PLAN DE TRATAMIENTO DE RIESGOS Y SEGURIDAD DE LA INFORMACIÓN 2026

E.S.E. HOSPITAL
SAN VICENTE DE PAÚL
MISTRATO
comprometidos con la salud

ENERO DE 2026

Cra 5 N° 8-36 - Tel: 3502702807
E-Mail: hospital.mistrato@hsvpmistrato.gov.co
Mistrató Risaralda

Contenido

1. INTRODUCCIÓN

La información es un activo estratégico y fundamental para la E.S.E Hospital San Vicente de Paúl Mistrató, ya que sustenta la toma de decisiones clínicas y administrativas, garantiza la continuidad de los servicios de salud y refleja el mejoramiento institucional logrado mediante planes de calidad y gestión del riesgo. En el contexto de una institución de salud, la información no solo posee valor operativo, sino que está sujeta a estrictos requerimientos éticos, legales y regulatorios, especialmente en lo referente a la confidencialidad, integridad y disponibilidad de los datos de los pacientes.

En el marco de la Política de Tecnologías de la Información y las Comunicaciones (TIC) y bajo los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) de la estrategia de Gobierno en Línea del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, este documento establece los principios, procesos y controles necesarios para proteger los activos de información del Hospital. Estos lineamientos son de obligatorio cumplimiento para todos los colaboradores, contratistas, proveedores y terceros que accedan a los sistemas de información, la red de datos o la infraestructura tecnológica de la institución.

El Sistema de Gestión de Seguridad de la Información (SGSI) del Hospital se fundamenta en la norma internacional ISO/IEC 27001:2013 y en las buenas prácticas del MSPI, con el propósito de preservar los tres atributos esenciales de la información:

- Confidencialidad: garantizar que la información solo sea accesible para aquellas personas o sistemas autorizados.
- Integridad: asegurar que la información sea exacta, completa y no sea modificada de manera no autorizada.
- Disponibilidad: garantizar que la información y los sistemas que la soportan estén accesibles cuando se requieran para la prestación de los servicios de salud.

Estos atributos se aplican a todos los procesos estratégicos, misionales, de apoyo y de evaluación de la institución, y deben ser conocidos, comprendidos y cumplidos por todo el personal, incluyendo servidores públicos, proveedores y terceros que interactúen con los sistemas de información o las instalaciones físicas del Hospital.

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información tiene como finalidad identificar, evaluar y tratar los riesgos que puedan afectar los activos informativos del Hospital, con el fin de prevenir su materialización, mitigar su impacto y asegurar la continuidad de las operaciones asistenciales y administrativas. Este plan se enmarca dentro del ciclo de mejora continua PHVA (Planificar, Hacer, Verificar,

Actuar), iniciando con un diagnóstico de riesgos en todas las áreas, su medición mediante indicadores de control y la implementación de planes de mejora cuando sea necesario.

La Alta Dirección del Hospital asume su compromiso con la implementación, mantenimiento y mejora continua del SGSI y del MSPI, proporcionando los recursos necesarios y promoviendo una cultura de seguridad de la información entre todos los colaboradores. Asimismo, se reserva el derecho de aplicar medidas disciplinarias, en el marco legal vigente, en caso de incumplimiento de las políticas de seguridad establecidas.

La responsabilidad general de la seguridad de la información recae en la Gerencia, el profesional universitario, el Coordinador de Sistemas de Información y el Líder de facturación, mientras que todos los colaboradores y contratistas tienen la obligación de reportar incidentes de seguridad mediante los canales establecidos en el manual institucional.

Este documento integra las buenas prácticas del SGSI con los procedimientos del Sistema de Gestión de Calidad de la institución, buscando la optimización de recursos y la mejora continua en la eficacia y eficiencia de los procesos hospitalarios.

Mediante este plan, no solo se busca proteger la información, sino también fomentar la conciencia y el compromiso de todo el personal con las normas y procedimientos de seguridad, asegurando así un entorno confiable para nuestros pacientes, colaboradores y la comunidad en general.

2. JUSTIFICACIÓN

La E.S.E Hospital San Vicente de Paúl Mistrató, como institución prestadora de servicios de salud, maneja información crítica y sensible que incluye datos personales de pacientes, historiales clínicos, información financiera, administrativa y operativa. Esta información constituye un activo estratégico que requiere protección integral, no solo por su valor institucional, sino por las implicaciones éticas, legales y de seguridad que conlleva su manejo inadecuado.

En el contexto actual, las instituciones de salud enfrentan amenazas crecientes en materia de seguridad de la información, tales como:

- Ciberataques dirigidos a robo de información sensible.
- Pérdida o filtración de datos por errores humanos o fallas técnicas.
- Vulnerabilidades en sistemas tecnológicos y de almacenamiento.

- Exigencias normativas cada vez más rigurosas en protección de datos personales.

Adicionalmente, la transformación digital del sector salud y la adopción de herramientas tecnológicas para la gestión clínica y administrativa han incrementado la exposición a riesgos informáticos, haciendo indispensable la implementación de un marco estructurado de seguridad que garantice la confidencialidad, integridad y disponibilidad de la información en todo momento.

La Resolución 3100 de 2019 del Ministerio de Salud y Protección Social, junto con la Ley 1581 de 2012 (Ley de Protección de Datos Personales) y el Marco de Seguridad y Privacidad de la Información (MSPI) del Gobierno en Línea, establecen obligaciones específicas para las entidades del sector público en materia de gestión de riesgos y protección de datos. Asimismo, la adopción de estándares internacionales como la ISO/IEC 27001:2013 permite al Hospital alinearse con mejores prácticas globales y fortalecer la confianza de pacientes, colaboradores y entes de control.

Este Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se justifica porque:

1. **Protege la continuidad del servicio de salud**: Garantiza que los sistemas de información clínicos y administrativos estén disponibles y operativos, incluso ante incidentes de seguridad o desastres naturales.
2. **Cumple con el marco legal y regulatorio:** Implementa controles que permiten al Hospital cumplir con las disposiciones nacionales e internacionales en protección de datos, seguridad informática y gestión documental.
3. **Preserva la reputación institucional**: Un incidente de seguridad puede afectar la imagen pública y la confianza de la comunidad en la institución. Este plan mitiga ese riesgo mediante controles proactivos.
4. **Optimiza la gestión de recursos**: Al identificar y priorizar riesgos, el Hospital puede asignar recursos técnicos, humanos y financieros de manera eficiente, enfocándose en las áreas de mayor impacto.
5. **Fomenta una cultura de seguridad**: Involucra a todo el personal en la protección de la información, mediante capacitación, concienciación y procedimientos claros que reducen la probabilidad de errores humanos.
6. **Facilita la auditoría y el control interno**: Proporciona un marco documentado y trazable que permite realizar auditorías internas y externas, demostrando transparencia y gestión responsable de la información.

En consecuencia, la implementación de este plan no es solo una necesidad operativa, sino un imperativo estratégico que permite al Hospital operar en un entorno seguro, resiliente y

alineado con los más altos estándares de calidad y seguridad de la información.

3. ALCANCE

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aplica a todos los activos de información, sistemas tecnológicos, procesos, personal e instalaciones de la E.S.E Hospital San Vicente de Paúl Mistrató, incluyendo sus sedes principales, consultorios externos, puntos de atención y cualquier otra dependencia bajo su administración.

INCLUYE:

1. **Activos de información:**
   - ✓ Datos personales de pacientes, familiares y acompañantes.
   - ✓ Historias clínicas en formato físico y digital.
   - ✓ Información administrativa, financiera y contable.
   - ✓ Documentación legal, contractual y normativa.
   - ✓ Correos electrónicos institucionales y comunicaciones internas.
   - ✓ Bases de datos clínicas y administrativas (R-FAST, SIFYMED, ANNAR, entre otros).
2. **Sistemas y plataformas tecnológicas:**
   - ✓ Infraestructura de red (servidores, routers, switches, firewalls).
   - ✓ Estaciones de trabajo, computadores portátiles y dispositivos móviles institucionales.
   - ✓ Aplicaciones de software clínico, administrativo y de soporte.
   - ✓ Sistemas de almacenamiento y respaldo (NAS, discos duros externos, servicios en la nube).
   - ✓ Dispositivos médicos con conectividad a red o almacenamiento de datos.
3. **Procesos y procedimientos:**
   - ✓ Atención al paciente (registro, consulta, hospitalización, urgencias).
   - ✓ Gestión documental (archivo clínico, archivo administrativo).
   - ✓ Soporte técnico y mantenimiento de sistemas.
   - ✓ Copias de seguridad y recuperación de información.
   - ✓ Intercambio de información con terceros (entidades de salud, proveedores, entes de control).
4. **Personal y terceros:**
   - ✓ Servidores públicos, empleados administrativos y personal de salud.
   - ✓ Contratistas, practicantes y voluntarios.
   - ✓ Proveedores de servicios tecnológicos y de soporte.

- ✓ Cualquier persona que acceda a los sistemas o instalaciones del Hospital.

5. **Instalaciones físicas:**
   - ✓ Áreas de atención al paciente (consultorios, urgencias, hospitalización).
   - ✓ Centros de datos y salas de servidores.
   - ✓ Archivos físicos (clínico y administrativo).
   - ✓ Oficinas administrativas y áreas de soporte.

EXCLUYE:

- Información personal de los empleados manejada exclusivamente por el área de Gestión Humana bajo políticas internas de confidencialidad laboral.
- Sistemas, equipos o información propiedad de pacientes, visitantes o personal que no estén bajo custodia institucional.
- Dispositivos móviles personales (BYOD) no autorizados para uso institucional.
- Plataformas de redes sociales o servicios en la nube no administrados por el área de Tecnología.

LIMITACIONES:

- Este plan no cubre riesgos asociados a eventos de fuerza mayor o catástrofes naturales de escala regional, salvo lo establecido en el Plan de Contingencia institucional
- Los controles de seguridad física general del Hospital (vigilancia, control de accesos) se rigen por procedimientos específicos del área de Seguridad y Vigilancia.
- La implementación de controles tecnológicos avanzados (ej. cifrado de datos en tránsito, segmentación de red) estará sujeta a la disponibilidad presupuestal y técnica.

Este documento es de aplicación obligatoria desde su aprobación y será revisado anualmente o cuando cambios tecnológicos, normativos u operativos lo requieran.

4. OBJETIVOS

4.1. Objetivo General

Establecer e implementar un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información que permita identificar, evaluar, tratar y monitorear de manera sistemática los riesgos asociados a los activos de información y sistemas tecnológicos de la E.S.E Hospital San Vicente de Paúl Mistrató, garantizando la confidencialidad, integridad y disponibilidad de la información clínica, administrativa y financiera, en cumplimiento con el Plan Estratégico de Tecnologías de la Información (PETI), el Modelo de Seguridad y Privacidad de la Información (MSPI) del Gobierno en Línea, la normativa sectorial (Resolución 3100 de 2019, Ley 1581 de 2012) y el estándar internacional ISO/IEC

27001:2013, con el fin de proteger la continuidad de los servicios de salud, la seguridad del paciente y la sostenibilidad institucional.

