

	ESE HOSPITAL DEL ROSARIO		
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - PTRSI</b>		
VIGENCIA: 17-ENE-2024	CODIGO: CGO-PL-01	VERSION: 02	Página 0 de 14



# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - PTRSI




E.S.E. HOSPITAL DEL ROSARIO

CAMPOALEGRE - HUILA

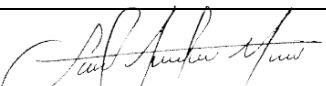

**VIGENCIA 2024**

"RECUPERAR TU SALUD ES NUESTRA PRIORIDAD"		
 Elaboró: Saul Andrés Murcia Jurado Cargo: Asesor Tic	 Revisó: Martha Cecilia Puentes Arias Cargo: Profesional Universitaria Administrativo Y Financiero	Aprobó: Nelson Leonardo Fierro González (Acta 17/01/2024 Comité Institucional De Gestión Y Desempeño) Cargo: Gerente

	ESE HOSPITAL DEL ROSARIO		
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - PTRSI</b>		
VIGENCIA: 17-ENE-2024	CODIGO: CGO-PL-01	VERSION: 02	Página 1 de 14

## TABLA DE CONTENIDO

1. Introducción.....	2
2. Objetivo .....	2
3. Alcance.....	2
4. Definiciones .....	3
5. Marco normativo .....	6
6. Tratamiento de riesgos.....	7
6.1. Factores de riesgo .....	7
6.2. Valoración del riesgo .....	8
6.3. Estrategia de tratamiento de riesgo .....	9
6.3.1. Estrategia orientada al conocimiento .....	9
6.3.2. Estrategia orientada a la continuidad .....	9
6.3.3. Estrategia orientada al control de acceso .....	10
6.3.4. Estrategia de controles tecnológicos .....	10
7. Seguimiento y Evaluación Vigencia 2020 – 2023.....	11
8. Plan de trabajo.....	13

“RECUPERAR TU SALUD ES NUESTRA PRIORIDAD”		
 Elaboró: Saul Andrés Murcia Jurado Cargo: Asesor Tic	 Revisó: Martha Cecilia Puentes Arias Cargo: Profesional Universitaria Administrativo Y Financiero	Aprobó: Nelson Leonardo Fierro González (Acta 17/01/2024 Comité Institucional De Gestión Y Desempeño) Cargo: Gerente

	ESE HOSPITAL DEL ROSARIO		
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - PTRSI</b>		
VIGENCIA: 17-ENE-2024	CODIGO: CGO-PL-01	VERSION: 02	Página 2 de 14

## 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 2024.

## 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 2024.

## 3. Alcance

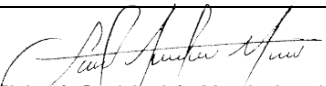

Este documento describe el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSI) para la vigencia 2024 de la **E.S.E HOSPITAL DEL ROSARIO DE CAMPOALEGRE - HUILA**, las directrices de actualización de este Plan estratégico serán dadas por el Coordinador de Sistemas y la Gerencia de la ESE.


### 3.1. A QUIEN VA DIRIGIDO

A todos los colaboradores y/o funcionarios de la E.S.E Hospital del Rosario involucrados en la gestión de los recursos respectivos a las Tecnologías de la Información y la Comunicación (TIC).

### 3.2. RESPONSABLE DEL DOCUMENTO

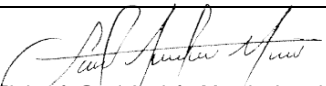

Coordinador del Área de Sistemas del Hospital del Rosario.


“RECUPERAR TU SALUD ES NUESTRA PRIORIDAD”		
 Elaboró: Saul Andrés Murcia Jurado Cargo: Asesor Tic	 Revisó: Martha Cecilia Puentes Arias Cargo: Profesional Universitaria Administrativo Y Financiero	Aprobó: Nelson Leonardo Fierro González (Acta 17/01/2024 Comité Institucional De Gestión Y Desempeño) Cargo: Gerente

	ESE HOSPITAL DEL ROSARIO		
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - PTRSI</b>		
VIGENCIA: 17-ENE-2024	CODIGO: CGO-PL-01	VERSION: 02	Página 3 de 14

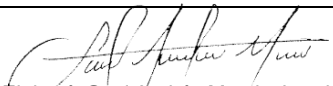

## 4. Definiciones



- **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 controle 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)
- **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).

