PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DEL AÑO 2025

ESE HOSPITAL SAN LUCAS DE EL MOLINO

ISABEL PAULINA APONTE DIAZ

EL MOLINO LA GUAJIRA AÑO 2025

TABLA DE CONTENIDO

INTRODUCCION

El presente plan se elabora con el fin de dar a conocer como se realizará la implementación y socialización de la Política de **Seguridad y Privacidad de la Información**, el cual busca guardar los datos de los ciudadanos como un tesoro, garantizando la seguridad de la información.

La Gestión del Riesgo es una herramienta gerencial que apoya la toma de decisiones organizacionales facilitando con ello el cumplimiento de los objetivos del negocio.

La gestión de los riesgos de seguridad de la información son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

Según la Norma Técnica NTCGP1000:2009, el riesgo es “Toda posibilidad de ocurrencia de aquella situación que pueda afectar el desarrollo normal de las funciones de la entidad y el logro de sus objetivos”.

Casi siempre una situación no prevista regularmente provoca una crisis y consecuencias que, de acuerdo a su impacto y valor, pueden ser catastróficas para los intereses de la Entidad, y atentos a ello, pretendemos definir un documento asertivo y ejecutable para la entidad municipal, en materia de recuperación de la normalidad para situaciones que se generen en los activos de información.

Conocer los riesgos a los cuales están expuestos los activos de información es la única manera de poderlos gestionar y poder reducir sus impactos, y para ello es necesario identificar los activos de información, sus amenazas, vulnerabilidades, valorarlos de acuerdo al impacto de integridad, disponibilidad y confidencialidad.

A través del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información la ESE Hospital San Lucas de El Molino busca garantizar la continuidad delos servicio como entidad pública. Por esta razón, se encontró la necesidad de

desarrollar un análisis de riesgo de seguridad de la información ajustado a la realidad que enfrenta en su infraestructura tecnológica. Antes de la formulación y ejecución del Plan de Gestión se ha construido el diagnóstico donde primero se describe los aspectos básicos de la entidad, se conoce la situación actual de la organización y la identificación de los activos con sus respectivas amenazas, para continuar con la medición de riesgos existentes y sugerir las protecciones necesarias que podrían formar parte del Plan de Gestión de Riesgos en la seguridad de la información.

1. DEFINICIONES

- **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).

- **Aceptación del Riesgo:**

  Decisión de aceptar un riesgo.

- **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.

  Información: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la ESE HOSPITAL SAN LUCAS de El Molino Ejemplo: archivo de Excel.

  Activos físicos: hace referencia a los activos fijos tales como equipos de cómputo, de comunicaciones, de soporte (impresoras, escáner y teléfono IP) y demás bienes muebles.

  Aplicaciones: Es todo el software que se utiliza para la gestión de la información.

  Ejemplo: SYSMAN

  Personal: Es todo el personal de la EMPRESA SOCIAL DEL ESTADO HOSPITAL SAN LUCAS de El Molino La Guajira, subcontratado, los clientes, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la Entidad.
  Servicios: Son tanto los servicios internos, como los externos, aquellos que la organización suministra a personal interno, clientes y usuarios.

- **Administración del Riesgo:**

  Actividades encaminadas a la intervención de los riesgos de la entidad, a través de la identificación, valoración, evaluación, manejo y monitoreo de los mismos de forma que se apoye el cumplimiento de los objetivos de la entidad.

- **Análisis de Riesgos**:

  Determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del riesgo.

- **Activos de Información:**

  Es el elemento de información que cada entidad territorial recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre presente en forma impresa, escrita en papel, transmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo datos contenidos en registros, archivos, bases de datos, videos e imágenes.

- **Amenaza:**

  Es un evento accidental o intencionado que puede causar un daño a un activo de información. Puede ser:

  - **Natural:** Terremoto.
  - **Agente externo:** Virus o malware.
  - **Agentes internos:** Funcionario molesto

- **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).

- **Análisis de Riesgo**

  Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC27000).

- **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).

- **Consecuencias:** Hechos o acontecimientos que se derivan o resultan de la ocurrencia o la materialización de un riesgo.

- **Corrupción:** Uso del poder para desviar la gestión de lo público hacia el beneficio privado.