4.1. Objetivos Específicos

1. **Evaluar los riesgos de seguridad de la información** mediante una metodología estructurada, considerando las amenazas, vulnerabilidades e impactos potenciales sobre los sistemas críticos identificados en el PETI, como la Historia Clínica Electrónica (R-FAST), los servicios de conectividad y las plataformas de reporte institucional.
2. **Asignar responsabilidades claras** para la gestión de riesgos, vinculando a los líderes de procesos, al área de Sistemas, a la Gerencia y al Comité de gestión y desempeño, en concordancia con la estructura organizacional definida en el PETI.
3. **Implementar un programa de concienciación y capacitación** en seguridad de la información dirigido a todo el personal, con énfasis en el manejo adecuado de datos sensibles, prevención de phishing y cumplimiento de políticas institucionales, como parte de la iniciativa de "Cultura y apropiación de TIC en el talento humano" del PETI.
4. **Garantizar el cumplimiento normativo y contractual** en materia de protección de datos personales, seguridad digital y reportes a entes de control, integrando los requerimientos de plataformas como SIVIGILA, PAIWEB, SECOP II, SUIT e INVIMA en los controles de seguridad.
5. **Documentar y socializar los procedimientos de respuesta a incidentes** y continuidad operativa, basados en el Plan de Contingencia Informático del PETI, asegurando una recuperación ordenada y oportuna de los servicios tecnológicos críticos ante eventos adversos.
6. **Optimizar la asignación de recursos tecnológicos y financieros** para el tratamiento de riesgos, priorizando las iniciativas de mayor impacto según la matriz de riesgos y la disponibilidad presupuestal institucional.
7. **Integrar la gestión de riesgos de seguridad de la información** con el **Sistema de Gestión de Calidad** y otros sistemas institucionales, promoviendo un enfoque transversal y sostenible que fortalezca la resiliencia organizacional.

5. MARCO LEGAL

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la E.S.E Hospital San Vicente de Paúl Mistrató se fundamenta en los siguientes marcos normativos

y estratégicos:

Norma	Año	Objeto / Alcance	Aplicación en la E.S.E.
Constitución Política de Colombia	1991	Reconoce el derecho fundamental a la intimidad personal y familiar, al buen nombre (art. 15) y el acceso a documentos públicos con las limitaciones legales (art. 74).	Fundamenta la obligación de proteger la información personal, clínica y sensible, garantizando su reserva y uso adecuado.
Ley 1581	2012	Establece el régimen general de protección de datos personales y los principios para su tratamiento (legalidad, finalidad, seguridad, confidencialidad, entre otros).	Obliga a la E.S.E. a proteger los datos personales de usuarios, funcionarios y contratistas, especialmente datos sensibles y de salud.
Decreto 1377	2013	Reglamenta parcialmente la Ley 1581 de 2012, definiendo autorizaciones, políticas de tratamiento y responsabilidades de responsables y encargados.	Regula la forma en que la E.S.E. recolecta, usa, almacena y protege la información contenida en bases de datos y archivos físicos o digitales.
Ley 1712	2014	Establece la Ley de Transparencia y del Derecho de Acceso a la Información Pública, definiendo excepciones por reserva legal.	Permite clasificar la información clínica, financiera y sensible como información reservada, garantizando su protección.
Ley 1952 (Código General Disciplinario)	2019	Define los deberes de los servidores públicos, incluyendo la obligación de mantener la reserva de la información conocida por razón de sus funciones.	Aplica a servidores públicos y contratistas de la E.S.E. que tengan acceso a información confidencial, con consecuencias disciplinarias en caso de incumplimiento.
Resolución 1995	1999	Regula la historia clínica, su manejo, custodia, reserva y acceso.	Establece la confidencialidad obligatoria de la historia clínica y el acceso restringido solo para fines asistenciales,

			legales o autorizados.
Ley 23 (Ética Médica)	1981	Establece principios éticos del ejercicio médico, incluyendo el secreto profesional.	Refuerza la obligación de confidencialidad del personal asistencial frente a la información de los pacientes.
Decreto 1074	2015	Compila normas relacionadas con protección de datos personales en el sector comercio, aplicables de forma general.	Complementa el marco normativo de protección de datos personales aplicable a la E.S.E.
Modelo Integrado de Planeación y Gestión – MIPG	Vigente	Integra políticas de gestión y control, incluyendo seguridad de la información, transparencia y control interno.	Articula el acuerdo de confidencialidad con la política de seguridad de la información y control interno institucional.

6. MARCO CONCEPTUAL

La seguridad de la información se define como la preservación de la confidencialidad, integridad y disponibilidad de los activos informativos de la organización. En el contexto del Hospital San Vicente de Paúl Mistrató, esto implica proteger datos sensibles como historias clínicas, información financiera y registros administrativos contra accesos no autorizados, alteraciones o pérdidas.

Un riesgo de seguridad de la información representa la combinación de la probabilidad de que ocurra un evento adverso y el impacto que este tendría sobre los activos institucionales. Estos riesgos pueden materializarse a través de amenazas como ciberataques, errores humanos o desastres naturales, que explotan vulnerabilidades existentes en los sistemas, procesos o infraestructura tecnológica.

Los activos de información son todos aquellos recursos que tienen valor para la institución, incluyendo datos digitales, documentos físicos, sistemas informáticos y aplicaciones. En el hospital, los activos críticos incluyen la Historia Clínica Electrónica (HCE), el sistema R-FAST, las bases de datos clínicas y administrativas, y los registros en plataformas externas como SIVIGILA y SECOP II.

El tratamiento de riesgos es el proceso mediante el cual la organización selecciona e implementa controles para modificar el nivel de riesgo, ya sea mediante su mitigación (implementación de controles), transferencia (contratación de seguros o tercerización), aceptación (cuando el riesgo está dentro de niveles tolerables)

o evitación (eliminación de la actividad riesgosa).
La gestión de riesgos sigue una metodología estructurada que incluye identificación, análisis, evaluación y tratamiento, alineada con la norma ISO 27005 y articulada con las iniciativas del PETI institucional. Este proceso se enmarca dentro del ciclo de mejora continua PHVA (Planificar-Hacer-Verificar-Actuar), que garantiza la revisión periódica y actualización de los controles implementados.

El Sistema de Gestión de Seguridad de la Información (SGSI) según ISO 27001 proporciona el marco integral para gestionar de manera sistemática la protección de la información, mientras que el Modelo de Seguridad y Privacidad de la Información (MSPI) del Gobierno en Línea establece los lineamientos específicos para entidades públicas colombianas.

Conceptos operativos clave incluyen el RTO (Tiempo Objetivo de Recuperación), que para sistemas críticos como la HCE es de 4 horas según el PETI, y el RPO (Punto Objetivo de Recuperación), que define la pérdida máxima de datos aceptable. La continuidad operativa se asegura mediante el Plan de Contingencia Informático institucional, que establece procedimientos para la recuperación ordenada de servicios tecnológicos.

La clasificación de información permite categorizar los datos según su sensibilidad (Pública, Interna, Confidencial, Restringida), asignando responsabilidades claras donde los propietarios de la información (líderes de área) definen los requisitos de protección y los custodios (área de Sistemas, Archivo) implementan los controles físicos y lógicos.

Finalmente, la cultura de seguridad se refiere al conjunto de valores, actitudes y comportamientos del personal respecto a la protección de la información, fomentada mediante programas de capacitación, concienciación y políticas institucionales que promueven el reporte oportuno de incidentes de seguridad y el cumplimiento de los procedimientos establecidos.

7. DEFINICIONES

Activo de Información: Cualquier dato o conjunto de datos que posee valor para la E.S.E Hospital San Vicente de Paúl Mistrató, incluyendo información clínica, administrativa, financiera y de gestión, ya sea en formato físico, digital o electrónico. Ejemplos: Historias clínicas, bases de datos R-FAST, registros de laboratorio, documentos contractuales.
Amenaza: Evento o circunstancia potencial que puede causar daño a los activos de información, explotando vulnerabilidades existentes. Puede ser de origen natural, humano, técnico o ambiental. Ejemplos: Ataques de ransomware, errores de personal, fallas eléctricas, inundaciones.
Vulnerabilidad: Debilidad o deficiencia en un activo, proceso o control que puede ser aprovechada por una amenaza para causar daño. Ejemplos: Software desactualizado, contraseñas débiles, falta de capacitación del personal, equipos obsoletos.
Riesgo de Seguridad de la Información: Potencial de que una amenaza explote una

Cra 5 N° 8-36 - Tel: 3502702807
E-Mail: hospital.mistrato@hsvpmistrato.gov.co
Mistrató Risaralda

vulnerabilidad de un activo de información, causando impacto adverso a la institución en términos de confidencialidad, integridad o disponibilidad. Se expresa como combinación de probabilidad e impacto.

Tratamiento de Riesgos: Proceso de selección e implementación de medidas para modificar el riesgo. Las opciones incluyen: Mitigar (implementar controles), Transferir (compartir con terceros), Aceptar (asumir conscientemente) o Evitar (eliminar la fuente del riesgo).

Control de Seguridad: Medida o conjunto de medidas implementadas para reducir el riesgo a un nivel aceptable. Pueden ser preventivos, detectivos o correctivos. Ejemplos: Firewall, políticas de contraseñas, sistema de respaldo, capacitación.

Confidencialidad: Propiedad que garantiza que la información solo sea accesible para aquellos autorizados a tener acceso, previniendo la divulgación no autorizada.

Integridad: Propiedad que salvaguarda la exactitud y completitud de la información y sus métodos de procesamiento, previniendo modificaciones no autorizadas.

Disponibilidad: Propiedad que asegura que la información y los sistemas asociados sean accesibles y utilizables cuando sean requeridos por usuarios autorizados.

Sistema de Gestión de Seguridad de la Información (SGSI): Marco de trabajo basado en el enfoque de procesos, establecido para instaurar, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información dentro de la organización, según los requisitos de la norma ISO/IEC 27001.

Historia Clínica Electrónica (HCE): Registro digital de la información clínica relevante de un paciente, generada durante su atención en salud, que cumple con los requisitos técnicos de la Resolución 3100 de 2019 y se gestiona a través del sistema R-FAST.

Plan de Contingencia Informático: Conjunto de procedimientos y recursos tecnológicos establecidos para responder, recuperar y restablecer los servicios de tecnología de la información ante incidentes o desastres que afecten su operación normal.

Tiempo Objetivo de Recuperación (RTO): Tiempo máximo aceptable durante el cual un servicio de tecnología puede estar indisponible después de un incidente, sin afectar críticamente las operaciones institucionales. Para la HCE es de 4 horas según el PETI.

