E.S.E. Hospital
San Vicente de Paúl
Paipa nos mueve
Un Hospital que construimos todos

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

2025

Fecha del cambio	Descripción del cambio	Justificación	Versión
12-01-2025	Elaboración del documento		01

INTRODUCCION

Este plan define el análisis, evaluación y tratamiento de los riesgos de seguridad y privacidad de la información, tomando como base la Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública (DAFP) y la "Guía de Gestión de Riesgos" del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), realizando la identificación, análisis, valoración, tratamiento de los riesgos e identificación de las vulnerabilidades y amenazas asociadas a los riesgos conforme a la norma ISO/IEC 27005:2011 Tecnologías de la información - Técnicas de Seguridad - Administración de riesgos de Seguridad de la Información.

La E.S.E Hospital San Vicente de Paul de Paipa, es una entidad descentralizada proveedora de información tanto magnética como física, la cual se encuentra en continuo procesamiento para el reporte de diferentes informes tanto internos como externos, hecho que implica riesgo en la perdida de la misma, lo que podría traer problemas económicos, legales y/o administrativos por lo cual, este documento busca establecer una línea de trabajo que permita a la entidad sortear los riesgos a la cual está expuesta y lograr que su información este segura.

Por lo anterior es fundamental que la E.S.E elabore y adopte el plan de tratamiento de riesgos de seguridad y privacidad de la información en cumplimiento al decreto 612 de 2018, como medio o herramienta para el logro de los objetivos de mantener la información de la Entidad de forma confidencial, integra y disponible.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

1. OBJETIVO

Elaborar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la E.S.E Hospital San Vicente de Paul de Paipa, como herramienta que proporcione las pautas necesarias para desarrollar y fortalecer una adecuada gestión de los riesgos de seguridad de la información.

1.1 Objetivos Específicos

- Diagnosticar la situación actual de la institución en materia de riesgos de seguridad y privacidad de la Información.
- Gestionar los riesgos de seguridad y privacidad de la información. para el control, minimización y protección contra el riesgo de pérdida y/o privacidad de la información de la E.S.E Hospital San Vicente de Paul de Paipa.
- Mejorar el sistema de Seguridad y Privacidad de la Información, con el fin de que las partes interesadas tengan mayor confianza en el tratamiento de la información que se almacena y maneja en la Entidad; de tal forma que la prestación de servicios integrales de salud sea satisfactoria para nuestros usuarios con calidad técnica, científica humana y oportuna.
- Proteger los activos informáticos mediante la implementación de acciones de mitigación frente al riesgo.
- Aportar avances al modelo integrado de planeación y gestión en sus políticas de gobierno digital, seguridad digital, transparencia, acceso a la información pública y lucha contra la corrupción entre otras.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

2. ALCANCE

El plan de Riesgos de Seguridad y Privacidad de la Información de la E.S.E. Hospital San Vicente de Paul de Paipa, aplica a todos los procesos que manejen, procesen o interactúen con información física y magnética.

3. RESPONSABLES

Gerente
Líderes de Proceso
Gestión de la Información y comunicación

4. SOPORTE LEGAL

Ley 57 (05 de julio de 1985): "Por la cual se ordena la publicidad de los actos y documentos oficiales."

Ley 527 (18 de agosto de 1999): 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, y Se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 962 (08 de julio de 2005): "Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos."

Ley 1266 (31 de diciembre de 2008): "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, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones."

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

Ley Estatutaria 1581 (17 de octubre de 2012): "Por la cual se dictan disposiciones generales para la protección de datos personales."

Ley 1712 (06 de marzo de 2014: Ley de Transparencia y acceso a la información pública nacional.

Decreto Ley 2150 de (05 de diciembre de 1995): "Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública."

Decreto 1747 (11 de septiembre de 2000): "Por el cual se reglamenta parcialmente la ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales"

Decreto 019 de 2012: "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública".

Decreto 2364 (22 de noviembre de 2012): Firma electrónica.

Decreto 1078 (26 de mayo de 2015): "Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones."

Resolución 3564 de 2015 (31 de diciembre de 2015): Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.

5. DEFINICIONES

Para la adecuada gestión del presente plan, se debe manejar con propiedad los siguientes términos:

Acciones asociadas: son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

Activo de información: Todo aquel elemento de información, recibido, gestionado o producido, que posee valor para la entidad y, por lo tanto, debe protegerse para el logro de la misión. Serán activos de información críticos aquellos que son imprescindibles o su valor es clave para la operación de la entidad. Cuando se trate de activos informáticos, se entenderán como aquellos dispositivos tecnológicos que permiten la emisión, transmisión, procesamiento y recepción de información.

Amenaza: situación externa que no controla la entidad y que puede afectar su operación.

Análisis del riesgo: etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).

Asumir el riesgo: opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.

Causa: Es todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Calificación del riesgo: Estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

Cibernético. Ciencia que estudia las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas.

Compartir o transferir el riesgo: Opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. (ISO/IEC 27001).

Contexto estratégico: son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. (ISO/IEC 27001).

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.

Infraestructura: Conjunto de activos o recursos técnicos, servicios o instalaciones que se consideran necesarios para el desarrollo normal de procesos o actividades.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos. (ISO/IEC 27001).

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorías de los sistemas integrados de gestión.

Plan de contingencia: Conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio.

Privacidad: 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, que genera la obligación de proteger dicha información en observancia del marco legal vigente.

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).