- **Causas:** Medios, circunstancias, situaciones o agentes generadores del evento**.**

- **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 CRC2258 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 (Ley1712 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.

(Ley1581 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)

- **Evento:**

  Hecho que se genera durante la gestión de un proceso afectando el logro del objetivo del mismo, tiene relación directa con las actividades críticas de los planes operativos, las actividades de ruta crítica de los Proyectos de Inversión y las actividades críticas de control de los procesos.

- **Frecuencia:**

  Periodicidad con que ha ocurrido un evento.

- **Gestor del Riesgo:**

  Funcionario líder de la dependencia, quien apoya al responsable del riesgo.

- **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).

- **Identificación del Riesgo:**

  Descripción de la situación no deseada.

- **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 Ley1712 de 2014. (Ley 1712 de 2014, art 6).

- **Impacto:**

  Consecuencias de la materialización de una amenaza.

- **Mapa de riesgos:**

  Herramienta metodológica que permite hacer un inventario de los riesgos por proceso, haciendo la descripción de cada uno de ellos, las posibles consecuencias y su forma de tratamiento.

- **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 lamisma. (ISO/IEC 27000).

- **Políticas de manejo del Riesgo:**

  Son los criterios que orientan la toma de decisiones para tratar, y en lo posible minimizar, los riesgos en la entidad, en función de su evaluación.

- **Probabilidad**:

  Medida para estimar la posibilidad de que ocurra un evento.

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

- **Responsable del riesgo:**

  Es el encargado de identificar, valorar y definir el plan de contingencia, el manejo y monitoreo para cada uno de los riesgos del proceso bajo su responsabilidad.

- **Riesgo Residual:**

  Nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.

- **Riesgo Inherente:**

  Es el riesgo puro, al cual no se han aplicado controles, para controlarlo y buscar evitar su materialización.

- **Riesgo de corrupción:**

  Posibilidad de que, por acción u omisión, se use el poder para poder desviar la gestión de lo público hacia un beneficio privado.

- **Riesgo de seguridad de la información:**

  Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera.

  También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten

- **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).

- **Tratamiento:**

  Opciones que determinan el tipo de acciones a implementar para administrar el riesgo.

- **Titulares de la información**

  Personas naturales cuyos datos personales sean objeto de Tratamiento. (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).

- **Valoración:**

  Grado de exposición al riesgo con la clasificación de probabilidad e impacto aplicando los controles existentes.

- **Vulnerabilidad:**

  Debilidad de un activo que puede ser aprovechada por una amenaza para producir pérdidas o daños a la entidad.

2. OBJETIVOS

2.1 Objetivo General

Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en la ESE Hospital San Lucas de El Molino con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

2.2 Objetivos Específicos

- Ejecutar el plan de trabajo específico validando los recursos con los que se cuentan actualmente en la ESE Hospital San Lucas de El Molino para tener un plan de tratamiento de riesgo de seguridad y privacidad de la información.

- Identificar, evaluar y solucionar cualquier anomalía, de manera rápiday eficaz, que exista en los activos de información de la entidad.

- Implementar plan de contingencia que oriente recuperación de información en las diferentes secretarias y oficinas de la ESE HOSPITAL SAN LUCAS.
- Reducir al máximo la materialización de los riesgos asociados infraestructura tecnológica y sistemas de información.

- Garantizar la disponibilidad, integridad y confidencialidad de los activos de información de la entidad.

- Garantizar el normal desarrollo de los macro procesos de gestión dela entidad.

3. ALCANCE

Aplica a los activos de información de la ESE Hospital San Lucas de El Molino todos los funcionarios y terceros que laboren o tengan relación con la entidad, que sean dueños de activos de información de la entidad, son responsables por el análisis y valoración de los riesgos asociados a estos.

4. ROLES Y RESPONSABILIDADES

El plan de tratamiento de riesgos de seguridad digital de la Entidad es una responsabilidad conjunta y liderada por la secretaría de planeación en aras de cumplir con la Transformación Digital.

5. NORMATIVIDAD

- **Ley 1273 de 2009:** "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 1581 De 2012:** “Por la cual se dictan disposiciones generales para la protección de datos personales”.