Punto Objetivo de Recuperación (RPO): Pérdida máxima de datos aceptable medida en tiempo, que determina la frecuencia mínima requerida para las copias de seguridad. Define cuánta información puede perderse sin impactar críticamente la operación.

Incidente de Seguridad de la Información: Evento identificado que indica una posible violación de la política de seguridad o falla de los controles, que puede comprometer la confidencialidad, integridad o disponibilidad de la información.

Propietario del Activo de Información: Persona o área con autoridad delegada para gestionar un activo específico, responsable de definir sus requisitos de protección, clasificación y controles apropiados. Generalmente corresponde a los líderes de procesos.

Custodio del Activo de Información: Persona o área responsable de la protección física o lógica del activo, implementando los controles definidos por el propietario. En el hospital, corresponde principalmente al área de Sistemas para activos digitales y al Archivo para documentos físicos.

Clasificación de la Información: Proceso de categorizar la información según su nivel de sensibilidad y criticidad, asignando etiquetas como: Pública, Uso Interno, Confidencial o Restringida, para determinar los controles de protección requeridos.

PETI (Plan Estratégico de Tecnologías de la Información): Documento rector institucional que define las iniciativas, proyectos y acciones en materia tecnológica para el período 2024-2026, sirviendo como marco de referencia para la gestión de riesgos de seguridad de la información.
MSPI (Modelo de Seguridad y Privacidad de la Información): Marco técnico del Ministerio de Tecnologías de la Información y las Comunicaciones que establece los lineamientos para implementar controles de seguridad en entidades públicas colombianas.
Ciclo PHVA (Planificar-Hacer-Verificar-Actuar): Metodología de mejora continua aplicada a la gestión de seguridad de la información, que garantiza la revisión periódica y actualización de controles y procedimientos.
Cultura de Seguridad: Conjunto de valores, actitudes, percepciones y comportamientos compartidos por el personal respecto a la protección de la información institucional, promovida mediante programas de concienciación, capacitación y políticas claras.
Copia de seguridad: También conocida como "copia de respaldo". En tecnologías de la información es una copia de los datos originales, que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
Herramienta de Backup: Es un programa o software que se utiliza para garantizar la actividad de copia de respaldo de la información de manera automática. Permite definir una serie de parámetros para automatizar la actividad, en un periodo definido por el administrador.
Información: Datos dotados de significado y propósito para la E.S.E HOSPITAL SAN VICENTE DE PAÚL MISTRATÓ.
Instructivo: Permite darle cumplimiento a una tarea o actividad determinada, mediante una secuencia paso a paso, que puede ser interpretada como una serie de instrucciones a seguir. Los instructivos también pueden hacer uso de imágenes que permiten ganar claridad en la secuencia a seguir.
Información: Grupo de datos ya supervisados y ordenados, que sirven para construir uno o varios registros.
Integridad: Es el estado en que se encuentra algo. Una información es integra cuando, después de elaborada y/o alojada en algún sistema de información, no se experimenta ninguna modificación sobre ella, sin previa autorización de su propietario. También dentro del concepto de integridad, cabe destacar la veracidad de la información, puesto que una información es integra cuando es veraz también.
Restauración: Es la acción que permite devolver algo, al estado o circunstancia, en la que se encontraba antes.

8. MARCO DE GOBERNANZA Y RESPONSABILIDADES

El Sistema de Gestión de Seguridad de la Información (SGSI) del Hospital San Vicente de Paúl Mistrató se fundamenta en una estructura de gobernanza simplificada y operativa, donde la Gerencia General ejerce la máxima autoridad en materia de seguridad de la

información, con decisiones clave tomadas en el Comité de Gestión y Desempeño institucional.

Nivel Estratégico - Toma de Decisiones
Responsable: Gerente General
Funciones:

- Aprobar políticas, estándares y procedimientos de seguridad de la información
- Asignar recursos presupuestales para la implementación de controles
- Validar la matriz de riesgos institucional y los planes de tratamiento
- Tomar decisiones sobre incidentes de seguridad críticos
- Asegurar el cumplimiento del marco legal y normativo
- Revisar el desempeño del SGSI en el Comité de Gestión y Desempeño
- Designar responsables y delegar autoridad para la ejecución

Nivel Táctico - Coordinación y Supervisión
Responsable: Planeación y control interno
Funciones:

- Coordinar la implementación de las políticas de seguridad aprobadas
- Supervisar la ejecución del Plan de Tratamiento de Riesgos
- Gestionar los recursos asignados para seguridad de la información
- Actuar como enlace entre la Gerencia y el nivel operativo
- Revisar reportes de incidentes y planes de acción correctiva
- Velar por la integración del SGSI con otros sistemas de gestión
- Convocar reuniones técnicas cuando sea necesario

Nivel Operativo - Ejecución y Gestión
Responsable: Coordinador de Sistemas
Funciones:

- Implementar y mantener los controles de seguridad técnica
- Gestionar el inventario de activos de información
- Ejecutar la evaluación periódica de riesgos
- Administrar el Plan de Contingencia Informático
- Supervisar las copias de seguridad y recuperación
- Capacitar al personal en temas de seguridad
- Investigar y reportar incidentes de seguridad

Cra 5 N° 8-36 - Tel: 3502702807
E-Mail: hospital.mistrato@hsvpmistrato.gov.co
Mistrató Risaralda

9. DERECHOS Y RESPONSABILIDADES DE LA INSTITUCIÓN

La E.S.E., en su calidad de responsable de los activos de información y de los sistemas que los soportan, define los siguientes derechos y responsabilidades, los cuales son de obligatorio cumplimiento para todos los servidores públicos, contratistas y terceros que tengan acceso a la información institucional:

a. La institución se reserva todos los derechos sobre sus activos de información, incluyendo los datos, mensajes y contenidos que reposen o transiten por sus sistemas de información y medios de almacenamiento. En consecuencia, los usuarios de los sistemas institucionales no deberán tener allí información de carácter personal.
b. Se prohíbe el manejo, almacenamiento, procesamiento o transmisión de información institucional en sistemas, dispositivos o plataformas ajenas a la entidad, salvo cuando sea estrictamente necesario para el cumplimiento de obligaciones legales o contractuales y cuente con autorización expresa de la institución.
c. La institución conserva los derechos de propiedad intelectual sobre cualquier material generado en el marco de sus funciones, aun cuando dicho material sea publicado o divulgado en foros, medios o plataformas de acceso público.
d. Con el fin de proteger los equipos, archivos y medios de almacenamiento, se prohíbe el consumo de alimentos en los puestos de trabajo donde se manipule información o se utilicen equipos tecnológicos.
e. En concordancia con las normas de seguridad y salud en el trabajo, se prohíbe fumar en las instalaciones de la institución.
f. Todo equipo, archivo o medio de almacenamiento extraíble que sea conectado a los sistemas institucionales deberá contar con las medidas de protección y verificación establecidas por el área de tecnología, con el fin de prevenir la introducción de software malicioso.
g. La información que sea registrada, reportada o procesada en los sistemas de información institucionales deberá ser completa, veraz, oportuna y confiable, siendo responsabilidad del usuario que la genera o administra.
h. Ante cualquier sospecha, indicio o evidencia de fuga, pérdida, alteración o uso indebido de la información, se deberá informar de manera inmediata a la Gerencia y al responsable de tecnología o sistemas de la información, conforme a los procedimientos establecidos.
i. Se prohíbe iniciar, reenviar o distribuir correos electrónicos encadenados, mensajes masivos no autorizados o comunicaciones que no guarden relación con las funciones institucionales.
j. Se prohíbe el uso del correo electrónico institucional para el envío o recepción de correo no deseado, publicidad no autorizada o mensajes que puedan afectar la seguridad de la información o la imagen institucional.
k. Se prohíbe el abandono de documentos impresos que contengan información confidencial o sensible en impresoras, fotocopiadoras u otros dispositivos similares, debiendo garantizarse su custodia y disposición segura.

10. CONFIDENCIALIDAD DE LA INFORMACIÓN

a. Toda la información generada, administrada o custodiada por la institución será considerada confidencial, salvo aquella que por disposición legal tenga el carácter de información pública, y se adoptarán las medidas técnicas, administrativas y organizacionales necesarias para garantizar su protección, privacidad y uso adecuado.
b. Es responsabilidad de cada servidor público, contratista o tercero autorizado velar por la custodia, uso correcto y protección de la información a la que tenga acceso, así como de los documentos, archivos y equipos ubicados en su puesto de trabajo o bajo su responsabilidad.
c. El acceso a la información institucional estará restringido únicamente a usuarios internos o externos debidamente autorizados, de conformidad con los roles y funciones asignados. Las autorizaciones de acceso serán otorgadas, modificadas o revocadas por la Gerencia, en coordinación con el área de sistemas.
d. La información institucional será centralizada y administrada por el área de Sistemas de Información, la cual será responsable de su gestión, protección, disponibilidad y respaldo, de acuerdo con las políticas y procedimientos establecidos.
e. La entidad realizará copias de seguridad diarias de la información contenida en los sistemas de información y de aquella almacenada en los servidores institucionales, garantizando la recuperación oportuna de la información en caso de incidentes.
f. Los equipos tecnológicos de la institución deberán contar con mecanismos de protección actualizados, incluyendo software antivirus y otras herramientas de seguridad, los cuales serán revisados y actualizados periódicamente por el área de tecnología.
g. La información privada y confidencial estará protegida mediante controles de acceso lógico y físico, asegurando que únicamente el personal autorizado pueda acceder a ella, de acuerdo con los niveles de seguridad definidos.
h. El acceso físico a las áreas donde se maneja información confidencial o sensible, el área de servidores estará restringido y controlado, permitiendo el ingreso únicamente a personal autorizado.
i. Se deberá evitar el envío de información confidencial por fuera de los sistemas institucionales. En los casos excepcionales en que sea necesario realizarlo, el receptor deberá garantizar la confidencialidad, integridad y seguridad de la información, de conformidad con la normativa vigente.
j. Todo servidor público, contratista, estudiante o tercero que ingrese a la institución deberá suscribir un Acuerdo de Confidencialidad como requisito obligatorio para el acceso a la información institucional.

11. METODOLOGÍA DE GESTIÓN DE RIESGOS

El Hospital San Vicente De Paul Mistrató Risaralda Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento. La Alta Dirección y Comité Institucional de Coordinación de Control Interno, les corresponde Establecer y aprobar la Política para la Administración del Riesgo del Hospital San Vicente de Paul Mistrató. Revisar el cumplimiento de la Política para la Administración de Riesgos de manera periódica, evaluar su impacto y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento a las que pueda haber lugar.

Se establecen tres líneas de defensa.

a. La primera línea de defensa tiene como propósitos, define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento
b. La segunda línea de defensa, Asegurara que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados y funcionen correctamente.
c. Y una tercera línea que proporcionará a través de la auditoría independiente información sobre la efectividad del Sistema de Control interno, con un enfoque basado en el riesgo e incluidas la manera en que funciona la primera y segunda línea de defensa.