"RECUPERAR TU SALUD ES NUESTRA PRIORIDAD"		
 Elaboró: Saul Andrés Murcia Jurado Cargo: Asesor Tic	 Revisó: Martha Cecilia Puentes Arias Cargo: Profesional Universitaria Administrativo Y Financiero	Aprobó: Nelson Leonardo Fierro González (Acta 17/01/2024 Comité Institucional De Gestión Y Desempeño) Cargo: Gerente

	ESE HOSPITAL DEL ROSARIO		
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - PTRSI</b>		
VIGENCIA: 17-ENE-2024	CODIGO: CGO-PL-01	VERSION: 02	Página 4 de 14

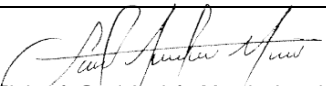

- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple,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


"RECUPERAR TU SALUD ES NUESTRA PRIORIDAD"		
 Elaboró: Saul Andrés Murcia Jurado Cargo: Asesor Tic	 Revisó: Martha Cecilia Puentes Arias Cargo: Profesional Universitaria Administrativo Y Financiero	Aprobó: Nelson Leonardo Fierro González (Acta 17/01/2024 Comité Institucional De Gestión Y Desempeño) Cargo: Gerente

	ESE HOSPITAL DEL ROSARIO		
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - PTRSI</b>		
VIGENCIA: 17-ENE-2024	CODIGO: CGO-PL-01	VERSION: 02	Página 5 de 14

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).
- **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).
- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **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.
- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25).

"RECUPERAR TU SALUD ES NUESTRA PRIORIDAD"		
 Elaboró: Saul Andrés Murcia Jurado Cargo: Asesor Tic	 Revisó: Martha Cecilia Puentes Arias Cargo: Profesional Universitaria Administrativo Y Financiero	Aprobó: Nelson Leonardo Fierro González (Acta 17/01/2024 Comité Institucional De Gestión Y Desempeño) Cargo: Gerente

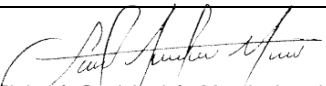

	ESE HOSPITAL DEL ROSARIO		
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - PTRSI</b>		
VIGENCIA: 17-ENE-2024	CODIGO: CGO-PL-01	VERSION: 02	Página 6 de 14



- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele 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).
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).
- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad:** Cualidad 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).
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

## 5. 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.

"RECUPERAR TU SALUD ES NUESTRA PRIORIDAD"		
 Elaboró: Saul Andrés Murcia Jurado Cargo: Asesor Tic	 Revisó: Martha Cecilia Puentes Arias Cargo: Profesional Universitaria Administrativo Y Financiero	Aprobó: Nelson Leonardo Fierro González (Acta 17/01/2024 Comité Institucional De Gestión Y Desempeño) Cargo: Gerente

	ESE HOSPITAL DEL ROSARIO		
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - PTRSI</b>		
VIGENCIA: 17-ENE-2024	CODIGO: CGO-PL-01	VERSION: 02	Página 7 de 14

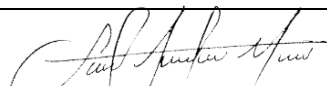

Marco Normativo	Año	Descripción
Decreto 2573 de 2014	2018	Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones
Decreto 1377 de 2013	2018	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno 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 1581 de 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 Colombia 1991 - 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.