Riesgo residual: Es un nivel de riesgo que permanece, luego de determinar y aplicar controles para su administración.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

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

Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

T.I. Tecnología de la Información: Generalmente se conoce así al área o dependencia que administra la tecnología en una entidad. Para el presente documento, OTI o TI hacen referencia a la Oficina de Tecnología de la Información del AGN.

Valoración del riesgo: Establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización.

Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información.

6. DESARROLLO

Para el desarrollo del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la E.S.E. Hospital San Vicente de Paul de Paipa, se tomaron como referencia las Guías No 7 Gestión de riesgos y la No. 8 Controles de seguridad de la información del Ministerio de Tecnologías de la Información y las comunicaciones – MINTIC.

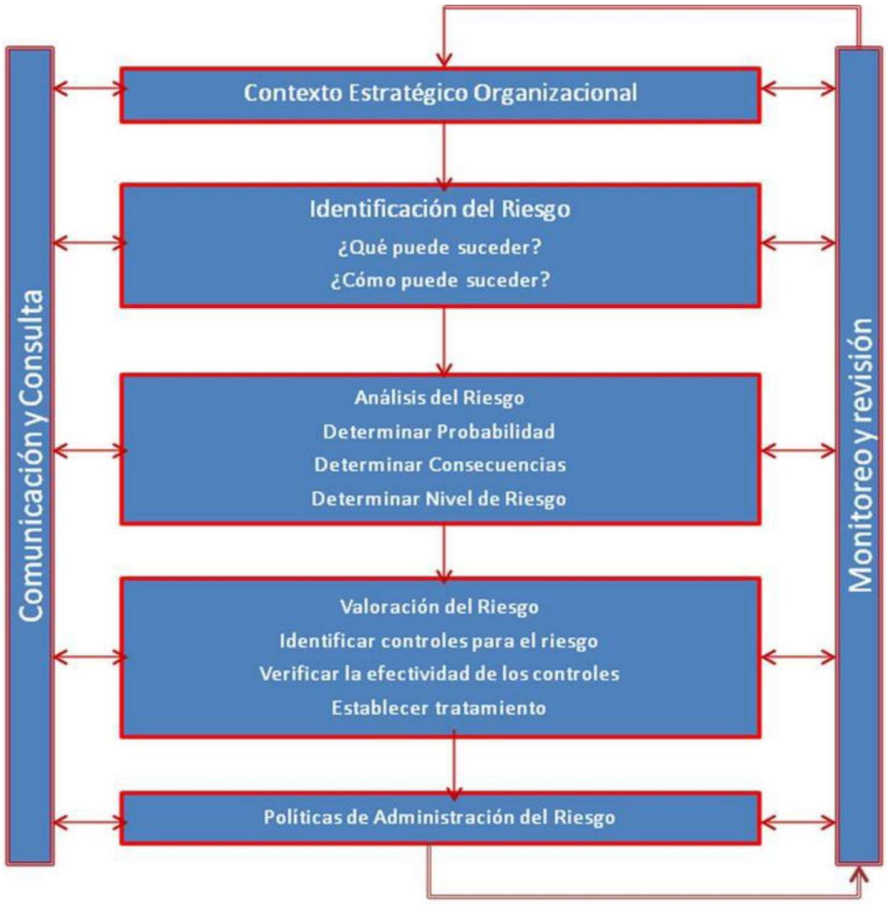
6.1 VISION GENERAL PARA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

El proceso de gestión de riesgo en la seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento.

Proceso para la administración del riesgo:

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

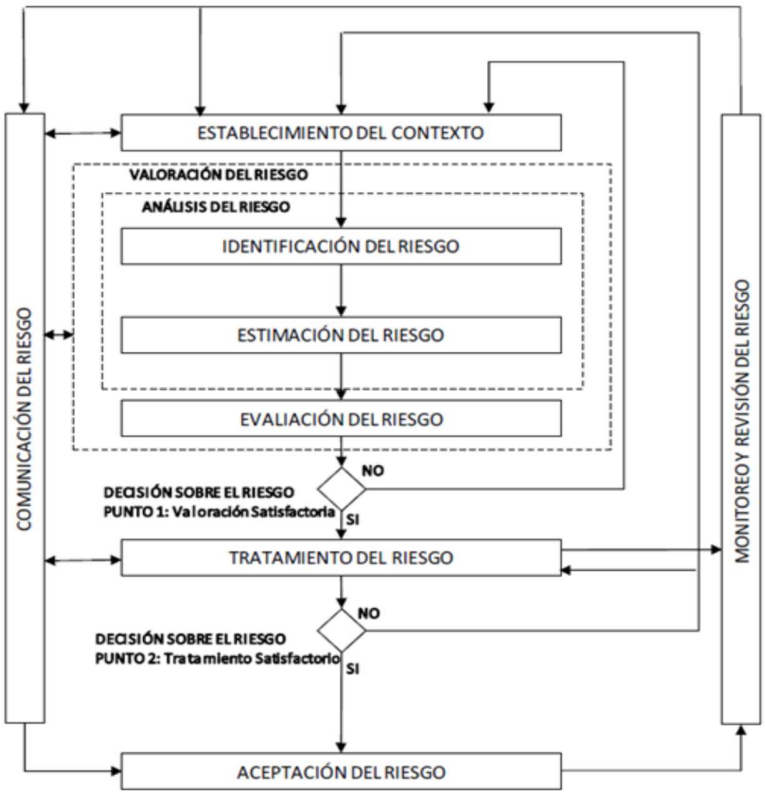
Imágen1. Proceso para la Administración del Riesgo.