- **Ley 1712 de 2014:** “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”,

- **ISO 27001:2013:** Sistemas De Gestión De Seguridad De La Información

6. IDENTIFICACIÓN, ANÁLISIS Y VALORACIÓN DE RIESGOS DE SEGURIDAD YPRIVACIDAD DE LA INFORMACIÓN

La ESE Hospital San Lucas de El Molino percibiendo la importancia y necesidad de proteger los activos de información derivados de los sistemas de información, redes de comunicaciones y servicios web, destinara recursos para la adquisición e implementación de controles de tipo tecnológicos, procedimentales y operaciones, minimizando de esta forma la exposición a peligros en el contorno digital que pueden afectar la integridad, confidencialidad y disponibilidad de la información.

Luego de revisión exhausta, mediante lluvia de ideas, se califican cada uno de los activos y se identifican amenazas y/o vulnerabilidades de cada uno de ellos para identificar los posibles riesgos de los activos de información.

La identificación de las amenazas que pueden afectar los activos de información de la ESE Hospital San Lucas de El Molino, de acuerdo a su integridad, confidencialidad y disponibilidad.

Fuego: Posibilidad que el fuego ocasiones daños en los recursos del sistema.

Inundación: Posibilidad que el agua ocasiones daños en los recursos del sistema.

Tormentas Eléctricas: Posibilidad que los rayos y descargas eléctricas ocasiones daños en los activos.

Alteración de Orden público: Desordenes que atenten contra personas y activos de información, que ocasionan daños y pérdidas.

Contaminación Mecánica: Vibraciones, polvo, suciedad que causan daños en los activos.

Contaminación Electromagnética: Interferencias de radio, ondas electromagnéticas, luz ultravioleta.

Daño Físico por Deterioro Natural: Desgaste de un activo por el uso y paso del tiempo.

Fallo en el Servicio de Comunicaciones: Cese de la capacidad de transmisión dela red, ya sea por daños físicos o lógicos.

Degradación de Medios de Almacenamiento: Desgaste de los medios de almacenamiento por el paso del tiempo.

Errores de los Usuarios: Equivocaciones de las personas cuando usan los servicios, datos, etc.

Errores de Configuración: Introducción de datos de configuración erróneo su omisión de parámetros de configuración.

Software Dañino: Virus, programas espías (spyware), gusanos, troyanos, bombas lógicas, spam, entre otros.

Fuga de Información: Revelación por indiscreción de manera verbal, medios electrónicos, soportes en papel, entre otros.

Alteración de Información: Alteración o cambios en la información.

Destrucción de Información: Eliminación de la información.

Errores en el Software: Defectos en el código que originan una operación defectuosa, sin intención por parte del usuario, pero que trae consecuencias en la eficiencia del sistema.

Ingeniería Social: Uso de la buena fe de las personas para realizar actividades que interesan a un tercero.

Instalación de Software no Autorizado: Instalación de software no licenciado.

Caída Servidor Externo: Fallos en servidor externo a la Entidad.

Accesos no Autorizados: Se tiene acceso a los activos sin estar autorizado para ello.

Denegación del Servicio: Indisponibilidad del uso del servicio ya sea por ataques intencionados o por agotamiento de recursos.

Robo: Sustracción de un activo de información, que provoca la carencia de este medio para prestar algún servicio.

Interceptación de Información: Tener acceso a la información, sin que esta sea alterada.

Repudio: Negación posterior de actuaciones.

Corte de Suministro Eléctrico: Cese o interrupción del servicio de fluido eléctrico.

Emanaciones Electromagnéticas: Poner en el campo electromagnético datos

para beneficios de terceros.

Errores de Seguimiento – LOGS: Falta de seguimiento, inadecuado registro de actividades: falta de registros, registros incompletos o incorrectos.

Sanciones por Entes de Control: Sanciones por incumplimiento en la normatividad.