## 6. Tratamiento de riesgos



### 6.1. Factores de riesgo

Se priorizan los siguientes:

- Los ataques cibernéticos inician regularmente mediante el envío de correos electrónicos o WhatsApp (Phishing) aparentemente de una fuente confiable, que se redirige a un sitio

"RECUPERAR TU SALUD ES NUESTRA PRIORIDAD"		
 Elaboró: Saul Andrés Murcia Jurado Cargo: Asesor Tic	 Revisó: Martha Cecilia Puentes Arias Cargo: Profesional Universitaria Administrativo Y Financiero	Aprobó: Nelson Leonardo Fierro González (Acta 17/01/2024 Comité Institucional De Gestión Y Desempeño) Cargo: Gerente



	ESE HOSPITAL DEL ROSARIO		
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - PTRSI</b>		
VIGENCIA: 17-ENE-2024	CODIGO: CGO-PL-01	VERSION: 02	Página 8 de 14

web falso con gran cantidad de malware, que se define como un código malicioso que permite la evasión de controles de seguridad y aprende de forma autónoma a escalar accesos en la red.

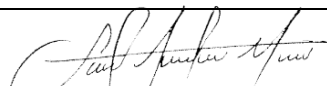

- Los ataques BEC tienen como objetivo controlar cuentas de correos empresariales, mediante técnicas de suplantación avanzada.
- Los Ransomware se definen como un programa de software malicioso que secuestra la información de una entidad, como bases de datos, para luego exigir un pago para reestablecer la recuperación de la información.
- 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.



## 6.2. 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).

"RECUPERAR TU SALUD ES NUESTRA PRIORIDAD"		
 Elaboró: Saul Andrés Murcia Jurado Cargo: Asesor Tic	 Revisó: Martha Cecilia Puentes Arias Cargo: Profesional Universitaria Administrativo Y Financiero	Aprobó: Nelson Leonardo Fierro González (Acta 17/01/2024 Comité Institucional De Gestión Y Desempeño) Cargo: Gerente

	ESE HOSPITAL DEL ROSARIO		
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - PTRSI</b>		
VIGENCIA: 17-ENE-2024	CODIGO: CGO-PL-01	VERSION: 02	Página 9 de 14

### 6.3. 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.

#### 6.3.1. Estrategia orientada al conocimiento

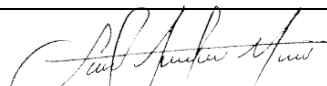
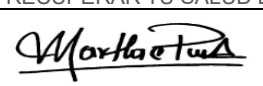
Mediante actividades de inducción, sensibilización y capacitación periódica se busca que todos los funcionarios, contratistas y demás colaboradores apropien conocimientos en materia de:


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

#### 6.3.2. 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)

"RECUPERAR TU SALUD ES NUESTRA PRIORIDAD"		
 Elaboró: Saul Andrés Murcia Jurado Cargo: Asesor Tic	 Revisó: Martha Cecilia Puentes Arias Cargo: Profesional Universitaria Administrativo Y Financiero	Aprobó: Nelson Leonardo Fierro González (Acta 17/01/2024 Comité Institucional De Gestión Y Desempeño) Cargo: Gerente

	ESE HOSPITAL DEL ROSARIO		
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - PTRSI</b>		
VIGENCIA: 17-ENE-2024	CODIGO: CGO-PL-01	VERSION: 02	Página 10 de 14

- 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.

### 6.3.3. Estrategia orientada al control de acceso

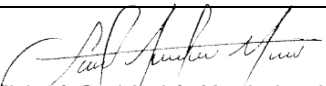

El hospital estima las siguientes acciones:

- 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.
- Elaborar el inventario de usuarios y contraseñas de las diferentes plataformas utilizadas en la ESE

### 6.3.4. 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.

"RECUPERAR TU SALUD ES NUESTRA PRIORIDAD"		
 Elaboró: Saul Andrés Murcia Jurado	 Revisó: Martha Cecilia Puentes Arias	Aprobó: Nelson Leonardo Fierro González (Acta 17/01/2024 Comité Institucional De Gestión Y Desempeño)
Cargo: Asesor Tic	Cargo: Profesional Universitaria Administrativo Y Financiero	Cargo: Gerente

	ESE HOSPITAL DEL ROSARIO		
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - PTRSI</b>		
VIGENCIA: 17-ENE-2024	CODIGO: CGO-PL-01	VERSION: 02	Página 11 de 14

## 7. Seguimiento y Evaluación Vigencia 2020 – 2023

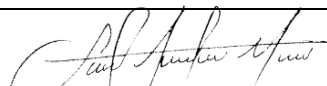

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSI) se sometió a un riguroso monitoreo para evaluar la efectividad de los controles de seguridad implementados. Se realizaron auditorías regulares y revisiones de las políticas de seguridad para asegurar la protección continua de la información sensible y la adaptación a posibles amenazas.