Fuente: Guía para Administración de Riesgo DAFP 2018.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

Imágen2. Proceso para la Administración del Riesgo.



Fuente: Guía para Administración de Riesgo DAFP 2018.

De acuerdo a la imagen 2, el proceso de gestión del riesgo en la seguridad de la información, puede ser iterativo para las actividades de valoración del riesgo y/o el tratamiento de este. Un enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración.

El contexto se establece como primera medida, luego se realiza la valoración del riesgo y si se cuenta con la información suficiente para determinar de manera eficaz las acciones que se necesitan para modificar los riesgos a un nivel aceptable, entonces la labor está determinada y sigue el tratamiento del riesgo. Si la

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

información no es suficiente, se llevará a cabo otra iteración de la valoración del riesgo con un contexto revisado.

6.2 IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

Según la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección**.**

Los activos de información se clasifican en dos tipos:

a. Primarios:

Procesos o subprocesos y actividades de la entidad: procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización.

- información del área de facturación.
- Información de historias clínicas

Información: información que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados; información de alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo.

- Información del área de tesorería, presupuesto y contabilidad.
- Información del área de contratación.
- Información de talento humano.
- Inventarios del área de farmacia.
- Inventarios área de almacén.

Actividades y procesos de negocio: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

- Información del área de tesorería.
- Información del área de contratación.
- Información de procesos jurídicos de la entidad.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

b. De Soporte

Hardware: Consta de todos los elementos físicos que dan soporte a los procesos y los colaboradores en el desarrollo de sus tareas diarias.

- Computadores.
- Servidor.
- Impresoras.
- Historias clínicas de usuarios de la E.S.E Hospital San Vicente de Paul de Paipa
- Contratos y documentos de legalización y pago.

Software: Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos y enmarcan la información recolectada de los colaboradores, usuarios y sus familias.

Redes: Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores y/o teléfonos físicamente o los elementos de un sistema de información (cableado, puntos de acceso, etc.).

Personal: Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, colaboradores, responsables, etc.).

- Personal a cargo de elementos de cómputo de la institución.

6.3 IDENTIFICACIÓN DE RIESGO

El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida.

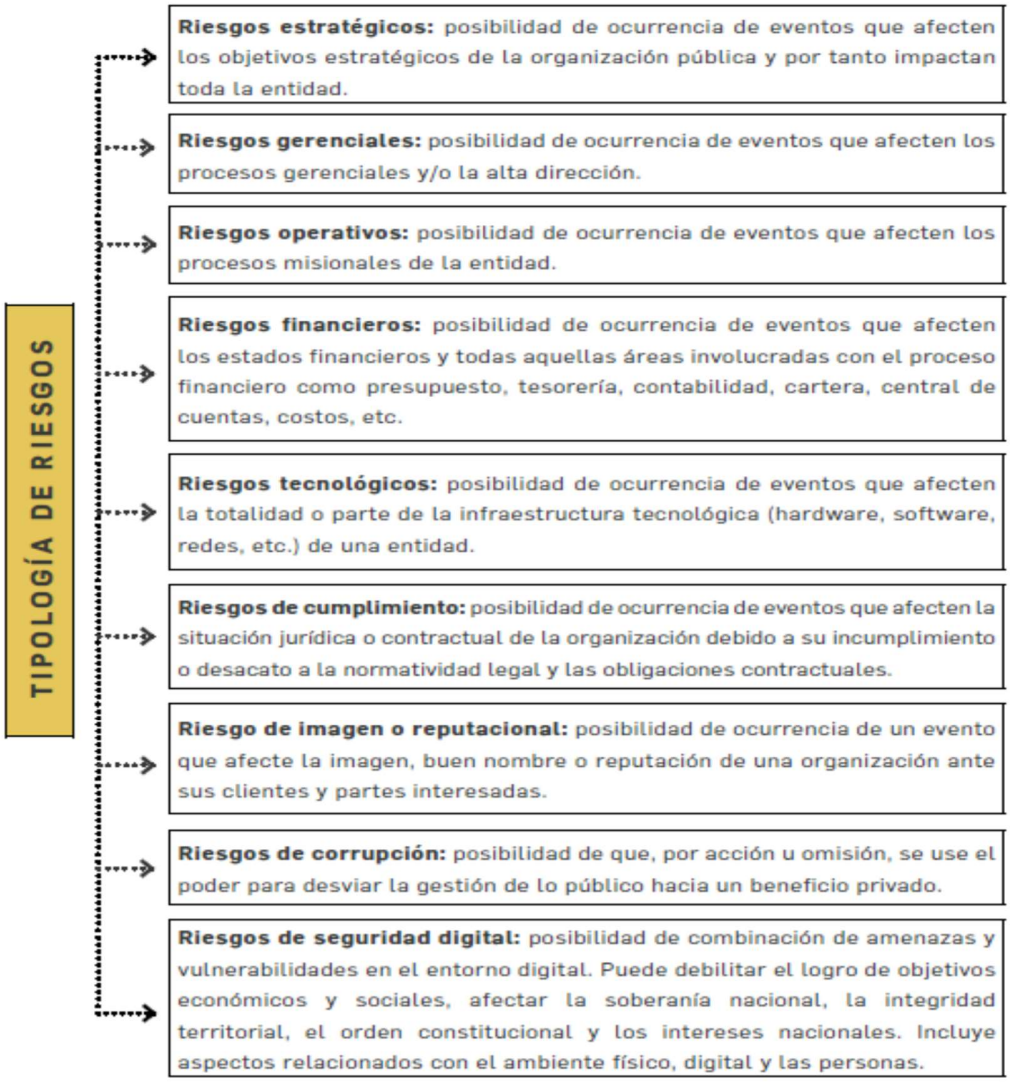
a. Tipología de riesgo:

La identificación de amenazas que posiblemente causen daños a la información con que cuenta la E.S.E Hospital San Vicente de Paul de Paipa, se realiza a partir de herramientas importantes como lo son la Inspección física.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

Se identifican los tipos de riesgo y la magnitud con la que pueden afectar a la seguridad y privacidad de la información. Entre los principales tipos de riesgo tenemos:

Imagen 3. Tipología de Riesgos



Fuente: Guía para Administración de Riesgo DAFP 2018.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

b. Descripción de Causas.