9.1. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

A continuación, se presenta cada una de las etapas a desarrollar durante la administración del riesgo; en la descripción de cada etapa se desplegarán los aspectos conceptuales y operativos que se deben tener en cuenta.

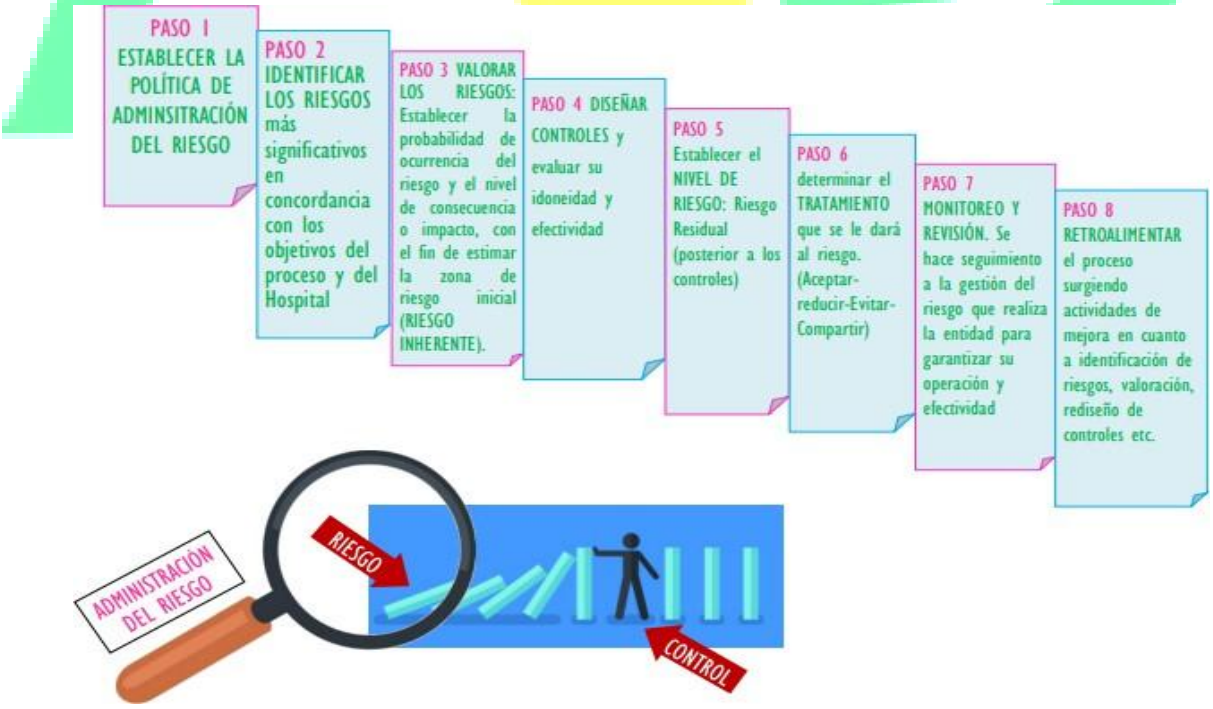
- Socializar la metodología de riesgos, los lineamientos de la primera línea de defensa frente al riesgo, objetivo del proceso, comunicación de los planes y proyectos del proceso asesorados.
- Capacitar al grupo de trabajo de cada dependencia en la herramienta para la gestión del riesgo.
- Liderar las mesas de trabajo de identificación del riesgo.
- Verificar que las acciones de control se documenten conforme a los requerimientos de la metodología.
- Identificar claramente, junto con el equipo de trabajo, los responsables de las acciones y las fechas de realización, y registrarlas en la herramienta para la gestión del riesgo.
- Elaborar el mapa de riesgos de proceso con toda la información respectiva,

a partir de la información construida con los equipos de trabajo.

- Socializar y publicar el mapa de riesgos institucional a partir de los mapas de proceso, con los riesgos altos, extremos y de corrupción.
- Garantizar que todo su grupo de trabajo conozca el concepto de administración del riesgo, su política y metodología y actores que intervienen.
- Delegar cuando sea necesario en los profesionales que se encargarán de la identificación, monitoreo, reporte y socialización del riesgo del proceso.

9.2. ETAPAS PARA LA GESTION DE LOS RIESGOS

Se definen 8 etapas que se muestran en forma organizada en el siguiente cuadro



9.3. NIVEL DE ACEPTACION Y TRATAMIENTO DEL RIESGO

La ESE Hospital San Vicente de Paul Mistrató Risaralda adopta la matriz de riesgo de la metodología DAFP en cuanto a los niveles de aceptación del riesgo así:

Acorde con los riesgos residuales aprobados por el Comité Institucional de Coordinación de Control Interno, se deberá definir la periodicidad de seguimiento y estrategia de tratamiento a los riesgos residuales aceptados, así:

Opciones de tratamiento de acuerdo con zona de riesgo					
Zona de riesgo	Semáforo	Evitar	Reducir	Compartir	Aceptar
Extremo	Rojo	x	x	x	
Alto	Naranja	x	x	x	
Moderado	Amarillo	x	x	x	
Bajo	Verde				x

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

a) Evitar. Cuando el comportamiento del riesgo se considera demasiado extremo se deben tomar las acciones pertinentes para abandonar, no iniciar o no continuar con las acciones o actividades que lo generan o sustituyendo la actividad por otra en donde haya menos exposición o las posibles pérdidas sean menores.

b) Reducir. Definir y aplicar medidas de tratamiento orientadas a minimizar la probabilidad de ocurrencia y/o materialización del riesgo a través de la implementación de controles preventivos y/o detectivos apropiados o pertinentes. Además de los controles se deben señalar las responsabilidades de tal manera que el tratamiento adoptado logre la reducción del riesgo prevista. Para mitigar y tratar los riesgos de seguridad digital.

c) Compartir. Los riesgos en los cuales la entidad carezca de capacidad necesaria para

su gestión pueden ser compartidos o transferidos mediante la aplicación de medidas como contratos de seguros y tercerización; por ejemplo, actividades como: seguro de vehículo, vigilancia, aseo, entre otras que la entidad considere pertinente; lo anterior a fin de reducir la probabilidad o el impacto de su posible materialización.

d) Aceptar. Los riesgos de gestión y de seguridad digital que se ubiquen dentro de una zona baja después de evaluados sus controles, deben contar con un monitoreo y seguimiento continuo, dado que pueden quedar riesgos residuales.

En la siguiente tabla se indican las opciones de tratamiento del riesgo de acuerdo con la zona de riesgo.

Tratamiento del Riesgo		
Tipo de Riesgo	**Zona de Riesgo Residual**	**Estrategia de tratamiento**
Riesgos de Gestión y Seguridad digital	Baja	Se ACEPTA el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado y se realiza en el reporte mensual de su desempeño.
	Moderada	Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad o el impacto de ocurrencia del riesgo, se hace seguimiento BIMESTRAL y se registran sus avances en la matriz de gestión del riesgo.
	Alta y Extrema	Se debe incluir el riesgo tanto en el Mapa de riesgo del Proceso como en el Mapa de Riesgo Institucional y se establecen acciones de Control Preventivas que permitan EVITAR la materialización del riesgo. Se monitorea MENSUALMENTE y y se registran sus avances en la matriz de gestión del riesgo.

9.4. IDENTIFICACIÓN DEL RIESGO

Identificación de activos

El principal activo de una organización es la información, la cual puede estar en forma física como documentos (Archivo de gestión) o escritos a mano (libros de cirugía, libros de vigilancia, libros de defunción o nacimiento), en medios electrónicos almacenados en Discos Duros Externos (Back up), Memorias USB (firmas digitales o informes) o en forma digital (bases de datos), en los equipos de cómputo o en la Nube. Toda esta información requiere ser analizada para su protección. (Un activo es todo aquello que genera valor para una empresa u organización.)

Para este proceso se llevará a cabo un inventario de activos mediante una encuesta en la que se identificará su tipología si es software o hardware, si esta información se encuentra de manera digital o física, y si se encuentra en digital que tipo de archivo es. Aparte de conocer toda la información al interior de la institución también se realizará una valoración de esta información mediante los siguientes criterios:

Confidencialidad

Nivel	Descripción Criterio de Confidencialidad	Denominación
0	Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado o no	**Publico**
1	Información que puede ser conocida y utilizada por todos los empleados y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la institución, el Sector Público Nacional o terceros.	**Reservada –Uso Interno**
2	Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la institución o a terceros.	**Reservada – Confidencial**

3	**Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de la institución, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo o a terceros.**	**Reservada Secreta**

Integridad

Nivel	Descripción Criterio de Integridad
0	**Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operación.**
1	**Información cuya modificación no autorizada puede repararse, aunque podría ocasionar pérdidas leves.**
2	**Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas.**
3	**Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves.**

Disponibilidad

Nivel	Descripción Criterio de Disponibilidad
0	**Información cuya inaccesibilidad no afecta la operación.**
1	**Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas.**
2	**Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas.**
3	**Información cuya inaccesibilidad permanente durante una hora podría ocasionar pérdidas significativas.**

Después de este proceso se procederá a identificar también su ubicación ya sea al interior de la institución o por fuera en algún servicio en la nube y en cualquier caso las credenciales de ingreso si se necesitase.

Identificación Del Riesgo

Los riesgos numerados a continuación son identificados en la guía metodológica del ministerio de las TICS:

1. **Riesgo Estratégico**: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas,

diseño y conceptualización de la entidad por parte de la alta gerencia.

2. **Riesgos de Imagen**: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
3. **Riesgos Operativos**: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.
4. **Riesgos Financieros**: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
5. **Riesgos de Cumplimiento**: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, de acuerdo con su misión.
6. **Riesgos de Tecnología**: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras, y el cumplimiento de la misión.

En cuanto a los riesgos que afectan directamente a la información se ha evidenciado en la literatura en los siguientes.

Riesgos Informáticos	Causas	Efecto

Perdida Robo o Fuga de Informaci ón	- Fallas en el proceso de copia de respaldo o de restauración de la información, o pérdida de la misma. - Fallas en los análisis y socialización de las vulnerabilidades de la infraestructura de IT - No contar con acuerdos de confidencialidad con los empleados y terceros. - Falta de autorización para la extracción de información generadas por requerimientos. - Ingreso a la red y acceso a los activos de TI por parte de máquinas ajenas a la entidad. - Habilitación de puertos USB en modo lectura y escritura para medios de almacenamiento - Ataques cibernéticos internos o externos - Empleados no capacitados en los temas de riesgos informáticos. - Desconocimiento del riesgo. - Prestar los equipos informáticos a personal no autorizado. - No cerrar sesión cuando se desplaza del puesto. - Acceso no autorizado a las dependencias. - Conectar dispositivos externos a los equipos.	- Afectación parcial o total de la continuidad de las operaciones de los servicios del Incumplimiento normativo. - Vulneración de los sistemas de seguridad operando actualmente. - Mala imagen, multas, sanciones y pérdidas económicas. - Generación de consultas, funcionalidades o reportes con información sensible de los clientes. - Pérdida o fuga de información.

