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

PTRSI

2021

HOSPITAL DEL ROSARIO ESE IAMI
CAMPOALEGRE - HUILA

TABLA DE CONTENIDO

1. Introducción

Durante el segundo semestre del año 2020, el Consejo Nacional de Política Económica y Social, publico el Documento CONPES 3995 sobre POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL, el cual resalta que "El entorno digital es un escenario en el que globalmente se desarrollan cada vez más todo tipo de actividades socioeconómicas. Esto expone tanto a las personas como a las mismas organizaciones a amenazas cibernéticas por parte de delincuentes que aprovechan el creciente intercambio de información. Se debe apuntar a que existan las medidas suficientes, tanto en el fortalecimiento de la seguridad, como en la generación de la confianza digital, respecto a una adecuada anticipación, gestión de riesgos, atención oportuna y defensa ante las amenazas existentes en el entorno digital, dentro de un marco de gobernanza nacional eficiente, acorde con las necesidades actuales y en constante desarrollo, en el que se pueda materializar rápidamente la confianza y la seguridad digital ante la aparición de nuevas tecnologías."

Sobre el anterior contexto el Hospital define el plan de tratamiento de riesgos de seguridad de la información para la vigencia 2021.

2. Objetivo

Identificar y controlar los riesgos asociados a los diferentes procesos tecnológicos que se llevan en la E.S.E HOSPITAL DEL ROSARIO. Con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de los usuarios encargados de dichos procesos.

El presente documento es el resultado de la actualización correspondiente a la vigencia 2021.

3. Marco normativo

La actualización del plan estratégico se define teniendo en cuenta el siguiente marco normativo:

Marco Normativo	Año	Descripción
Decreto 103 de 2015,	2019	Compendio de políticas aplican para todos los servidores públicos y contratistas de Función Pública que procesan y/o manejan información de la entidad.
Decreto 1494 de 2015	2019	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 1008	2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
Ley 1712 de 2014;	2018	Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.
Decreto 2573 de 2014	2018	Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones
Decreto 1377 de 2013	2018	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 2609 de 2012.	2017	Por el cual se reglamenta parcialmente la Ley 1581de 2012.
Ley estatutaria 1581 de 2012,	2017	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones
Ley 1474 de 2011	2017	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
Decreto 4632 de 2011	2017	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
Ley 1273 de 2009,	2016	Se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.

Ley 527 de 1999	2015	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
Constitución Política de Colombia1991 - Artículo 15	2015	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.
Ley 23 de 1982	2015	Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.
Norma técnica colombiana NTC - ISO/IEC 27001	2013	Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa
Ley 1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.

4. Tratamiento de riesgos

4.1. Factores de riesgo

Se priorizan los siguientes:

- Nivel de conocimiento del personal en amenazas digitales, políticas y controles de seguridad.
- Disponibilidad permanente de servicios esenciales como telecomunicaciones, energía e infraestructura.
- Identificación y protección de los datos de carácter personal.
- Adecuada clasificación de la información bajo custodia del hospital de acuerdo con el marco legal vigente.
- Segregación apropiada de roles y privilegios en todos los sistemas de información.

4.2. Valoración del riesgo

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y valorándolos con el fin de obtener información para establecer su nivel y las posibles acciones a implementar.

Dicho análisis incluye las fuentes, así como los factores que generan las consecuencias y aumentan la probabilidad de que ocurran. En la etapa de análisis se identifican los controles

existentes ya sean administrativos, técnicos y/o procedimientos implementados en la entidad. Por lo tanto, se analiza el riesgo combinando estimaciones de impacto y probabilidades en el contexto de las medidas de control existente.

La aplicación de análisis cualitativo facilita la calificación y evaluación de los riesgos al aplicar formas descriptivas para presentar la magnitud de las consecuencias potenciales (consecuencia) y la posibilidad de ocurrencia (probabilidad).

4.3. Estrategia de tratamiento de riesgo

Las estrategias en el tratamiento de riesgos consisten en minimizar la probabilidad de materialización del riesgo. Para ello, se puede evidenciar cuatro opciones:

- **Transferir:** Son procedimientos que permiten eliminar el riesgo por medio de la transferencia.
- **Mitigar:** Permite reducir la probabilidad de ocurrencia del riesgo o reducir sus consecuencias. La probabilidad de ocurrencia de un riesgo puede reducirse a través de controles de gestión, políticas y procedimientos encaminados a reducir la materialización del riesgo.
- **Evitar:** Puede evitarse el riesgo no procediendo con la actividad que incorporaría el riesgo, o escoger medios alternativos para la actividad que logren el mismo resultado y no incorporen el riesgo detectado.
- **Aceptar:** consiste en hacer frente a un riesgo (positivo o negativo) o porque no se ha identificado ninguna otra estrategia de respuesta adecuada.

4.3.1. Estrategia orientada al conocimiento

Mediante actividades de inducción, sensibilización y capacitación periódica se busca que todos los funcionaros, contratistas y demás colaboradores apropien conocimientos en materia de:

- Políticas institucionales de seguridad de la información.
- Uso seguro de los recursos informáticos.

4.3.2. Estrategia orientada a la continuidad

Para afrontar escenarios de riesgo asociados a la pérdida de continuidad, el hospital adelantará las siguientes acciones:

- Fortalecimiento de la infraestructura TIC.
    - Servidores (Hardware)
    - Seguridad perimetral
    - Antivirus
- Elaboración de planes de contingencia para la operación en cada una de las áreas en caso de: pérdida de continuidad de servicios informáticos o imposibilidad de acceso a la información.

4.3.3. Estrategia orientada al control de acceso

El hospital estima las siguientes acciones:

- Definir los instrumentos de acceso a la información pública.
- Definir los controles de acceso a activos de información con roles y privilegios más precisos.
- Elaborar los acuerdos de confidencialidad para funcionarios, contratistas y demás colaboradores.

4.3.4. Estrategia de controles tecnológicos

El hospital implementará:

- Identificación de eventos potencialmente nocivos por medio del UTM.
- Reforzamiento de controles de acceso a servicios TIC.
- Verificación y control de copias de seguridad.
- Aplicación de parches de seguridad y actualización de equipos.

4.4. Plan de trabajo

Estrategia	2021											
	01	02	03	04	05	06	07	08	09	10	11	12
Conocimiento						x	x	x	x	x	x	x
Continuidad						x	x	x	x	x	x	x
Control acceso						x	x	x	x	x	x	x
Control técnico						x	x	x	x	x	x	x

Nelson Leonardo Fierro González
Gerente E.S.E. Hospital del Rosario