Valoración de las Amenazas

Se realiza la valoración de las amenazas teniendo en cuenta su posibilidad de ocurrencia, de acuerdo con la siguiente escala cualitativa:

Nivel	Descriptor	Descripción	Frecuencia
1	Muy Baja	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en el último año
2	Baja	El evento puede ocurrir en algún momento	Al menos una vez en elúltimo año
3	Media	El evento podría ocurrir en algún momento	Al menos una vez Mensualmente
4	Alta	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos una vez semanalmente
5	Muy Alta	Se espera que el evento ocurra en la mayoría de las circunstancias	Al menos una vezen el Día

Tabla 1: Criterios para calificar amenazas

IDENTIFICACIÓN DE VULNERABILIDADES

La identificación de las vulnerabilidades o debilidades los activos de información de la ESE Hospital San Lucas de El Molino, las realiza el dueño del activo.

A cada activo de información se le identifica las vulnerabilidades que puedan ser explotadas por una amenaza.

VALORACION DEL RIESGO

La valoración del riesgo consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial o propio de la actividad también llamado ***"RIESGO INHERENTE"*.**

A continuación se establecen los criterios para definir el nivel de probabilidad:

NIVEL	FRECUENCIA DE LA ACTIVIDAD	FRECUENCIA DE EVENTOS	PROBABILIDAD
MUY BAJA	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año.	El evento puede ocurrir solo en circunstancias excepcionales (Poco comunes o anormales).	20%
BAJA	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	El evento puede ocurrir en algún momento.	40%
MEDIA	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	El evento podrá ocurrir en algún momento.	60%
ALTA	La actividad que conlleva el riesgo se ejecuta de 500 veces al año y máximo 5.000 veces por año.	Es viable que el evento ocurra en lamayoría delas circunstancias.	80%

MUY ALTA	La actividad que conlleva el riesgo se ejecuta más de 5.000 veces por año.	Se espera que el evento ocurra en la mayoría de las circunstancias.	100%

Tabla 2. Criterios para definir el nivel de PROBABILIDAD de ocurrencia de los riesgos.

Nota: En materia de tecnología (incluye disponibilidad de aplicativos) se tiene en cuenta 1hora de funcionamiento = 1 vez.

RIESGO DE SEGURIDAD DE LA INFORMACION		
NIVEL	**CUANTITATIVAS - ECONOMICA**	**CUALITATIVAS - REPUTACIONAL**
CATASTRÓFICO 100%	-Afectación mayor o igual al 50% de la población. -Afectación mayor o igual al 50% del presupuesto anual de seguridad digital. -Afectación muy grave del medio ambiente que requiere de mayor o igual a 3 años de recuperación.	-Afectación muy grave de la integridad de la información debido al interés Particular de los empleados y terceros. - Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. - Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MAYOR 80%	-Afectación en un valor igual o mayor al 20% e inferior al 50% de la población. -Afectación en un valor igual o mayor al 20% e inferior al 50% del presupuesto anual de seguridad digital. -Afectación importante del medio ambiente que requiere de 1 a 3 años de recuperación.	-Afectación grave de la integridad de la información debido al interés particular delos empleados y terceros. -Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. -Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

MODERADO 60%	-Afectación en un valor igual o mayor al 10% y menor al 20% de la población. -Afectación en un valor igual o mayor al 10% y menor al 20% del presupuesto anual de seguridad digital. - Afectación leve del medio ambiente requiere de 3 meses a 1 año de recuperación.	-Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. -Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. -Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MENOR 40%	-Afectación en un valor igual o mayor al 1% y menor al 10% de la población. -Afectación en un valor igual o mayor al 1% y menor al 10% del presupuesto anual de seguridad digital. -Afectación leve del medio ambiente requiere de Afectación leve del medio ambiente requiere de 1 a 3 meses de recuperación.	-Afectación leve de la integridad. -Afectación leve de la disponibilidad. -Afectación leve de la confidencialidad.
LEVE 20%	-Afectación en un valor menor al 1% de la población. -Afectación en un valor menor al 1% del presupuesto anual de seguridad digital. -No hay afectación medioambiental.	-Sin afectación de la integridad. -Sin afectación de la disponibilidad. -Sin afectación de la confidencialidad.

