PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VIGENCIA 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

Tabla de contenido

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

CAPÍTULO 1
GENERALIDADES

INTRODUCCIÓN

La seguridad y privacidad de la información constituyen un pilar fundamental para la adecuada prestación de los servicios de salud y la gestión institucional de la E.S.E. HOSPITAL SAN VICENTE DE PAÚL DE MISTRATÓ. En el desarrollo de sus funciones misionales, estratégicas y de apoyo, la entidad administra información crítica y sensible que requiere ser protegida frente a riesgos asociados a la pérdida, alteración, acceso no autorizado, divulgación indebida o indisponibilidad, garantizando en todo momento la confidencialidad, integridad, disponibilidad y privacidad de los datos.

En un contexto de transformación digital y fortalecimiento de los sistemas de información en el sector salud, el hospital reconoce la necesidad de adoptar un enfoque estructurado y preventivo para la gestión de la seguridad de la información, que permita minimizar riesgos operativos, legales y reputacionales, y asegurar la continuidad de la atención en salud. La implementación del Modelo de Seguridad y Privacidad de la Información se concibe como una herramienta estratégica que articula los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones con el Modelo Integrado de Planeación y Gestión – MIPG y el Sistema de Control Interno.

Este documento establece el marco institucional para la implementación del Modelo de Seguridad y Privacidad de la Información en la E.S.E. HOSPITAL SAN VICENTE DE PAÚL DE MISTRATÓ, definiendo las acciones, responsabilidades y mecanismos de seguimiento necesarios para fortalecer la protección de los activos de información y el cumplimiento de la normativa vigente en materia de protección de datos personales y manejo de la historia clínica. Su aplicación contribuye a consolidar una cultura organizacional orientada al uso responsable de la información, al mejoramiento continuo de los procesos y a la protección de los derechos de los usuarios, funcionarios y demás grupos de interés.

JUSTIFICACIÓN

La E.S.E. HOSPITAL SAN VICENTE DE PAÚL DE MISTRATÓ administra información crítica y altamente sensible relacionada con la atención en salud de la población, la gestión administrativa, financiera y contractual, así como datos personales de usuarios, funcionarios y terceros. La adecuada protección de esta información es un requisito fundamental para garantizar la continuidad de los servicios de salud, la seguridad del paciente, la confianza

de la comunidad y el cumplimiento de la normativa vigente en materia de seguridad de la información y protección de datos personales.

La implementación del Modelo de Seguridad y Privacidad de la Información responde a la necesidad de fortalecer los controles institucionales frente a riesgos asociados a la pérdida, alteración, acceso no autorizado, divulgación indebida o indisponibilidad de la información, los cuales pueden generar impactos asistenciales, legales, financieros y reputacionales para la entidad. En un entorno cada vez más dependiente de los sistemas de información, la ausencia de un modelo estructurado incrementa la exposición del hospital a incidentes de seguridad que pueden afectar directamente la calidad y oportunidad de la atención en salud.

Este Plan de Implementación se justifica, además, en el cumplimiento de los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, el Modelo Integrado de Planeación y Gestión – MIPG, la Ley 1581 de 2012 sobre protección de datos personales, la normativa del sector salud relacionada con la historia clínica y las directrices del Sistema de Control Interno. Su adopción permite articular la seguridad y privacidad de la información con los procesos misionales, estratégicos y de apoyo del hospital, evitando enfoques aislados y promoviendo una gestión integral del riesgo.

La ejecución del Plan de Implementación con seguimiento mensual facilita la identificación temprana de brechas, el control permanente sobre los activos de información y la mejora continua del sistema, garantizando que las medidas adoptadas sean efectivas y sostenibles en el tiempo. Asimismo, promueve una cultura institucional de responsabilidad y uso adecuado de la información, reconociendo que el factor humano es uno de los principales determinantes en la ocurrencia de incidentes de seguridad.

La adopción del Modelo de Seguridad y Privacidad de la Información fortalece la gobernanza institucional, mejora la toma de decisiones basada en información confiable y protege los derechos fundamentales de los titulares de los datos, contribuyendo al logro de los objetivos estratégicos del HOSPITAL SAN VICENTE DE PAÚL DE MISTRATÓ y al cumplimiento de su misión de prestar servicios de salud seguros, humanizados y de calidad a la comunidad.

ALCANCE

El presente plan aplica a:

- Todos los funcionarios, contratistas, practicantes y terceros que tengan acceso a información institucional.
- Todos los procesos misionales, estratégicos y de apoyo.
- Toda la información generada, procesada o almacenada por la E.S.E., en formato físico o digital.
- Los sistemas de información **R-FAST - ANNARLAB**.

- La infraestructura tecnológica (servidores, red local, equipos de cómputo y dispositivos de almacenamiento).

OBJETIVO GENERAL

Implementar y fortalecer el Sistema de Seguridad y Privacidad de la Información de la E.S.E. HOSPITAL SAN VICENTE DE PAÚL DE MISTRATÓ, mediante la definición de lineamientos, controles y actividades que garanticen la confidencialidad, integridad, disponibilidad y privacidad de la información institucional, en cumplimiento del marco normativo vigente y los lineamientos del MinTIC.