La causa es el fundamento, motivo, origen y principio de algo; con respecto al riesgo estas pueden ser generadas por personas, procesos, equipos, tiempo, entre otras que provocan un mal uso, una inadecuada acción o mal trabajo como origen de un hecho ya sea positivo o negativo.

c. Consecuencias:

Son los efectos asociados a la materialización del riesgo, estos pueden ser de diferente índole de acuerdo a la acción realizada y al perjuicio que se presente después de lo acontecido.

6.4 ANÁLISIS DEL RIESGO

Para ello se utilizará una escala cuantitativa de valoración donde uno (1) es el valor más bajo y cinco (5) más alto, ello con el fin proyectar una comparación y priorización del riesgo de la información tanto en su seguridad como en la privacidad.

a. Probabilidad

Es la posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos.

CONCEPTO	DESCRIPCION	FRECUENCIA	VALOR
Raro	El evento puede ocurrir sólo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años	1
Improbable	Es muy poco factible que el evento se presente.	Al menos 1 vez en los últimos 5 años.	2
Posible	El evento podría ocurrir en algún momento.	Al menos 1 vez en Los últimos 2 años.	3
Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias,	Al menos 1 vez en el último año.	4
Casi-certeza	Se espera que ocurra en la mayoría de las circunstancias	Más de 1 vez al año.	5

Fuente: Guía para administración de riesgo DAFP 2018

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

b. Impacto

Es el conjunto de consecuencias que origina la materialización de un riesgo, es decir, la afectación que este causaría en la institución, puede ser económicas, legales, reputacionales entre otras.

Escala para calificar el impacto del riesgo							
Tipos de efecto o impacto		a) Estratégico	b) Operativo	c) Financieros	d) Cumplimiento	e) Tecnología	f) Imagen
INSIGNIFICANTE	El acontecimiento puede ser controlado y las consecuencias son mínimas.	Afecta el cumplimiento de algunas actividades	Genera ajustes a una actividad concreta	La pérdida no afecta la operación normal de la ESE.	Genera un requerimiento	Afecta a una persona o una actividad del proceso	Afecta a un grupo de servidores del proceso
MENOR	Tiene un bajo impacto, no afectando al proceso de información de la entidad.	Afecta el cumplimiento de las metas del proceso	Genera ajustes en los procedimientos	La pérdida afecta algunos servicios administrativos de la ESE.	Genera investigaciones disciplinarias, fiscales y/o penales	Afecta el proceso	Afecta a los servidores del proceso
MODERADO	Si el hecho llega a presentarse tendría medianas consecuencias o efectos sobre la entidad	Afecta el cumplimiento de las metas de un grupo de procesos	Genera ajustes o cambios en los procesos	La pérdida afecta considerablemente e e la prestación delservicio	Genera interrupciones en la prestación del servicio	Afecta varios procesos de la ESE.	Afecta a todos los servidores de la ESE.
MAYOR	El impacto sería significativo y tendría altas consecuencias y/o efectos sobre la entidad.	Afecta el cumplimiento de las metas de la ESE.	Genera intermitencia en el servicio	La pérdida afecta considerablemente e e el presupuestode la ESE.	Genera sanciones	Afecta a toda la entidad	Afecta el sector
CATASTRÓFICO	La materialización del riesgo imposibilita el cumplimiento de los objetivos de la Agencia, tiene un impacto y las consecuencias serían catastróficas.	Afecta el cumplimiento de las metas del sector y del gobierno	Genera paro total de la ESE.	Afecta al presupuesto de otras entidades o a de la del departamento	Genera cierre definitivo de la ESE.	Afecta al Departamento	Afecta al Departamento Gobierno, Todos los usuarios de la ESE.

Fuente: Guía para administración de riesgo DAFP 2018

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

6.5 ETAPAS PARA LA ADMINISTRACION DEL RIESGO

A continuación, se presentan las etapas a desarrollar durante la administración del riesgo.

1. **Contexto para la gestión del riesgo:** Determinar los factores que afectan el riesgo.
2. **Identificación de Riesgos:** Identificar las causas, riesgo, consecuencias y clasificación del riesgo.
3. **Análisis:** Calificación y evaluación del riesgo.
4. **Valoración:** Identificación y evaluación de controles.
5. **Manejo:** Determinar, las acciones para el fortalecimiento de los controles.
6. **Seguimiento:** Evaluación integral de los riesgos.

1. Contexto para la gestión del riesgo

Definir el contexto para la gestión del riesgo marca la ruta que la E.S.E Hospital San Vicente de Paul, debe asumir frente a la exposición del riesgo, ya que permite conocer las situaciones que pueden afectar el cumplimiento de los objetivos de seguridad y privacidad de la información desde la estructura organizacional, los recursos físicos y tecnológicos entre otros.