Correos electrónicos de extraña procedencia	- Empleados no capacitados en los temas de riesgos informáticos. - Desconocimiento del riesgo. - No generar una Cultura de Seguridad de la Información. - Falta de Filtros en el Servidor de Correo. - Programas de DLP (Data Lost Prevention). - Falta de instalación de EndPoint (programa seguridad punto final) en las estaciones de trabajo.	- Cifrado o secuestro de la información. - Monitoreo de las actividades realizadas en el equipo. - Ataque remoto mediante un troyano o gusano. - Robo de contraseñas. - Equipo usado como Zombie. - Robo de documentos y/o archivos. - Sistema con mal Funcionamiento
Daño en los equipos tecnológicos	- Manejo inadecuado de los equipos. - Falta de mantenimiento o mala conexión de los mismos en las instalaciones eléctricas. - Falta de equipos de potenciación. - Fallas por defectos de fábrica. - Derrame de líquido. - Falta de ambiente adecuado para los equipos. - Falta Educación a los usuarios en el manejo de los equipos de computo	- Perdida de información. - Perdidas de los - quipos informáticos. - Indisponibilidad del Servicio. - Traumatismos en los procesos.
Perdida de conectividad	- Daño externo del proveedor de internet. - Ataque DDoS o DOS (denegación de servicios distribuidos o Denegación de servicios).	

Ataques Informáticos	- Estimulo o Reto personal. - Rebelión. - Ánimo de lucro. - Espionaje.	- Daño en los equipos tecnológicos. - Incidente en la confidencialidad, integridad y disponibilidad de la información. - Denegación de servicios. - Secuestro de la información. - Divulgación ilegal de la información. - Suplantación de identidad. - Destrucción de la información. - Soborno de la información.

Identificación de amenazas

Una amenaza se identifica como un evento, persona, situación o fenómeno que pueda causar daño no solo a un activo sino también a varios activos de la organización por ende hay que identificarlos de la mejor manera. Las amenazas pueden ser de origen Humano o Ambientales.

Tipo	Amenaza
Daño físico	Fuego
	Agua
	Contaminación
	Accidente Importante
	Destrucción del equipo o medios
	Polvo, corrosión, congelamiento
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
	Fenómenos meteorológicos
	Inundación
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado
	Perdida de suministro de energía
	Falla en equipo de telecomunicaciones
Perturbación debida a la radiación	Radiación electromagnética
	Radiación térmica
	Impulsos electromagnéticos
	Espionaje remoto

	Escucha encubierta
	Hurto de medios o documentos
	Hurto de equipo
	Recuperación de medios reciclados o desechados
	Divulgación
	Datos provenientes de fuentes no confiables
	Manipulación con hardware
	Manipulación con software
	Detección de la posición
Fallas técnicas	Fallas del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información.
Acciones no autorizadas	Uso no autorizado del equipo
	Copia fraudulenta del software
	Uso de software falso o copiado
	Corrupción de los datos
	Procesamiento ilegal de datos
Compromiso de las funciones	Error en el uso
	Abuso de derechos
	Falsificación de derechos
	Negación de acciones
	Incumplimiento en la disponibilidad del personal

Identificación de las vulnerabilidades

Las vulnerabilidades son las Fallas o debilidades en un sistema, que puede ser explotada por quien la conozca. Cuando la amenaza encuentra la vulnerabilidad es cuando se crea el riesgo. Por eso es necesario conocer la lista de amenazas y el inventario de activos de información.

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento preventivo y correctivo insuficiente	Incumplimiento en el mantenimiento del sistema de información
Hardware	Instalación inadecuada de equipos o medios de almacenamiento	Daño o destrucción de equipos

Hardware	Ausencia de esquemas de reemplazo periódico	Fallas críticas de equipos
Hardware	Exposición a humedad, polvo o suciedad	Deterioro físico de equipos
Hardware	Sensibilidad a variaciones de voltaje	Pérdida del suministro de energía
Hardware	Sensibilidad a variaciones de temperatura	Fenómenos meteorológicos
Hardware	Almacenamiento de equipos sin protección física	Hurto de equipos o medios
Hardware	Falta de control en la disposición final de equipos	Fuga de información
Hardware	Copias no controladas de medios de almacenamiento	Hurto de información

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Software	Ausencia o insuficiencia de pruebas de software	Mal funcionamiento del software
Software	Defectos conocidos no corregidos	Corrupción de datos
Software	Asignación errada de permisos de acceso	Abuso de los derechos
Software	Gestión deficiente de contraseñas	Falsificación de derechos
Software	Ausencia de mecanismos de autenticación	Acceso no autorizado
Software	Configuración incorrecta de parámetros	Error en el uso
Software	Ausencia de documentación del software	Error en el uso
Software	Software no licenciado o no controlado	Uso de software falsificado
Software	Ausencia de copias de respaldo	Pérdida de información
Software	Descarga e instalación no controlada	Manipulación del software
Software	Ausencia de control de cambios	Mal funcionamiento del software

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Red	Cableado estructurado deficiente	Fallas en telecomunicaciones
Red	Punto único de falla en la red	Interrupción del servicio
Red	Arquitectura de red insegura	Espionaje remoto
Red	Transferencia de contraseñas en texto plano	Interceptación de información
Red	Conexiones a redes públicas sin protección	Uso no autorizado del equipo
Red	Ausencia de autenticación de emisor y receptor	Falsificación de derechos

Red	Gestión inadecuada del enrutamiento	Saturación del sistema

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Personal	Entrenamiento insuficiente en seguridad de la información	Error en el uso
Personal	Falta de conciencia en seguridad	Error en el uso
Personal	Uso incorrecto de software y hardware	Error en el uso
Personal	Ausencia de monitoreo de actividades críticas	Procesamiento ilegal de datos
Personal	Trabajo no supervisado de personal externo	Hurto de medios o documentos
Personal	Ausencia de políticas de uso de TIC	Uso no autorizado del equipo
Personal	Manejo inadecuado de controles de acceso físico	Daño a la infraestructura

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Lugar	Ubicación en zonas susceptibles a inundación	Daño a la infraestructura
Lugar	Red eléctrica inestable	Daño a equipos y sistemas
Lugar	Ausencia de protección física adecuada	Daño a infraestructura física y tecnológica

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Organización	Ausencia de procedimientos para creación y retiro de usuarios	Abuso de los derechos
Organización	Falta de revisión periódica de accesos	Acceso indebido
Organización	Ausencia de auditorías internas	Abuso de los derechos
Organización	Ausencia de identificación y valoración de riesgos	Fallas del sistema
Organización	Ausencia de acuerdos de nivel de servicio (ANS)	Incumplimiento del servicio
Organización	Ausencia de planes de continuidad	Interrupción del servicio
Organización	Falta de políticas de correo electrónico	Error en el uso
Organización	Ausencia de control de activos fuera de la entidad	Hurto de equipos
Organización	Falta de procedimientos disciplinarios	Reincidencia de incidentes
Organización	Ausencia de políticas de escritorio limpio	Hurto de información
Organización	Falta de monitoreo de incidentes de seguridad	Uso no autorizado del equipo

Identificación De Controles Existentes

La identificación de los controles existentes permite realizar la evaluación de riesgos. Es necesario realizar esta identificación para poder conocer si existen controles similares o incluso repetidos que se pueden unificar y posterior a esto evaluarlos para calificar como ineficaz, insuficiente o injustificado, si es injustificado o insuficiente, se debería revisar el control para determinar si se debe eliminar o reemplazar por otro más adecuado.

Evaluación de riesgo

La evaluación de riesgo se realiza con enfrentamiento entre la probabilidad de ocurrencia y el impacto que genera el riesgo en los activos de información, dado por la matriz de calificación, evaluación y respuestas a los riesgos.

Tabla de probabilidad

Valor	Nivel	Descripción	Criterio de ocurrencia
1	**Raro**	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos **5 años** en la institución.
2	**Improbable**	El evento puede ocurrir en algún momento, pero no es frecuente.	Se ha presentado **al menos una vez en los últimos 5 años**.
3	**Posible**	El evento podría ocurrir en algún momento bajo condiciones normales.	Se ha presentado **al menos una vez en los últimos 2 años**.
4	**Probable**	El evento probablemente ocurra en la mayoría de las circunstancias.	Se ha presentado **al menos una vez en el último año**.
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Se presenta **más de una vez al año**.

Tabla de impacto

Valor	Nivel	Descripción del impacto
1	**Insignificante**	Si el evento llegara a presentarse, tendría consecuencias o efectos **mínimos**, sin afectar la operación, la atención al usuario ni el cumplimiento normativo.
2	**Menor**	Si el evento llegara a presentarse, tendría un **bajo impacto**, con afectación leve y recuperable sobre los procesos de la entidad.
3	**Moderado**	Si el evento llegara a presentarse, tendría **consecuencias moderadas**, generando interrupciones parciales del servicio, reprocesos o afectación administrativa.
4	**Mayor**	Si el evento llegara a presentarse, tendría **altas consecuencias**, con impacto significativo en la continuidad del servicio, la seguridad del paciente o el cumplimiento legal.

5	**Catastrófico**	Si el evento llegara a presentarse, tendría **consecuencias desastrosas**, comprometiendo gravemente la operación institucional, la seguridad del paciente, la información crítica o la imagen de la entidad.

Tabla de evaluación del riesgo

Probabilidad	**Impacto**				
	Insignificante (1)	**Menor (2)**	**Moderado (3)**	**Mayor (4)**	**Catastrófico (5)**
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E
B: Zona de Riesgo Baja: Asumir el riesgo					
M: Zona de Riesgo Moderada: Asumir el riesgo, Reducir el riesgo					
A: Zona de Riesgo Alta: Reducir, Evitar, Compartir o Transferir					
E: Zona de Riesgo extrema: Reducir el riesgo, evitar compartir o transferir					

Ejemplo de análisis de riesgo.

Riesgo	Probabilidad	Impacto	Tipo de impacto	Evaluación (Pxl)	Zona de riesgo	Medidas de respuesta
Pérdida, robo o fuga de información	**3 (Posible)**	**5 (Catastrófico)**	Disponibilidad, Integridad y Confidencialidad de la información	**15**	**Extrema**	Reducir el riesgo / Evitar el riesgo / Transferir el riesgo

12. RIESGOS IDENTIFICADOS – SEGURIDAD DE LA INFORMACIÓN

1. Riesgos asociados al SUBPROCESO
Contingencia, Recuperación y Retorno a la Normalidad

1. **Interrupción prolongada de los servicios de información institucional:** *Posible*

Cra 5 N° 8-36 - Tel: 3502702807
E-Mail: hospital.mistrato@hsvpmistrato.gov.co
Mistrató Risaralda

ocurrencia de eventos naturales o provocados por el hombre que afecten la operación de la plataforma tecnológica, impidiendo la continuidad de los servicios asistenciales y administrativos.