Durante este periodo se realizaron actividades de capacitación e inducción de políticas institucionales de seguridad de la información y uso seguro de recursos informáticos, tienen como objetivo principal dotar al personal de las habilidades y conocimientos necesarios para proteger la integridad, confidencialidad y disponibilidad de la información institucional. Estas actividades incluyen sesiones formativas que abordan las políticas y procedimientos específicos relacionados con la seguridad de la información, así como la promoción de prácticas seguras en el uso de recursos informáticos. La capacitación busca sensibilizar al personal sobre las amenazas cibernéticas, promover comportamientos seguros, y asegurar el cumplimiento de las normativas internas y externas. Además, fomenta la creación de una cultura organizacional consciente de la importancia de la seguridad de la información y la responsabilidad compartida en su resguardo.

El fortalecimiento de la infraestructura y seguridad implica implementar medidas y mejoras significativas en los componentes tecnológicos y procedimientos relacionados con la infraestructura de la organización. Esto incluye la optimización de redes, servidores y sistemas, así como la adopción de tecnologías avanzadas para garantizar un entorno robusto y eficiente. En el contexto de seguridad, implica el desarrollo y la implementación de estrategias y controles que protejan activamente los activos digitales contra amenazas y vulnerabilidades. Estas acciones tienen como objetivo principal mejorar la disponibilidad, confidencialidad e integridad de los sistemas, asegurando al mismo tiempo un ambiente propicio para el manejo seguro de la información y la continuidad operativa. Durante esta vigencia se realizó una inversión importante en la adquisición de un sistema de seguridad perimetral completo que sirve para contrarrestar riesgos de seguridad de la información, bloqueo de páginas web, administración de VPN y creación de políticas de seguridad que sirvan para minimizar las vulnerabilidades en nuestra ESE.

Se han definido controles de acceso a activos de información, lo que implica establecer medidas y políticas que regulen y protejan la forma en que las personas y sistemas acceden a los recursos digitales de la organización. Este proceso abarca la identificación de usuarios autorizados, la asignación de niveles de acceso adecuados a cada usuario, y la implementación de tecnologías y políticas que restrinjan el acceso no autorizado. El objetivo principal es salvaguardar la confidencialidad, integridad y disponibilidad de la información, evitando accesos no permitidos y garantizando que cada usuario tenga únicamente el acceso necesario para realizar sus funciones. Este enfoque contribuye significativamente a la seguridad y gestión eficiente de los activos de información de la organización.

La verificación y control de copias de seguridad es una tarea importante que busca la implementación de procedimientos para asegurar la integridad y disponibilidad de la información almacenada en servidores y Discos Duros externos. Este proceso incluye la verificación regular de la realización exitosa de las copias

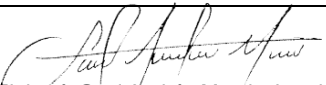

"RECUPERAR TU SALUD ES NUESTRA PRIORIDAD"		
 Elaboró: Saul Andrés Murcia Jurado Cargo: Asesor Tic	 Revisó: Martha Cecilia Puentes Arias Cargo: Profesional Universitaria Administrativo Y Financiero	Aprobó: Nelson Leonardo Fierro González (Acta 17/01/2024 Comité Institucional De Gestión Y Desempeño) Cargo: Gerente

	ESE HOSPITAL DEL ROSARIO		
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - PTRSI</b>		
VIGENCIA: 17-ENE-2024	CODIGO: CGO-PL-01	VERSION: 02	Página 12 de 14

de seguridad, la validación de la integridad de los datos almacenados y la garantía de que se puedan recuperar eficientemente en caso de pérdida de información. Además, implica establecer controles para prevenir accesos no autorizados a los respaldos y garantizar la confidencialidad de la información almacenada en ellos. El objetivo principal es asegurar que las copias de seguridad sean confiables, estén disponibles cuando se necesiten y cumplan con los estándares de seguridad establecidos, contribuyendo así a la continuidad operativa y la recuperación ante desastres.