Esta etapa se centra en determinar las amenazas y debilidades de la E.S.E Hospital San Vicente de Paul de Paipa, es la base para la identificación del riesgo, dado que su análisis suministrará la información sobre las CAUSAS del riesgo.

2. Identificación de Riesgos

El propósito de esta etapa permite conocer los potenciales eventos, estén o no bajo el control de la E.S.E San Vicente de Paul de Paipa, los cuales ponen en riesgo el logro de su misión, estableciendo las causas y los efectos que lo generan.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

Adicionalmente, en esta etapa también se realiza la clasificación del riesgo

Causas		Riesgos		Consecuencia		Clasificación		Identificación
Son los medios o circunstancias	+	Evento que tendrá un impacto	+	Efecto que se puede presentar	+	De acuerdo a las características	=	Identificación del Riesgo
Descripción a adecuada de los Riesgos								Resultado esperado

Se identifican los riesgos institucionales. Una vez se dispone de un listado de riesgos reales que pueden afectar a la institución, se puede realizar la evaluación del impacto que puede sufrir la E.S. E Hospital San Vicente de Paul de Paipa en caso de que se materialicen.

Como resultado de esta fase se obtiene:

- Un análisis detallado de los activos relevantes de seguridad de la empresa.
- Un estudio de las posibles amenazas sobre los sistemas de información, así como su impacto.

3. **Análisis:** Calificación y evaluación del riesgo.

El análisis del riesgo busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo.

Se realiza la identificación de causas, vulnerabilidades, amenazas (identificación, descripción, tipo), consecuencias y se determina la clase de riesgo(probabilidad e impacto), todo esto asociado a aquellos eventos o situaciones que afecten los activos de información que pueden dificultar el normal desarrollo de las actividades diarias.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

Identificación de las amenazas

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo (ej. Acciones no autorizadas, daño físico, fallas técnicas).

Algunas amenazas pueden afectar a más de un activo y en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.
A continuación, se describen una serie de amenazas comunes:
D = Deliberadas, A = Accidentales, E = Ambientales

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

TIPO	AMENAZA	ORIGEN
DAÑO FISICO	Fuego	A,D,E
	Agua	A,D,E
	Contaminación	A,D,E
	Accidente Importante	A,D,E
	Destrucción del equipo o medios	A,D,E
	Polvo, corrosión, congelamiento	A,D,E
EVENTOS NATURALES	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos meteorológicos	E
	Inundación	E
PERDIDA DE LOS SERVICIOS ESENCIALES	Fallas en el sistema de suministro de agua	E
	Perdida de suministros de energía	E
	Falla en el equipo de telecomunicaciones	A,D,E
COMPROMISO DE LA INFORMACION	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipos	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D
	Datos provenientes de fuestes no confiables	A,D
	Manipulación con hardware	D
	Manipulación con software	D
FALLAS TECNICAS	Fallas del equipo	A,D
	Mal funcionamiento del equipo	A,D
	Saturación del sistema de información	A,D
	Mal funcionamiento del software	A,D
	Falta de mantenimiento del sistema de información	A,D,E
ACCIONES NO AUTORIZADAS	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
COMPROMISO DE LAS FUNCIONES	Error en el uso	A,D
	Abuso de derechos	A,D
	Falsificación de derechos	A,D

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

Es recomendable tener particular atención a las fuentes de amenazas humanas, tales como Piratería, Ingeniería Social, Intrusión, accesos forzados al sistema, acceso no autorizado, suplantación de identidad, empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos

Descripción de vulnerabilidades

- **HARDWARE:**

Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento.
Incumplimiento en el mantenimiento del sistema de información.
Ausencia de esquemas de reemplazo periódico
Susceptibilidad a la humedad, el polvo y la suciedad
Ausencia de un eficiente control de cambios en la configuración. Error en el uso.
Susceptibilidad a las variaciones de voltaje. Variaciones en el suministro de energía.
Falta de cuidado en la disposición final. Hurtos medios o documentos.

- **SOFTWARE**

Defectos bien conocidos en el software
Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo
Disposición o reutilización de los medios de almacenamiento sin borrado adecuado
Asignación errada de los derechos de acceso
Configuración incorrecta de parámetros
Fechas incorrectas
Ausencia de mecanismos de identificación y autentificación de usuario
Contraseñas sin protección
Gestión deficiente de las contraseñas
Habilitación de servicios innecesarios

- **RED**

Ausencia de pruebas de envío o recepción de mensajes
Líneas de comunicación sin protección
Tráfico sensible sin protección
Conexión deficiente de los cables

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

Fallas del equipo de telecomunicaciones
Ausencia de identificación y autentificación de emisor y receptor
Arquitectura insegura de la red
Transferencia de contraseñas en claro
Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)
Conexiones de red pública sin protección

- **PERSONAL**

Ausencia del personal
Incumplimiento en la disponibilidad del personal
Procedimientos inadecuados de contratación
Destrucción de equipos y medios
Entrenamiento insuficiente en seguridad. Error en el uso
Uso incorrecto de software y hardware
Falta de conciencia acerca de la seguridad
Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería.

- **LUGAR**

Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos
Red energética inestable
Ausencia de protección física de la edificación (Puertas y ventanas)

- **ORGANIZACIÓN**

Ausencia de procedimiento formal para el registro y retiro de usuarios
Ausencia de proceso formal para la revisión de los derechos de acceso
Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)
Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información
Ausencia de auditorias
Ausencia de procedimientos de identificación y valoración de riesgos

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

Ausencia de reportes de fallas en los registros de administradores y operadores
Respuesta inadecuada de mantenimiento del servicio
Incumplimiento en el mantenimiento del sistema de información
Ausencia de acuerdos de nivel de servicio o insuficiencia de estos
Los documentos físicos que se manejan en la entidad no se han digitalizado por lo tanto están expuestos a perdidas y daños físicos debido a que los sitios de almacenamiento en las oficinas no son los adecuados.
Además, se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados teniendo en cuenta la probabilidad e impacto.