OBJETIVOS ESPECÍFICOS

- Proteger los activos de información críticos del hospital.
- Garantizar el adecuado tratamiento de los datos personales y sensibles.
- Reducir los riesgos asociados a la gestión de la información digital y física.
- Fortalecer los controles de acceso a los sistemas de información institucionales.
- Establecer mecanismos de respuesta ante incidentes de seguridad.
- Promover la cultura de seguridad de la información entre los funcionarios.
- Asegurar la continuidad de los procesos misionales y de apoyo.

MARCO NORMATIVO Y REFERENCIAL

La implementación del Modelo de Seguridad y Privacidad de la Información en la E.S.E. HOSPITAL SAN VICENTE DE PAÚL DE MISTRATÓ se fundamenta en el cumplimiento del marco normativo vigente que regula la protección de la información, los datos personales, el uso de las tecnologías de la información y la gestión institucional en las entidades públicas del sector salud. Este marco normativo orienta la adopción de medidas administrativas, técnicas y organizacionales destinadas a salvaguardar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional.

Norma	Año	Ámbito de aplicación	Aspecto que regula	Aplicación en el HOSPITAL SAN VICENTE DE PAÚL DE MISTRATÓ
Constitución Política de Colombia – Artículo 15	1991	Nacional	Derecho fundamental al habeas data y a la intimidad	Obliga a garantizar la confidencialidad, actualización y protección de los datos personales y sensibles de usuarios, funcionarios y terceros
Ley 1581	2012	Nacional	Régimen general de protección de datos personales	Establece las obligaciones del hospital como responsable del tratamiento de datos personales y sensibles, incluyendo la adopción de

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

				medidas de seguridad
Decreto 1377	2013	Nacional	Reglamenta parcialmente la Ley 1581 de 2012	Define procedimientos para la recolección, almacenamiento, uso y supresión de datos personales en bases de datos institucionales
Ley 1712	2014	Nacional	Transparencia y acceso a la información pública	Garantiza el acceso a la información pública, protegiendo la información clasificada, reservada y los datos sensibles
Ley 87	1993	Nacional	Sistema de Control Interno	Exige la identificación, evaluación y control de riesgos institucionales, incluidos los riesgos de seguridad de la información
Resolución 1995	1999	Sector salud	Manejo de la historia clínica	Define la historia clínica como documento privado y reservado, estableciendo responsabilidades sobre su custodia, confidencialidad y acceso
Ley 1438	2011	Sector salud	Reforma al Sistema General de Seguridad Social en Salud	Refuerza la responsabilidad institucional en la gestión de la información para la continuidad y seguridad de la atención en salud
Decreto 1499	2017	Nacional	Modelo Integrado de Planeación y Gestión – MIPG	Integra la seguridad digital como elemento transversal de la gestión pública y del control del riesgo
Lineamientos MSPI – MinTIC	Vigente	Nacional	Modelo de Seguridad y Privacidad de la Información	Establece el marco metodológico para la gestión de la seguridad y privacidad de la información en entidades públicas
Ley 594	2000	Nacional	Ley General de Archivos	Regula la gestión documental,

				conservación, custodia y disposición de documentos físicos y electrónicos
Decreto 1078	2015	Nacional	Sector TIC	Compila la normativa relacionada con tecnologías de la información y comunicaciones en entidades públicas
Ley 1273	2009	Nacional	Protección de la información y los datos	Tipifica los delitos informáticos y protege la información y los sistemas de información
Lineamientos de Control Interno y Auditoría	Vigente	Institucional	Gestión del riesgo y control	Orientan la evaluación, seguimiento y mejora de los controles asociados a la seguridad de la información

CONTEXTO INSTITUCIONAL

La E.S.E. HOSPITAL SAN VICENTE DE PAÚL DE MISTRATÓ presta servicios de salud integrales en los ámbitos hospitalario y ambulatorio, apoyándose en sistemas de información clínicos y administrativos que soportan procesos críticos como admisión de usuarios, atención médica, historias clínicas, facturación, laboratorio clínico, imágenes diagnósticas, inventarios, contabilidad, cartera y presupuesto.

Actualmente, la institución utiliza, entre otros, los siguientes sistemas:

- **R-FAST:** Sistema integral de información hospitalaria, alojado en servidores propios.
- **ANNARLABS:** Sistema externo para gestión de laboratorio clínico.

La operación de estos sistemas, junto con la infraestructura tecnológica local y los procesos manuales asociados, demanda la implementación de controles adecuados para prevenir riesgos relacionados con la pérdida, alteración, acceso no autorizado o divulgación indebida de la información.

ESTADO ACTUAL DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La E.S.E. HOSPITAL SAN VICENTE DE PAÚL DE MISTRATÓ presenta los siguientes avances y brechas:

Avances

- Uso de sistemas de información integrales.
- Asignación de usuarios y contraseñas individuales en R-FAST y ANNARLABS.
- Copias de seguridad diarias de bases de datos y servidores.
- Existencia de roles formales como responsable de Seguridad de la Información y Administrador de Sistemas.