El seguimiento y evaluación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2020-2023 implica un proceso continuo de monitoreo y revisión de las estrategias implementadas para mitigar los riesgos asociados a la seguridad de la información. Durante este periodo, se llevaron a cabo evaluaciones periódicas para medir la efectividad de las medidas adoptadas, identificar nuevas amenazas o vulnerabilidades, y ajustar el plan en consecuencia. El objetivo principal es garantizar la protección constante de la confidencialidad, integridad y disponibilidad de la información, así como la adaptación proactiva a cambios en el entorno de seguridad cibernética y normativas relacionadas. Este proceso permite una gestión ágil y eficiente de los riesgos, asegurando la continuidad operativa y la confianza en la gestión de la información.

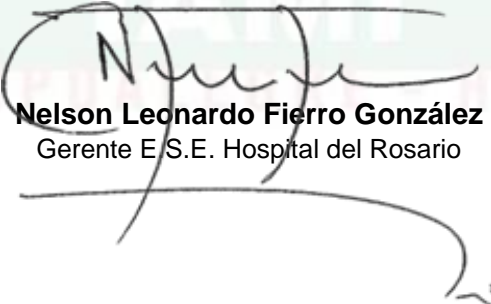


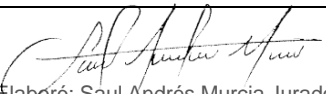

"RECUPERAR TU SALUD ES NUESTRA PRIORIDAD"		
 Elaboró: Saul Andrés Murcia Jurado Cargo: Asesor Tic	 Revisó: Martha Cecilia Puentes Arias Cargo: Profesional Universitaria Administrativo Y Financiero	Aprobó: Nelson Leonardo Fierro González (Acta 17/01/2024 Comité Institucional De Gestión Y Desempeño) Cargo: Gerente

	ESE HOSPITAL DEL ROSARIO		
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - PTRSI</b>		
VIGENCIA: 17-ENE-2024	CODIGO: CGO-PL-01	VERSION: 02	Página 13 de 14

## 8. Plan de trabajo

Estrategia		2024											
		1	2	3	4	5	6	7	8	9	10	11	12
Actividades de Capacitacion e induccion de politicas institucionales de seguridad de la informacion y uso seguro de recursos informaticos.	Políticas institucionales de seguridad de la informacion.			X			X			X			X
	Uso seguro de los recursos informaticos.												
	Uso seguro de plataformas bancarias.												
Fortalecimiento de la infraestructura y seguridad	Servidores (Hardware).	X	X	X	X	X	X	X	X	X	X	X	X
	Seguridad perimetral.												
	Antivirus.												
Definir los controles de acceso a activos de informacion	Definir los instrumentos de acceso a la informacion publica.												
	Definir los controles de acceso a activos de informacion con roles y privilegios mas precisos.												
	Elaborar los acuerdos de confidencialidad para funcionarios, contratistas y demas colaboradores.	X	X	X	X	X	X	X	X	X	X	X	X
	Elaborar el inventario de usuarios y contraseñas de las diferentes plataformas utilizadas en la ESE.												
Verificacion y control de copias de seguridad	Identificacion de eventos potencialmente nocivos por medio del UTM.												
	Reforzamiento de controles de acceso a servicios TIC.	X	X	X	X	X	X	X	X	X	X	X	X
	Verificacion y control de copias de seguridad.												
	Aplicación de parches de seguridad y actualizacion de equipos.												

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

"RECUPERAR TU SALUD ES NUESTRA PRIORIDAD"		
 Elaboró: Saul Andrés Murcia Jurado Cargo: Asesor Tic	 Revisó: Martha Cecilia Puentes Arias Cargo: Profesional Universitaria Administrativo Y Financiero	Aprobó: Nelson Leonardo Fierro González (Acta 17/01/2024 Comité Institucional De Gestión Y Desempeño) Cargo: Gerente