La etapa de análisis de los riesgos se divide en:

- **Calificación del riesgo**

Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo. La primera representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse, y la segunda se refiere a la magnitud de sus efectos. Para la determinación de la calificación del riesgo, con base en la probabilidad y el impacto se debe tener en cuenta las siguientes tablas

Escala para calificar la probabilidad del riesgo		
Nivel	**Concepto**	**Frecuencia**
Raro	Imposible que ocurra (Lleva más de 5 años sin ocurrir)	No ha ocurrido en los últimos cinco años.
Improbable	El evento puede ocurrir en algún momento.	Al menos de 1 vez en losúltimos 5 años.
Ocasional	El evento podría ocurrir en algún momento.	Al menos de 1 vez en losúltimos 2 años.
Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en elúltimo año.
Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

Fuente: Fuente: Guía para Administración de Riesgos DAFP, 2018

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

- **Evaluación del riesgo:**

Permite una comparación entre los riesgos que se presenta en la institución con el fin de discernir cuan peligrosos pueden ser, de tal forma que se tomen medidas para mitigar sus consecuencias.

PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Raro	B	B	B	M	M
Improbable	B	M	M	A	A
Ocasional	B	M	A	A	E
Probable	M	A	A	E	E
Casi Seguro	M	A	E	E	E

Color	Zona de riesgo
B	Zona de riesgo baja
M	Zona de riesgo moderada
A	Zona de riesgo alta
E	Zona de riesgo extrema

Fuente: Guía Gestión de Riesgos DAFP, 2018

4. **Valoración del Riesgo.** Identificación y evaluación de controles.

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos. La valoración del riesgo se realiza en tres momentos:

- **Identificación de los controles:** Los controles son las acciones orientadas a minimizar la probabilidad de ocurrencia o el impacto del riesgo; estos, deben estar relacionados con las causas o las consecuencias identificadas para el riesgo y eliminarlas o mitigarlas. La administración del riesgo contribuirá a la gestión de la entidad, en la medida en que los controles se identifiquen, documenten, apliquen y sean efectivos para prevenir o mitigar los riesgos.

- **Evaluación de Controles:** Permite determinar en qué medida los controles identificados están aportando para disminuir los niveles de probabilidad e impacto del riesgo.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

- **Riesgo residual y definición de opciones de Manejo:** Previo a la definición del riesgo residual se debe determinar qué escala (probabilidad, impacto o ambas) se afecta positivamente con la aplicación del control teniendo en cuenta las siguientes indicaciones:

5. **Manejo de riesgos.** Determinar, las acciones para el fortalecimiento de los controles.

Una vez determinada la zona en donde se encuentra ubicado el riesgo y, dependiendo de las opciones de manejo, se deben formular las acciones orientadas al mejoramiento y fortalecimiento de los controles identificados. Las acciones que se definan para el manejo del riesgo se deben contemplar bajo dos aspectos:

- Corregir las fallas identificadas en los controles según la evaluación realizada a cada uno.
- Reforzar o fortalecer los controles existentes.

Acción a Desarrollar	+	Definición de responsables	+	Definición de Plazo	=	Definición Adecuadade Acciones
Resolución adecuada de los Riesgos						Resultado esperado

Si la evaluación del riesgo residual, lo ubica en la zona baja no es necesario formular acciones de manejo, el manejo estará únicamente enfocado en garantizar que los controles previamente establecidos operan de manera adecuada. Los riesgos ubicados en las zonas moderada, alta o extrema, exigen realizar acciones que fortalezcan los puntos débiles identificados en la evaluación de los controles

6. **Seguimiento:** Evaluación integral de los riesgos.

Es necesario realizar seguimiento a la efectividad de los controles y cumplimiento de las acciones formuladas que contribuyen a la mitigación de los riesgos.

Este ejercicio permite hacer una comparación entre los riesgos que se presentan en la institución con el fin de establecer cuan peligrosos pueden ser, de tal forma que se tomen medidas para mitigar sus consecuencias.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

Responsable

Es la persona encargada y responsable de tomar medidas para dar solución a las circunstancias presentadas ya sea en mediano, corto o largo plazo, con el fin de remitir respuesta y dar solución a los eventos presentados.

La calificación y evaluación de los riesgos del sistema de seguridad de la información la realiza el dueño del proceso, con la supervisión de cumplimiento por parte de Control Interno.

Los resultados de la evaluación y las observaciones de Control Interno serán presentados a la Gerencia, en el momento que lo considere pertinente, para que se tomen las decisiones necesarias que garanticen la sostenibilidad de la Administración de estos riesgos.

6.6 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACION

La E.S.E. Hospital San Vicente de Paul de Paipa en su mapa de riesgos define los riesgos tecnológicos y de seguridad digital, los cuales serán el objeto de tratamiento para mantener la integridad y confidencialidad de la información.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

Mapa de Riesgos de Seguridad de la Información.