2. **Fallas en la activación oportuna del plan de contingencia:** *Riesgo de retrasos en la identificación del desastre, comunicación interna o ejecución del plan, incrementando el tiempo de indisponibilidad de los sistemas.*
3. **Deficiencias en la recuperación y retorno a la normalidad de los servicios TIC:** *Riesgo de no restablecer los sistemas en los tiempos definidos, afectando la atención al usuario, la facturación y los procesos misionales.*

2. Riesgos asociados al SUBPROCESO
Copia de Respaldo de la Información

4. **Pérdida irreversible de información institucional:** *Riesgo de que las copias de respaldo no se realicen, no se almacenen correctamente o se encuentren incompletas, afectando la disponibilidad de la información.*
5. **Copias de respaldo desactualizadas o inconsistentes:** *Riesgo de que la información respaldada no refleje la versión más reciente de los datos clínicos, administrativos o financieros.*
6. **Almacenamiento inseguro de copias de respaldo:** *Riesgo de accesos no autorizados, daño físico o lógico de los respaldos, comprometiendo la confidencialidad e integridad de la información.*

3. Riesgos asociados al SUBPROCESO
Restauración de la Información

7. **Imposibilidad de restaurar la información ante un incidente:** *Riesgo de fallas técnicas o procedimentales durante la restauración de copias de respaldo.*
8. **Restauración de información alterada o incompleta:** *Riesgo de pérdida de integridad de los datos restaurados, afectando la confiabilidad de la información institucional.*
9. **Falta de verificación de la información restaurada:** *Riesgo de reincorporar información defectuosa a los sistemas productivos sin detección oportuna.*

4. Riesgos asociados al SUBPROCESO
Creación de Usuarios en Plataformas de Información

10. **Asignación inadecuada de roles y privilegios de acceso:** *Riesgo de otorgar permisos superiores o diferentes a los requeridos por el perfil del funcionario.*
11. **Uso indebido de credenciales de acceso:** *Riesgo derivado de entrega insegura de usuarios y contraseñas o incumplimiento de las políticas de manejo de credenciales.*

12. **Permanencia de cuentas activas de personal desvinculado:** *Riesgo de accesos no autorizados por falta de eliminación o bloqueo oportuno de cuentas.*

5. Riesgos asociados al SUBPROCESO
Intercambio de Información Digital

13. **Divulgación no autorizada de información clasificada o reservada:** *Riesgo de intercambio de información sin validar nivel de acceso o clasificación.*
14. **Uso de métodos inseguros para el intercambio de información:** *Riesgo de pérdida de confidencialidad e integridad durante el envío de información digital.*
15. **Falta de trazabilidad del intercambio de información con terceros:** *Riesgo de no contar con evidencia del envío, recepción y autorización del intercambio.*

6. Riesgos asociados al SUBPROCESO
Intercambio de Información Física

16. **Pérdida o extravío de documentación física:** *Riesgo durante el transporte, entrega o custodia de documentos institucionales.*
17. **Acceso no autorizado a información física clasificada:** *Riesgo por fallas en los controles de acceso y custodia documental.*

7. Riesgos asociados al SUBPROCESO
Control de Documentos y Archivo Clínico / Administrativo

18. **Uso de documentos obsoletos o no controlados:** *Riesgo de aplicación de versiones incorrectas de documentos institucionales.*
19. **Pérdida, deterioro o extravío de historias clínicas:** *Riesgo que afecta la continuidad asistencial, la seguridad del paciente y el cumplimiento normativo.*
20. **Acceso indebido a archivos clínicos y administrativos:** *Riesgo de violación de la confidencialidad de la información.*

8. Riesgos asociados a Hardware, Software y Uso de Tecnología

21. **Infección por malware o virus informáticos:** *Riesgo por uso indebido de dispositivos externos, navegación insegura o descargas no autorizadas.*
22. **Uso no autorizado de software o licencias ilegales:** *Riesgo legal, operativo y de seguridad de la información.*
23. **Pérdida o robo de equipos informáticos o dispositivos móviles:** *Riesgo de fuga de información y afectación de la disponibilidad.*

Cra 5 N° 8-36 - Tel: 3502702807
E-Mail: hospital.mistrato@hsvpmistrato.gov.co
Mistrató Risaralda

13. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

La entidad establece controles organizacionales orientados a garantizar la adecuada gestión de la seguridad y privacidad de la información, mediante la adopción de una política formal de seguridad, la definición de roles y responsabilidades, la implementación de procedimientos para la creación, modificación y retiro de usuarios, la suscripción de acuerdos de confidencialidad con funcionarios, contratistas y terceros, la gestión de incidentes de seguridad de la información, el control de cambios en los sistemas de información, la formulación de planes de continuidad del negocio y recuperación ante desastres, la definición de políticas de uso aceptable de los recursos tecnológicos, la aplicación de lineamientos para la limpieza de escritorio y pantalla, la clasificación y manejo de la información, la ejecución de auditorías internas y la actualización periódica de la gestión de riesgos de seguridad de la información.

En materia de control de accesos, la institución implementa mecanismos de autenticación mediante credenciales individuales, asigna privilegios de acceso con base en perfiles y funciones, establece el bloqueo automático de sesiones por inactividad, asegura la eliminación oportuna de accesos de usuarios desvinculados, aplica lineamientos para la gestión segura de contraseñas, mantiene registros y monitoreo de accesos a los sistemas de información y controla el acceso físico a áreas críticas como archivo, centros de cómputo y dependencias administrativas, garantizando la custodia de llaves, tarjetas o códigos de acceso.

Respecto a los controles tecnológicos asociados a hardware y software, se adoptan medidas de protección mediante el uso de herramientas de seguridad informática actualizadas, la implementación de controles perimetrales de red, la restricción del uso de dispositivos de almacenamiento externos, la actualización periódica de sistemas operativos y aplicaciones, el uso de software debidamente licenciado, el monitoreo del funcionamiento de equipos críticos, la protección frente a variaciones eléctricas, la administración de inventarios de activos tecnológicos y la eliminación segura de información contenida en equipos dados de baja.

En relación con la disponibilidad y recuperación de la información, la entidad desarrolla procesos de generación periódica de copias de respaldo, define responsables para su ejecución, asegura el almacenamiento en medios protegidos, realiza verificaciones de la ejecución de los respaldos, efectúa pruebas de restauración, controla el acceso a los medios de almacenamiento y aplica mecanismos de protección adicionales cuando la naturaleza de la información lo requiere.
Para el intercambio de información, se establecen lineamientos que garantizan el uso de canales institucionales, la restricción del envío de información sensible por medios no

Cra 5 N° 8-36 - Tel: 3502702807
E-Mail: hospital.mistrato@hsvpmistrato.gov.co
Mistrató Risaralda

autorizados, la autorización previa para la entrega de información a terceros, la trazabilidad de los intercambios, la protección de la información transmitida por medios electrónicos y la custodia adecuada de la documentación física durante su traslado.

En lo relacionado con la gestión documental y archivo clínico, se aplican controles orientados a la custodia segura de las historias clínicas y demás documentos institucionales, el control de préstamos, la restricción de accesos a áreas de archivo, la digitalización controlada de documentos, la aplicación de las tablas de retención documental y la protección frente a factores ambientales que puedan deteriorar la información.

Frente al factor humano, la institución desarrolla acciones de capacitación y sensibilización en seguridad de la información, confidencialidad y protección de datos personales, procesos de inducción y reinducción, supervisión del personal externo, aplicación de medidas disciplinarias ante incidentes de seguridad y habilitación de canales para el reporte de eventos o debilidades en los controles de seguridad.

Se implementan controles orientados al monitoreo y la mejora continua mediante el seguimiento a indicadores, el registro y análisis de incidentes, la evaluación de la efectividad de los controles, la actualización periódica del análisis de riesgos y la formulación de planes de mejora derivados de auditorías, eventos o cambios en el entorno institucional.

14. PLAN DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La E.S.E. establece el presente Plan de Respuesta a Incidentes de Seguridad de la Información con el propósito de garantizar una actuación oportuna, coordinada y eficaz frente a eventos que puedan comprometer la disponibilidad, integridad o confidencialidad de la información institucional, asegurando la continuidad de los servicios asistenciales y administrativos, el cumplimiento normativo y la protección de los datos personales.

El plan aplica a todos los funcionarios, contratistas, estudiantes, proveedores y terceros que tengan acceso a la información, a los sistemas de información o a los activos tecnológicos de la entidad, independientemente del medio en el que se procese, almacene o transmita la información, ya sea físico o digital.

Se considera incidente de seguridad de la información cualquier evento real o potencial que implique pérdida, robo, acceso no autorizado, divulgación indebida, alteración, destrucción o indisponibilidad de la información, así como fallas en los sistemas de información, ataques informáticos, uso indebido de credenciales, infecciones por software malicioso, extravío de equipos o documentación, y cualquier situación que represente una amenaza para los

Cra 5 N° 8-36 - Tel: 3502702807
E-Mail: hospital.mistrato@hsvpmistrato.gov.co
Mistrató Risaralda

activos de información del hospital.

La gestión de los incidentes se desarrolla bajo un enfoque de mejora continua y comprende las fases de identificación, notificación, análisis, contención, erradicación, recuperación y cierre del incidente, garantizando la trazabilidad y el registro de cada evento atendido.

La identificación del incidente se realiza a partir del monitoreo de los sistemas de información, la detección de anomalías en los procesos, los reportes del personal o de terceros y los resultados de auditorías o controles internos. Todo funcionario o contratista que tenga conocimiento de un posible incidente debe reportarlo de manera inmediata a los canales institucionales definidos, garantizando la oportunidad en la atención y mitigación del riesgo.

Una vez notificado el incidente, se procede a su análisis y clasificación, determinando su naturaleza, alcance, activos afectados, impacto potencial o real sobre la información y los procesos institucionales, así como su nivel de criticidad. Con base en esta evaluación se definen las acciones de respuesta prioritarias y los responsables de su ejecución.

La contención del incidente busca limitar su propagación y reducir el impacto sobre los sistemas de información y los procesos asistenciales y administrativos. Esta fase puede incluir el aislamiento de equipos, la suspensión temporal de accesos, el bloqueo de cuentas, la desconexión de redes afectadas o la aplicación de controles de emergencia, garantizando siempre la seguridad del paciente y la continuidad de los servicios críticos.

Posteriormente, se desarrollan acciones de erradicación orientadas a eliminar la causa raíz del incidente, lo cual puede implicar la eliminación de software malicioso, la corrección de configuraciones, la actualización de sistemas, el fortalecimiento de controles de acceso o la aplicación de medidas disciplinarias cuando corresponda.