Tabla 3. Criterios para calificar el impacto / consecuencia – RIESGO DE SEGURIDAD DE LA INFORMACION

EVALUACIÓN DEL RIESGO – NIVEL DE RIESGO INHERENTE (SEVERIDAD)

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial **(RIESGO INHERENTE).** Para establecer el nivel de riesgo inherente (sin aplicación de controles) y residual (con aplicación de controles) se utilizan los Mapas de Calor, que permiten ubicar el riesgo en

la zona de acuerdo con la calificación de la **probabilidad** y el **impacto / consecuencia.** Para todos los riesgos de **gestión y de seguridad de la información**, se definen cuatro zonas de severidad en el mapa de calor como se menciona a continuación:

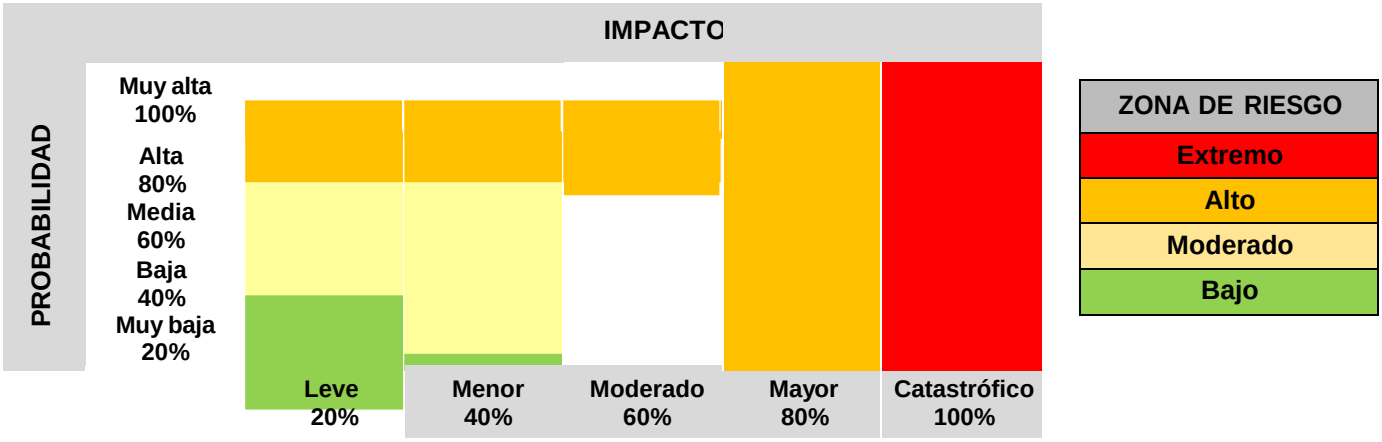

Figura 1. Mapa de Calor Riesgo Inherente

Según el plan de gestión de riesgos de seguridad y Privacidad de la Información, resultaron los diferentes riesgos a los que puede encontrarse sometida el área tecnológica y activos de información, ellos se pueden agrupar y resultan controlarse mediante acciones de mitigación, como se describe a continuación:

IDENTIFICACION, MITIGACION Y CALIFICACION DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION				
Riesgos	**Mitigación**	**Probabilidad**	**Impacto**	**Zona Riesgo**
Desastre natural	La estructura física de la sede de la ESE Hospital San Lucas de El Molino cuenta con una estructura sismo resistente y plan hospitalario de gestión del riesgo de desastres para respuestas a emergencias, ya sea de origen natural, o derivada de la misma acción del hombre sobre el medio ambiente.	1	3	Moderado
Interrupción del fluido eléctrico	La ESE Hospital San Lucas de E Molino cuenta con respaldo de una planta eléctrica en caso de fallas en fluido eléctrico, adicionalmente existe banco de UPS que respaldan el servidor o cuarto técnico.	3	1	Bajo
Pérdida o Robo de Información Digital	La ESE Hospital San Lucas de E Molino cuenta con respaldo de la información del servidor técnico en e área de facturación que se encuentran en el Data Center. Dicho respaldo se realiza todos los días en discos duros externos.	2	2	Bajo
Falla de equipos electrónicos	La ESE Hospital San Lucas de E Molino cuenta con plan de mantenimiento preventivo, predictivo y correctivo (hardware, software, telefonía IP) para todas las oficinas	2	2	Bajo
Falla en servidores	La ESE Hospital San Lucas de E Molino contrata profesionales que prestan los servicios técnicos de los servidores para actuar ante cualquie falla.	1	3	Moderado