IDENTIFICACION DEL RIESGO						ANALISIS DEL RIESGO INHERENTE						
N°	Descripción del Riesgo	Causa inmediata	Causa Raiz	Clasificación del Riesgo	Tipo de Riesgo	Probabilidad	%	Criterios de impacto	Impacto	%	% Zona de riesgo	Zona de riesgo
1	Posibilidad de vulnerabilidades de los sistemas de información por daño a los servidores de la entidad debido al descuido o desconocimiento por parte de los usuarios en lo referente a la seguridad informática.		Desconocimiento parte de los usuarios de las políticas sobre seguridad informática		OPERATIVO	POSIBLE	60	Un daño cibernético de los servidores de la institución causaría un impacto mayor a la operación de la entidad en la medida que podría generar perdidas de información y afectar las vulnerabilidades.	MAYOR	80	70	ALTO
2	Posibilidad de pérdida de la Disponibilidad, confidencialidad e integridad de la Información por tener software obsoleto debido a que no está actualizado y que no tenga soporte técnico de parte del proveedor de servicios informáticos.		No tener software actualizado que garantice un soporte adecuado de parte del proveedor de servicios informáticos.		SEGURIDAD DIGITAL	IMPROBABLE	40	Perder disponibilidad, confidencialidad e integridad de la información tiene consecuencias de perdida reputacional de la entidad y genera desconfianza en cuanto a la seguridad de los datos de los usuarios de los sistemas de la entidad.	MODERADO	60	50	MODERADO
3	Pérdida de los activos de información por no tener controles debido a un deficiente uso de los sistemas de información, bases de datos y aplicativos de la entidad		No disponer de políticas, procedimientos y controles de fuga de información en los sistemas de información, bases de datos y aplicativos		SEGURIDAD DIGITAL	PROBABLE	80	Fuga de información de la entidad puede tener impacto en Daño de la marca o del buen nombre de la Entidad o interrupción de la continuidad del negocio	MAYOR	80	80	ALTO

Fuente: Riesgos E.S.E. Hospital San Vicente de Paul de Paipa

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

6.7 ELABORACION DEL PLAN

Se establecen las medidas que se deben adoptar, labores, recursos y actuaciones para reducir los daños que se puedan producir.

IDENTIFICACION DEL RIESGO						ANALISIS		TRATAMIENTO		
RIESGO	PROCESO	DESCRIPCION	EVENTO ADVERSO	CAUSA	CONSECUENCIA	PROBABILIDAD	IMPACTO	EVALUACION	ACCION	RESPONSABLE
RIESGO TECNICO	GESTION INFORMATICA	Revisión e instalación de equipos de computo	Instalación de cableria en mal estado	Deterioro de cables por constante uso	Deficiente funcionalidad de equipos	3	3	M	Mantenimiento frecuente a equipos de cómputo e instalación eléctrica	Subgerente Líder de Almacen
		Copias de seguridad efectivas	Disco duro no apto para realizar copias de seguridad confiables	No realización de copias de seguridad, sin efectividad total	Pérdida económica	3	4	A	Adquisición de equipo Corporativo con capacidad de	Subgerente Líder Gestión de la información
		Equipos de computo aptos para el funcionamiento	Daño de equipos y pérdida de la información	Equipos de cómputo con baja capacidad para almacenamiento de información y capacidad de encendido permanente	Pérdida económica	3	4	A	Adquisición de equipos corporativos tipo servidor de alta funcionalidad.	Gerencia
RIESGO OPERATIVO	GESTION CLINICA	Diligenciamiento de historias clínicas	historias clínicas incompletas	Falta de datos personales de pacientes en historias clínicas	Archivo histórico clínico incompleto	5	3	M	Auditoria de histórias clínicas; capacitación a personal médico para correcto diligenciamiento de historias clínicas	Líderes Misionales
		Procesos de custodia de documentos de archivo de gestión, central e historico e Historia clínica físicaDeterioro	Deterioro de documentos	Material de baja resistencia	Pérdida de información	2	2	B	Digitalizar archivos	Lider de Archivo

6.8 INTERPRETACION DEL PLAN

El resultado de esta fase se concreta en un plan de tratamiento de riesgos, que nos permite definir como la información generada por la E.S.E Hospital San Vicente de Paul de Paipa, se encuentra expuesta a eventos adversos especialmente provocados por prácticas inadecuadas del personal de la entidad y falta de dotación

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

de equipos idóneos para cumplirlas, hecho que ponen en riesgo el cumplimiento de la misión encaminada a satisfacer las necesidades y expectativas de sus clientes bajo los principios de responsabilidad, rentabilidad económica y social, por tanto es conveniente que las partes responsables, encaminen medidas para solventar la problemática presentada y disminuir la exposición al riesgo en al que la información se ve expuesta, con medidas correctivas, preventivas y de mejora.

En cuanto a la privacidad de la información la E.S.E Hospital San Vicente de Paul de Paipa cumple este requisito protegiendo sus datos, dando acceso únicamente a personal autorizado.

6.9 DESARROLLO DEL PLAN

Se establecen las actividades de acuerdo con el enfoque en Riesgos, realizando el respectivo cruce entre lo establecido en el Modelo de Seguridad y Privacidad de la Información, la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, la matriz de autodiagnóstico del Modelo Integrado de Planeación y Gestión – MIPG del Departamento de la Función Pública – DAFP y las buenas prácticas aplicables. De igual manera se tiene en cuenta los siguientes recursos disponibles:

Humanos:

- Equipo Gestión de la Información: Infraestructura tecnológica y redes.
- Líderes de los procesos

Técnicos:

- Guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital del DAFP
- Matriz de riesgos Sistema de Gestión de Seguridad de la Información - SGSI

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

Logísticos:

- Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.

