b><i>Plan de tratamiento de riesgos de seguridad<br/>y privacidad de la información.</i></b> | <b>Ver. 03</b>       |

) Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas del Hospital y los centros de salud.

) Optimizar la gestión de la seguridad de la información al interior con los dispositivos de interconexión de redes.

## 4. RECURSOS

- ) Humano: Gerente General, Líderes del Proceso, Profesional 2 Tecnología, Personal Externo
- ) Físico: PC y equipos de cómputo y de interconexión de redes de datos.

## 5. RESPONSABLES


- ) Gerente General
- ) Líderes del Proceso
- ) Profesional en Tecnología

## 6. METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Plan de tratamiento de Seguridad y Privacidad de la Información en el HOSPITAL MALVINAS HECTOR OROZCO OROZCO y las sedes, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos.





|   |  |                      |
|---|--|----------------------|
|  | <b>PROCESO GESTIÓN TECNOLÓGICA E INFORMÁTICA.</b>                                  | <b>GTI-SIS-PI-03</b> |
|   | <i>Plan de tratamiento de riesgos de seguridad y privacidad de la información.</i> | <b>Ver. 03</b>       |

## 6. PLAN DE TRATAMIENTO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ACTIVIDADES


1. Realizar Diagnóstico
2. Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información
3. Realizar la Identificación de los Riesgos con los líderes del Proceso.
4. Valorar del riesgo
5. Realizar Mapas donde se ubican los riesgos
6. Plantear al plan de tratamiento de riesgo aprobado por los líderes

### DESCRIPCIÓN DEL CICLO DE OPERACIÓN



Fuente: Modelo de Seguridad y Privacidad de la Información emitida por MinTIC



|   |   |                      |
|---|---|----------------------|
|  | <b>PROCESO GESTIÓN TECNOLÓGICA E<br/>INFORMÁTICA.</b>   | <b>GTI-SIS-PI-03</b> |
|   | <b><i>Plan de tratamiento de riesgos de seguridad<br/>y privacidad de la información.</i></b> | <b>Ver. 03</b>       |

## 7. CUMPLIMIENTO DE IMPLEMENTACIÓN


De acuerdo a las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación

- ) Revisión y/o Modificación de la actual Política de Seguridad.
- ) Aspectos organizativos de la seguridad de la información
- ) Seguridad Ligada a los recursos humanos
- ) Revisión del Control de acceso
- ) Seguridad en la operativa
- ) Seguridad en las telecomunicaciones
- ) Gestión de Incidentes de Seguridad de la Información
- ) Aspectos de seguridad de la información en la gestión de continuidad del negocio.

## 8. CRONOGRAMA

| ACTIVIDAD   | ENERO | FEBRERO | MARZO | ABRIL | MAYO | JUNIO | JULIO | AGOSTO | SEPTIEMBRE | OCTUBRE | NOVIEMBRE | DICIEMBRE |
|---|-------|---------|-------|-------|------|-------|-------|--------|------------|---------|-----------|-----------|
| 1. Realizar Diagnostico   | X     | X       |       |       |      |       |       |        |            |         |           |           |
| 2. Realizar la identificación de los riesgos con los líderes del proceso                              |       |         | X     | X     |      |       |       |        |            |         |           |           |
| 3. Elaborar el alcance del plan del tratamiento de riesgo de seguridad y privacidad de la información |       |         |       |       | X    | X     | X     |        |            |         |           |           |
| 4. Valorar el riesgo  |       |         |       |       |      |       |       | X      |            |         |           |           |
| 5. Realizar mapas donde se ubican los riesgos   |       |         |       |       |      |       |       |        | X          | X       |           |           |
| 6. Plantear al plan de tratamiento de riesgo aprobado por los líderes                                 |       |         |       |       |      |       |       |        |            |         | X         | X         |



|   |  |                      |
|---|--|----------------------|
|  | <b>PROCESO GESTIÓN TECNOLÓGICA E<br/>INFORMÁTICA.</b>                                  | <b>GTI-SIS-PI-03</b> |
|   | <i>Plan de tratamiento de riesgos de seguridad<br/>y privacidad de la información.</i> | <b>Ver. 03</b>       |

## 9. SEGUIMIENTO Y EVALUACIÓN

Se estará pendiente de las revisiones y actualizaciones y de los cambios de cada área.


## 10. DIAGNOSTICO E IDENTIFICACION DE RIESGOS

| AREA ASISTENCIAL Y FINANCIERA | RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN |
|-------------------------------|---|
| ✓ Red eléctrica               | Cableado mal instalado sin normas                   |
| ✓ Equipos                     | Equipos sin polo a tierra                           |
| ✓ Red de datos                | La red inalámbrica                                  |
| ✓ UPS                         | Regulación de la energía                            |
| <b>DATOS LOGICOS</b>          |   |
| Claves                        | Préstamo de claves de acceso al sistema             |

|                 |   |
|-----------------|---|
| ✓ Red eléctrica | Cableado mal instalado sin normas, tomas de difícil acceso.   |
| ✓ Equipos       | Equipos sin polo a tierra   |
| ✓ Red de datos  | La red inalámbrica en áreas neurálgicas como consulta externa, urgencias, cirugía, maternidad y hospitalización   |
| ✓ UPS           | Regulación de la energía  |
| ✓ internet      | No se cuenta con un cortafuego para configurar las páginas de internet que se pueden bloquear, este proceso se realiza manual y algunos funcionarios pueden violar esa seguridad. |
| Claves          | Préstamo de claves de acceso al sistema   |
| Estática        | Las torres de los equipos de cómputo se llenan de estática por que se encuentran en el suelo.   |
| PC              | Ausencia de equipos de cómputo remanentes para cubrir las necesidades en caso de daños  |

| <b>CONTROL DE CAMBIOS</b> |                           |
|---------------------------|---------------------------|
| VERSIÓN                   | MODIFICACION              |
| Ver. 01                   | Se generó el documento.   |
| Ver. 02                   | Se modificó el documento. |



|   |   |                      |
|---|---|----------------------|
|  | <b>PROCESO GESTIÓN TECNOLÓGICA E<br/>INFORMÁTICA.</b>   | <b>GTI-SIS-PI-03</b> |
|   | <i><b>Plan de tratamiento de riesgos de seguridad<br/>y privacidad de la información.</b></i> | <b>Ver. 03</b>       |

|         |                           |
|---------|---------------------------|
| Ver. 03 | Se modificó el documento. |
|---------|---------------------------|