Virus informáticos	La ESE Hospital San Lucas de E Molino contrata profesionales que interactúan en la configuración de los equipos, de acuerdo con políticas de seguridad y privacidad de información. Además se cuenta con licencias de antivirus para protección de equipos en tiempo real y servicio de firmware para contrarrestar amenazas externas.	3	1	Bajo
Calentamiento del Servidor técnico	La ESE Hospital San Lucas de E Molino cuenta con una supervisión permanente para el control de temperatura en el salón provisto para e la ubicación del servidor. Igualmente, los profesionales de administración de servidores realizan seguimiento diario a posibles fallas ocasionadas por hardware en servidores, rack y ups.	1	2	Bajo

IDENTIFICACION, MITIGACION Y CALIFICACION DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION				
Riesgos	**Mitigación**	**Probabilidad**	**Impacto**	**Zona Riesgo**
No existan copias de seguridad sistemas de información	La ESE Hospital San Lucas de El Molino cuenta con respaldo de la información de los servidores que se encuentran en el servidor. Dicho respaldo se realiza todos los días en servidores y discos duros externos.	1	2	Bajo

Falta de planeación e inversión de recursos para infraestructura tecnológica.	La ESE Hospital San Lucas de E Molino no cuenta con el grupo de trabajo de arquitectura empresarial que evalúa impactos de decisiones de inversión que sobre la materia de arquitectura TIC, sistemas de información e infraestructura tecnológica adelantan todas las Dependencias de la Entidad.	2	3	Moderado
Atraso en Adquisición, actualización y mantenimiento de la Infraestructura tecnológica y nuevas tecnologías.	La ESE Hospital San Lucas de E Molino da prioridad en el resguardo de la seguridad de la información, por ta motivo se intenta contar como primer lugar con todos los proveedores y personal capacitado en TI, decisiones que se verán reflejadas en los planes de compra anuales.	1	3	Moderado
Equivocaciones humanas	La ESE Hospital San Lucas de E Molino bajo la coordinación de la oficina de personal, implementa el plan anual de capacitaciones, que contrarresta debilidades y desarrolla conocimientos relativos al servicio que presta cada funcionario.	1	3	Moderado
Equipos de red (switch) conectados a puntos de red a la vista de funcionarios y de fácil acceso.	La ESE Hospital San Lucas de E Molino se encuentra en etapa de transición para la adopción de Protocolo IPV6, para la cual realizará la 1ra fase de diagnóstico.	2	2	Bajo

Tabla 4: Identificación, mitigación y calificación de riesgos de seguridad y privacidad de la información

7. RESPONSABLES

- Gerente
- Líderes del Proceso (Jefes de Área y Coordinadores de Equipos)
- Profesional Tecnología

8. METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en la ESE Hospital San Lucas de El Molino, 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.

De acuerdo con esto, se definen las siguientes fases de implementación del MSPI:

- Diagnosticar
- Planear
- Hacer
- Verificar
- Actuar

Ilustración 1 – Marco de Seguridad y Privacidad de la Información

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

9. ACTIVIDADES

- Realizar Diagnóstico
- Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad Digital
- Realizar la Identificación de los Riesgos con los líderes del Proceso.
- Entrevistar con los líderes del Proceso

- Valoración del riesgo y del riesgo residual
- Realizar Mapas de calor donde se ubican los riesgos
- Plantear al plan de tratamiento de riego aprobado por los lideres

10. 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 de acuerdo a lo establecido por la ESE Hospital San Lucas de El Molino.

- 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.

11. SEGUIMIENTO Y EVALUACIÓN

Al finalizar cada etapa se realizará una reunión con la Gerente, Jefa de la Oficina de Recursos Humanos, Jefa del área de Almacén y el Asesor de Seguridad y Privacidad de la información presentar el informe del avance del proyecto y de esta manera evaluar todos los pasos se han ido realizado.

12. ENTREGABLES

- Informe de avance o resumen ejecutivo
- Acta de Reunión.
- Plan de tratamiento de riego aprobado por los lideres
- Política de Seguridad
- Productos de cada etapa

(Original Firmado)

YURIZAN YOHANA BARLIZA GOMEZ
Gerente