La fase de recuperación tiene como objetivo restablecer los servicios, sistemas y procesos afectados, asegurando que la información se encuentre íntegra, disponible y protegida antes de su reincorporación a los entornos productivos. En esta etapa se pueden utilizar copias de respaldo verificadas y se realizan pruebas que confirmen la correcta operación de los sistemas.

Una vez superado el incidente, se procede al cierre formal del mismo, documentando las acciones realizadas, los impactos generados, las lecciones aprendidas y las recomendaciones para prevenir la recurrencia de eventos similares. Esta información alimenta el proceso de gestión de riesgos y los planes de mejora institucional.

La entidad garantiza el registro y custodia de la información relacionada con los incidentes de seguridad, manteniendo la confidencialidad de los datos involucrados y asegurando su disponibilidad para procesos de auditoría, control interno o requerimientos de autoridades competentes.

El Plan de Respuesta a Incidentes es objeto de evaluación periódica, actualización y socialización, considerando cambios en los procesos, en la tecnología, en la normatividad vigente y en el contexto institucional, con el fin de fortalecer la capacidad de respuesta del hospital frente a eventos que puedan afectar la seguridad de la información.

15. PLAN DE CONTINUIDAD Y RECUPERACIÓN DE LOS SERVICIOS Y DE LA INFORMACIÓN

La E.S.E. adopta el presente Plan de Continuidad y Recuperación con el propósito de garantizar la prestación ininterrumpida de los servicios asistenciales y administrativos críticos, así como la protección de la información institucional, frente a eventos que puedan afectar la operación normal de la entidad, tales como fallas tecnológicas, incidentes de seguridad de la información, emergencias físicas o eventos naturales

El plan aplica a todos los procesos institucionales, con especial énfasis en los procesos misionales, estratégicos y de apoyo que dependen de los sistemas de información, de la infraestructura tecnológica y de la disponibilidad del recurso humano, y es de obligatorio cumplimiento para funcionarios, contratistas y terceros que intervienen en la operación del hospital.

La continuidad del negocio se fundamenta en la identificación de los procesos críticos cuya interrupción podría generar impactos significativos sobre la atención en salud, la seguridad del paciente, el cumplimiento normativo, la sostenibilidad financiera y la imagen institucional. Para cada uno de estos procesos se definen tiempos máximos tolerables de interrupción, niveles aceptables de operación y recursos mínimos requeridos para su restablecimiento.

La entidad establece medidas preventivas orientadas a reducir la probabilidad de interrupciones, mediante el mantenimiento periódico de la infraestructura tecnológica, la actualización de los sistemas de información, la protección de los activos físicos y digitales, la capacitación del personal, la gestión de riesgos y la implementación de controles de seguridad de la información.

Cra 5 N° 8-36 - Tel: 3502702807
E-Mail: hospital.mistrato@hsvpmistrato.gov.co
Mistrató Risaralda

Ante la materialización de un evento que afecte la operación, se activa el plan de continuidad, el cual contempla la notificación inmediata a la alta dirección y a los responsables de los procesos afectados, la evaluación del impacto del evento, la priorización de los servicios críticos y la ejecución de acciones de contingencia que permitan mantener o restablecer la operación en condiciones seguras.

Las acciones de recuperación están orientadas a restablecer los sistemas de información, la infraestructura tecnológica y los procesos institucionales en los tiempos definidos, garantizando la integridad, disponibilidad y confidencialidad de la información. Para ello, la entidad dispone de mecanismos de respaldo de información, procedimientos de restauración, recursos alternos de operación y estrategias de recuperación gradual de los servicios.

Durante la fase de recuperación se realizan verificaciones técnicas y operativas que aseguren que los sistemas y procesos se encuentren en condiciones adecuadas antes de su reincorporación total a la operación normal, minimizando el riesgo de reincidencia del evento o de afectaciones adicionales.

Una vez superada la contingencia, la entidad ejecuta el proceso de retorno a la normalidad, el cual incluye la desactivación progresiva de las medidas temporales, la normalización de los procesos, la validación de la información recuperada y la comunicación a los usuarios internos y externos sobre el restablecimiento de los servicios.

El plan contempla el registro y documentación de los eventos que activen la continuidad y recuperación, así como el análisis de las causas, impactos y lecciones aprendidas, con el fin de fortalecer los controles, ajustar los procedimientos y mejorar la capacidad de respuesta institucional.

La evaluación del Plan de Continuidad y Recuperación se realiza de manera periódica mediante pruebas, simulacros, auditorías y revisiones, garantizando su actualización frente a cambios en los procesos, en la infraestructura tecnológica, en la normatividad vigente y en el contexto del hospital.

La alta dirección es responsable de garantizar la adopción, difusión, seguimiento y mejora continua del presente plan, asegurando su articulación con el Sistema de Gestión de la Calidad, el Modelo Integrado de Planeación y Gestión y el Modelo de Seguridad y Privacidad de la Información.

16. ACUERDO DE CONFIDENCIALIDAD

La E.S.E. ha dispuesto un Acuerdo de Confidencialidad con el fin de garantizar la adecuada protección, reserva y uso responsable de la información institucional y de los datos personales a los que se tenga acceso en el ejercicio de las funciones. Este documento es de obligatorio cumplimiento para todos los servidores públicos, contratistas y demás personas que, por razón de su vínculo con la entidad, manejen información sensible, y hará parte integral del presente documento como anexo.

17. SEGURIDAD DEL REPOSITORIO INSTITUCIONAL DE DOCUMENTOS

Con el fin de garantizar la protección, integridad, disponibilidad y confidencialidad de la información institucional, el Hospital implementará controles de seguridad asociados al Repositorio Institucional Virtual de Documentos, el cual será la herramienta oficial para la custodia y consulta de la documentación del Sistema de Gestión Institucional.

Este repositorio podrá operar a través de una plataforma segura en la nube y/o mediante una carpeta compartida en el servidor institucional con posibilidad de acceso remoto controlado, asegurando que la información se encuentre centralizada y protegida frente a pérdidas, alteraciones no autorizadas o uso de versiones no oficiales.

1. Control de accesos

Se establecerán perfiles de usuario diferenciados, bajo el principio de mínimo privilegio:

- Permiso de edición: exclusivo para el Líder del Proceso de Calidad, quien será el responsable de cargar, actualizar, reemplazar versiones y mantener la coherencia documental.
- Permiso de consulta: otorgado a funcionarios y contratistas únicamente para visualización, lectura y descarga de documentos, sin posibilidad de modificación o eliminación.

Estos controles buscan prevenir cambios no autorizados, pérdida de información o manipulación indebida de documentos oficiales.

2. Integridad de la información

Todos los documentos disponibles en el repositorio corresponderán a versiones oficiales aprobadas. La actualización de documentos deberá realizarse bajo los lineamientos del Sistema de Gestión de Calidad, asegurando:

- Control de versiones
- Identificación clara de documentos vigentes y obsoletos
- Trazabilidad de actualizaciones realizadas

3. Disponibilidad

El área de Tecnologías de la Información garantizará que el repositorio cuente con mecanismos que favorezcan la disponibilidad de la información, tales como:

- Acceso remoto seguro para usuarios autorizados
- Respaldo periódico de la información almacenada
- Monitoreo básico de funcionamiento del servicio de almacenamiento

4. Responsabilidades

- Líder de Calidad: Administración funcional del repositorio, control de versiones y validación de documentos cargados.
- Área de Tecnologías de la Información: Administración técnica de la plataforma o servidor, configuración de permisos de acceso, respaldo de la información y soporte tecnológico.
- Usuarios institucionales: Uso adecuado de la información consultada y cumplimiento de las políticas de seguridad y confidencialidad.

5. Riesgos que se mitigan con este componente

- Uso de documentos desactualizados
- Pérdida de información institucional
- Modificación no autorizada de documentos oficiales
- Dispersión de la información en medios no controlados

18. ESTRATEGIAS POR EJECUTAR PARA CUMPLIR EL PLAN DE TRATAMIENTO DE RIESGOS Y SEGURIDAD DE LA INFORMACIÓN – VIGENCIA 2026

ACTIVIDADES PROGRAMADAS	META O PRODUCTO	RESPONSABLE	FECHA PROGRAMADA
Actualización y validación del inventario de activos de información, incluyendo activos físicos y digitales	100 % de los activos de información identificados, clasificados y valorados según criterios de confidencialidad, integridad y disponibilidad	Responsable de Sistemas	Enero – Marzo 2026
Revisión y actualización del mapa de riesgos de	Mapa de riesgos de seguridad de la información	Control Interno y Responsable de Sistemas	Febrero 2026

Cra 5 N° 8-36 - Tel: 3502702807
E-Mail: hospital.mistrato@hsvpmistrato.gov.co
Mistrató Risaralda

seguridad de la información, priorizando riesgos altos y extremos	actualizado y aprobado		
Implementación y fortalecimiento de controles técnicos y administrativos para el tratamiento de riesgos priorizados	100 % de los riesgos altos y extremos con controles definidos y documentados	Responsable de Sistemas	Marzo – Diciembre 2026
Socialización del Plan de Tratamiento de Riesgos y Seguridad de la Información a todo el personal	100 % del personal institucional informado y sensibilizado sobre el plan	Responsable de Sistemas	Marzo 2026
Capacitación al personal en riesgos de seguridad de la información, protección de datos personales y buenas prácticas digitales	Al menos 90 % del personal capacitado	Responsable de Sistemas	Abril – Mayo 2026
Implementación y seguimiento del Plan de Respuesta a Incidentes de Seguridad de la Información	100 % de los incidentes registrados, atendidos y documentados conforme al procedimiento	Responsable de Sistemas	Permanente – 2026
Ejecución y verificación periódica de copias de respaldo de la información institucional	100 % de respaldos realizados y verificados según el plan de copias de seguridad	Área de Sistemas	Diario – 2026
Realización de pruebas de restauración de información y validación de la efectividad del plan de	Al menos una prueba semestral de restauración documentada y exitosa	Área de Sistemas	Junio y Noviembre 2026

continuidad y recuperación			
Revisión periódica de usuarios y privilegios de acceso a los sistemas de información	100 % de usuarios activos y retirados revisados y actualizados	Área de Sistemas – facturación	Mensual – 2026
Seguimiento bimestral a los riesgos residuales y a la efectividad de los controles implementados	Informes bimestrales de seguimiento a riesgos y controles	Control Interno y Sistemas	Bimestral – 2026
Ejecución de auditorías internas relacionadas con la seguridad de la información	100 % de auditorías programadas ejecutadas	Control Interno	Segundo semestre 2026
Formulación, ejecución y cierre de acciones de mejora derivadas del monitoreo y auditorías	Al menos 90 % de acciones de mejora cerradas dentro del plazo establecido	Responsables de proceso	Permanente – 2026

19. MONITOREO, AUDITORÍA Y MEJORA CONTINUA

La E.S.E. implementa un proceso permanente de monitoreo, auditoría y mejora continua con el fin de evaluar la eficacia de los controles de seguridad de la información, la adecuada ejecución de los planes de respuesta a incidentes y de continuidad y recuperación, así como el cumplimiento de la normatividad vigente y de los lineamientos institucionales, garantizando la protección de la disponibilidad, integridad y confidencialidad de la información.