Con base en lo anterior, se cuenta con recursos para plasmar acciones de mejora que permitan enfocar a la entidad hacia la meta establecida, considerando actividades concretas, medibles y alcanzables, que admitan la mejora continua.

Además, se desarrollan actividades en cuanto a:

PLAN DE SEGURIDAD

- Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias de las oficinas.
- Establecer políticas de seguridad y privacidad de la información como también las políticas de seguridad informática.
- Implementar y socializar las políticas de seguridad y privacidad de la información con el personal de la E.S.E Hospital San Vicente de Paul de Paipa.

PLAN DE CONTINUIDAD

- Socializar con los colaboradores de la E.S.E Hospital San Vicente de Paul de Paipa la importancia del Plan de contingencia, para hacer frente a incidentes graves de seguridad de forma clara y sencilla de cada una de las actividades a desarrollar dentro del plan.
- Diseñar estrategias para el proceso de recuperación teniendo en cuenta los tiempos de reacción e implementación de contingencias ante la realización de los eventos identificados.
- Adoptar una de las tres posiciones, que permita minimizar la ocurrencia o los efectos colaterales sobre la red, esto de acuerdo con los siguientes enfoques:

- Detectar el riesgo
- Plantear controles y efectuar las implementaciones respectivas.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

- Mitigar el riesgo.

IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD PARA LA INFORMACIÓN

El análisis permitió identificar que la E.S.E Hospital San Vicente de Paul de Paipa requiere:

- Resocializar la política de Seguridad de la información, de tal forma que la conozcan todos los colaboradores de la institución.
- Capacitar en temas referentes a Seguridad Informática.
- Implementar Sistemas de respaldo para mantener soporte de la información en caso de eventualidades catastróficas.

PLAN DE CAPACITACIÓN

Elaborar Plan de capacitaciones para el personal encargado de la seguridad de la información, para fortalecer aspectos como:

- Detectar los requerimientos tecnológicos
- Evaluar los resultados de evaluaciones y monitoreo al sistema de seguridad.
- Elaborar un programa de capacitación en temas de ciberseguridad y políticas de seguridad de la información para todos los colaboradores de la E.S.E. Hospital San Vicente de Paul de Paipa.

6.10 CRONOGRAMA DE ACTIVIDADES

Se establece el siguiente cronograma de actividades, detallando en el plan de trabajo las acciones y el plazo de ejecución.

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa.
Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

DESCRIPCION DE ESTRATEGIAS Y ACTIVIDADES
Realizar el mantenimiento preventivo a la totalidad de equipos de comunicación e informática
* Administrar sistemas SIHOS, dar soporte y realizar los ajustes requeridos en el Sistema de Información Hospitalario * Genererar los informes requeridos por las diferentes áreas
Dar soporte en el menor tiempo posible a los usuarios en cuanto a los requeimientos por fallas en los equipos de comunicación e informática
Adquirir el servicio técnico, suministro de repuestos para computadores e impresoras, tintas y toner para las impresoras de la E.S.E HOSPITAL SAN VICENTE DE PAUL DE PAIPA
Realizar el proceo de diagnóstico para evaluar los equipos que requieren actualización o reposición y soliciutd de adquisición.
Realizar el proceso contractual para la adquisición de Antivirus para Servidores y equipos de computo
Realizar el proceso de cambio de equipos en las áreas que se requiere.
Adquirir Hosting, Dominio y capacidad de almacenamiento para el optimo funcionamiento de la página Web
Adquirir servicoos de almacenamiento en la nube para el correcto funcionamiento de los correos electrónicos
Actualizar la página Web de acuerdo a los líneamientos normativos
1. Realizar el proceso contractual de Contratación de la Actualización del Sistema Hospitalario SIHOS
1. Implementar la Actualización de los diferentes procesos del Sistema de Información Hospitalaria 2. Implementar los diferentes Manuales de Usuario, definiendo roles y responsabilidades. 3. Evaluar la efectividad y generar acciones de mejora
1.Realizar el proceso de Actualización del Sistema de información Web Almera para realizar el Seguimiento a los diferentes Planes Institucionales 2. Administrar y mantener consolida la información generada en los diferentes procesos, en el sistema de información Almera.
Realizar el proceso contractual para gestionar y almacenar los laboratorios Clínicos
Realizar cronograma con las fechas de reporte establecidas, por los diferentes entes de control Solicitar la información requerida al área correspondiente con dependiendo de la información a reportar con suficiente tiempo de antelación para posteriormente validarla y enviarla en la plataforma correspondiente de manera exitosa.
1. Contestar las llamadas y realizar la asignación de los servicios de forma efectiva 2. Realizar devolución de llamadas no contestadas 3. Relizar Demanda Inducida
Actualizar e implementar el Proceso de Gestión Documental
Formular POA para la vigencia 2026

Fuente: Elaboración E.S.E. Hospital San Vicente de Paul de Paipa

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa

Elaborado por:	**Cargo:**	**Fecha: 21/01/2025**
Deicy Jimena Gutierrez Perez	Líder Gestión de la Información y Comunicaciones	**Firma:**
Revisado Por:	**Cargo:**	**Fecha: 21/01/2025**
Nelly Nayibe Dallos Lara	Líder Gestión de Calidad	**Firma:**
Aprobado por:	**Cargo:**	**Fecha: 21/01/2025**
Catherine Van Arcken Martínez	Gerente	**Firma:**

Este documento es propiedad de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa. Prohibida su reproducción por cualquier medio, sin previa autorización de la Empresa Social del Estado Hospital San Vicente de Paul de Paipa