El monitoreo se realiza de manera sistemática sobre los activos de información, los sistemas tecnológicos y los procesos institucionales, mediante el seguimiento a indicadores definidos, la revisión de registros, bitácoras y reportes, la supervisión del acceso a los sistemas de información y la identificación oportuna de eventos o comportamientos

anómalos que puedan representar riesgos para la entidad.

La auditoría interna constituye un mecanismo fundamental de verificación y control, orientado a evaluar el cumplimiento de políticas, procedimientos y controles de seguridad de la información, así como la efectividad de las acciones implementadas para la gestión de riesgos. Estas auditorías se desarrollan de acuerdo con el plan anual de auditorías institucional, en articulación con el Sistema de Gestión de la Calidad, el PAMEC y el Sistema de Control Interno, y permiten identificar conformidades, no conformidades, oportunidades de mejora y riesgos emergentes.

Los resultados del monitoreo y de las auditorías son analizados por los responsables de los procesos y por la alta dirección, con el propósito de definir acciones correctivas, preventivas y de mejora, priorizadas de acuerdo con el nivel de riesgo, el impacto institucional y la criticidad de los procesos afectados.
La mejora continua se materializa a través de la formulación, ejecución y seguimiento de planes de mejora, los cuales incluyen actividades específicas, responsables, plazos e indicadores de cumplimiento, orientados a fortalecer los controles de seguridad de la información, optimizar los procesos, reducir la ocurrencia de incidentes y mejorar la capacidad de respuesta del hospital.

La entidad promueve la cultura de mejora continua mediante la capacitación permanente del personal, la socialización de los resultados de auditorías e incidentes relevantes, la actualización de políticas y procedimientos, y la incorporación de lecciones aprendidas derivadas de eventos, simulacros y evaluaciones periódicas.

El proceso de monitoreo, auditoría y mejora continua es objeto de revisión periódica, considerando cambios en el entorno normativo, tecnológico y organizacional, así como los resultados de la gestión del riesgo, con el fin de asegurar la pertinencia, suficiencia y efectividad del Sistema de Seguridad de la Información y su alineación con los objetivos institucionales.

20. INDICADORES DE CUMPLIMIENTO DEL PLAN

Proceso / Componente	Indicador	Descripción	Fórmula	Meta	Periodicidad	Responsable
Seguridad de la Información	Cumplimiento de políticas y procedimie	Mide el grado de formalización,	(Número de políticas y procedimientos vigentes /	≥ 95 %	Anual	Gerencia / Sistemas

	ntos de seguridad	aprobación y vigencia de las políticas y procedimientos de seguridad de la información	Total de políticas y procedimientos requeridos) × 100			
Gestión de Riesgos	Riesgos de seguridad de la información evaluados	Mide el porcentaje de riesgos identificados que cuentan con evaluación de probabilidad e impacto	(Número de riesgos evaluados / Total de riesgos identificados) × 100	100 %	Anual	Control interno / Sistemas
Gestión de Riesgos	Riesgos con plan de tratamiento	Mide el porcentaje de riesgos priorizados que cuentan con plan de tratamiento definido	(Número de riesgos con plan de tratamiento / Total de riesgos priorizados) × 100	≥ 90 %	Semestral	Sistemas / Planeación
Gestión de Incidentes	Oportunidad en la atención de incidentes	Mide el porcentaje de incidentes atendidos dentro del tiempo establecido	(Incidentes atendidos oportunamente / Total de incidentes reportados) × 100	≥ 90 %	Trimestral	Sistemas
Gestión de Incidentes	Incidentes de seguridad cerrados	Evalúa el cierre formal de incidentes con registro y análisis de causa	(Incidentes cerrados / Total de incidentes reportados) × 100	100 %	Trimestral	Sistemas
Continuid	Disponibilid	Mide el	(Tiempo	≥	Mensual	Sistemas

ad del Servicio	ad de sistemas críticos	tiempo de disponibilidad de los sistemas de información críticos	disponible / Tiempo total del período) × 100	99 %		
Copias de Respaldo	Cumplimiento del plan de respaldos	Evalúa la ejecución efectiva de las copias de seguridad programadas	(Respaldos realizados / Respaldos programados) × 100	100 %	Mensual	Sistemas
Copias de Respaldo	Pruebas de restauración exitosas	Mide el porcentaje de pruebas de restauración realizadas con éxito	(Pruebas exitosas / Total de pruebas realizadas) × 100	≥ 95 %	Semestral	Sistemas
Control de Accesos	Usuarios con accesos revisados	Mide el porcentaje de usuarios con revisión periódica de privilegios de acceso	(Usuarios revisados / Total de usuarios activos) × 100	≥ 95 %	Semestral	Sistemas – facturación
Control de Accesos	Retiro oportuno de accesos	Evalúa la eliminación o bloqueo de accesos de personal desvinculado	(Accesos retirados oportunamente / Total de desvinculaciones) × 100	100 %	Mensual	Sistemas – facturación nto
Capacitación	Personal capacitado en seguridad de la información	Mide el porcentaje de funcionarios capacitado	(Funcionarios capacitados / Total de funcionarios) × 100	≥ 90 %	Anual	Sistemas

		s en políticas y controles de seguridad				
Auditoría	Cumplimiento del plan de auditorías	Evalúa la ejecución del plan anual de auditorías relacionadas con seguridad de la información	(Auditorías realizadas / Auditorías programadas) × 100	100 %	Anual	Control Interno
Mejora Continua	Acciones de mejora implementadas	Mide el porcentaje de acciones de mejora cerradas dentro del plazo	(Acciones cerradas / Acciones formuladas) × 100	≥ 90 %	Trimestral	Responsables de proceso

21. RESPONSABLES DEL PLAN

Rol / Cargo	Responsabilidad dentro del Plan
Gerente de la E.S.E.	Aprobar el Plan de tratamiento de riesgos y seguridad de la información de la Información, garantizar la asignación de recursos necesarios, liderar la toma de decisiones estratégicas frente a incidentes críticos y asegurar la articulación del plan con los objetivos institucionales.
Profesional universitario	Apoyar la implementación del plan, garantizar la disponibilidad de recursos administrativos y financieros, y supervisar el cumplimiento de las acciones definidas en los planes de mejora.
Responsable de Sistemas / TIC	Coordinar la implementación técnica del plan, administrar los controles de seguridad, gestionar los incidentes de seguridad de la información, ejecutar y verificar las copias de respaldo, activar los planes de continuidad y recuperación y realizar el monitoreo de los sistemas de información.
Responsable de	Articular el plan con el MIPG, la gestión del riesgo institucional

Planeación	y los planes estratégicos, realizar seguimiento a los indicadores de cumplimiento y apoyar la formulación y evaluación de los planes de mejora.
Control Interno	Evaluar el cumplimiento del plan mediante auditorías, verificar la efectividad de los controles, emitir recomendaciones y realizar seguimiento a las acciones correctivas, preventivas y de mejora.
Responsable de Archivo Clínico y Gestión Documental	Garantizar la custodia, confidencialidad y control de acceso a la información física y documental, aplicar las tablas de retención documental y apoyar la respuesta ante incidentes que involucren información clínica o administrativa.
Líderes de Proceso	Implementar y cumplir los controles definidos en el plan dentro de sus procesos, reportar oportunamente incidentes de seguridad, participar en las acciones de mejora y garantizar el uso adecuado de la información bajo su responsabilidad.
Funcionarios y Contratistas y demás colaboradores	Cumplir las políticas y procedimientos de seguridad de la información, proteger los activos de información asignados, reportar incidentes o debilidades de seguridad y participar en las capacitaciones institucionales.
Proveedores y Terceros	Cumplir las cláusulas de confidencialidad y seguridad de la información establecidas en los contratos, utilizar la información únicamente para los fines autorizados y reportar incidentes que puedan afectar a la entidad.

OLGA PATRICIA COLORADO PUERTA
Gerente

Cra 5 N° 8-36 - Tel: 3502702807
E-Mail: hospital.mistrato@hsvpmistrato.gov.co
Mistrató Risaralda

22. BIBLIOGRAFÍA

- Colombia. Congreso de la República. (2009, 30 de julio). *Ley 1341 de 2009*. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
- Colombia. Congreso de la República. (2012, 17 de octubre). *Ley 1581 de 2012*. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Colombia. Congreso de la República. (2014, 6 de marzo). *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. Diario Oficial No. 49.101. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=57939
- Colombia. Congreso de la República. (2020, 13 de febrero). *Ley 2015 de 2020*. Por medio de la cual se crea la historia clínica electrónica interoperable y se dictan otras disposiciones.
- Colombia. Ministerio de Tecnologías de la Información y las Comunicaciones. (2023). *Plan Estratégico de Tecnologías de la Información (PETI) 2023-2026*. https://www.mintic.gov.co/portal/715/articles-274095_recurso_1.pdf
- Colombia. Ministerio de Tecnologías de la Información y las Comunicaciones. (2023, 29 de diciembre). *Resolución 1978 de 2023*. Por la cual se adopta la versión 3 del Marco de Referencia de Arquitectura Empresarial para el Estado Colombiano. Colombia. Presidencia de la República. (2015, 26 de mayo). *Decreto 1078 de 2015*. Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Colombia. Presidencia de la República. (2018, 10 de abril). *Decreto 612 de 2018*. Por el cual se modifican los artículos 2.2.1.2.3, 2.2.1.2.6 y 2.2.1.2.7 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, sobre la incorporación del Plan Estratégico de Tecnologías de la Información – PETI, en el Plan de Acción Institucional.
- Colombia. Presidencia de la República. (2020, 21 de abril). *Decreto 620 de 2020*. Por el cual se reglamentan parcialmente aspectos de gobierno digital y servicios ciudadanos digitales dentro del Decreto Único Reglamentario del sector TIC.
- Colombia. Presidencia de la República. (2022, 21 de enero). *Decreto 088 de 2022*. Por el cual se reglamentan los conceptos, lineamientos y plazos para la digitalización y automatización de trámites.
- Colombia. Presidencia de la República. (2022, 9 de mayo). *Decreto 767 de 2022*. Por el cual se actualizan los lineamientos generales de la Política de Gobierno

Digital.

- Hospital San Vicente de Paúl de Mistrató. (2026). *Plan Estratégico de Tecnologías de la Información (PETI) 2026-2028*. ESE Hospital San Vicente de Paúl de Mistrató.