Brechas identificadas

- Política de seguridad de la información implementada de forma parcial.
- Ausencia de política formal de protección de datos personales.
- Usuario compartido en el sistema ANNARLABS.
- Inexistencia de comité formal de seguridad de la información.
- Falta de procedimiento documentado para gestión de incidentes.

CAPÍTULO 2
DESARROLLO DEL SISTEMA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PROCESO DE SEGURIDAD Y PRIVACIDAD

La seguridad y privacidad de la información se gestionará como un proceso transversal, integrado al sistema de gestión institucional, bajo un enfoque de mejora continua, identificación de riesgos y aplicación de controles preventivos y correctivos.

Política General

La E.S.E. HOSPITAL SAN VICENTE DE PAÚL DE MISTRATÓ se compromete a proteger la información institucional y los datos personales, garantizando su uso adecuado, acceso controlado y tratamiento conforme a la ley.

Objetivos Estratégicos

- Consolidar el sistema de seguridad de la información.
- Formalizar políticas y procedimientos.
- Fortalecer controles técnicos y administrativos.
- Mejorar la capacidad de respuesta ante incidentes.

ESTRATEGIAS Y MODELO DE OPERACIÓN

- Implementación gradual del MSPI.
- Fortalecimiento de controles de acceso.
- Capacitación del talento humano.
- Seguimiento periódico a riesgos.
- Articulación con control interno y calidad.

PORTAFOLIO DE ACTIVIDADES – VIGENCIA 2026

- Formalización de políticas institucionales.
- Elaboración y adopción del procedimiento de gestión de incidentes.
- Capacitación anual al personal.
- Evaluación y actualización de copias de seguridad.
- Seguimiento a riesgos de seguridad de la información.

MATRIZ PHVA – MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Proveedores (ENTRADAS)

La implementación del Modelo de Seguridad y Privacidad de la Información en el HOSPITAL SAN VICENTE DE PAÚL DE MISTRATÓ se nutre de lineamientos, normas, directrices técnicas y requerimientos provenientes de instancias internas y externas. Entre los principales proveedores de información y directrices se encuentran el Ministerio de Tecnologías de la Información y las Comunicaciones a través del Modelo de Seguridad y Privacidad de la Información, el Ministerio de Salud y Protección Social, el Departamento Administrativo de la Función Pública, los organismos de control, así como los procesos institucionales internos como Control Interno, Planeación, Sistemas, calidad, Talento Humano y Gestión Documental.

Estas entradas permiten orientar la planeación, ejecución, seguimiento y mejora continua de la seguridad de la información, garantizando coherencia normativa y operativa.

Planear (P)

El HOSPITAL SAN VICENTE DE PAÚL DE MISTRATÓ planifica la seguridad y privacidad de la información mediante la identificación de los activos de información críticos, la

clasificación de la información, la identificación y valoración de riesgos de seguridad y privacidad, y la definición de políticas, lineamientos y planes institucionales. En esta fase se establecen el Plan de Seguridad y Privacidad de la Información, el Plan de Implementación del MSPI, los roles y responsabilidades, así como la articulación con el MIPG, el Sistema de Control Interno y el Plan de Continuidad de la Operación.

La planeación considera las particularidades del entorno hospitalario, priorizando la protección de la historia clínica, los sistemas de información asistenciales, las bases de datos de usuarios y el soporte tecnológico necesario para garantizar la continuidad de la atención en salud.

Hacer (H)
En esta fase el hospital ejecuta las acciones definidas en la planeación, implementando los controles administrativos, técnicos y físicos necesarios para proteger la información. Se desarrollan actividades como la gestión de accesos a los sistemas de información, la aplicación de controles sobre la historia clínica física y electrónica, la implementación de copias de seguridad, la gestión de incidentes de seguridad de la información y la protección de los datos personales y sensibles.

Asimismo, se realizan procesos de capacitación y sensibilización al talento humano, se socializan las políticas de seguridad de la información y se asegura que los procedimientos institucionales incorporen prácticas seguras en el manejo de la información, tanto en los procesos asistenciales como administrativos.

Verificar (V)
El HOSPITAL SAN VICENTE DE PAÚL DE MISTRATÓ realiza el seguimiento y la medición permanente de la implementación del Modelo de Seguridad y Privacidad de la Información, mediante la revisión del cumplimiento de las actividades programadas, la medición de indicadores, la verificación del tratamiento de riesgos y el análisis de los incidentes de seguridad reportados.

Esta verificación se articula con las auditorías internas, el Control Interno, el PAMEC y los comités institucionales, permitiendo identificar desviaciones, debilidades o brechas en la gestión de la seguridad de la información. Los resultados del seguimiento se documentan y se reportan a la Gerencia para la toma de decisiones.

Actuar (A)
Con base en los resultados del seguimiento y la verificación, el hospital define e implementa acciones de mejora orientadas a fortalecer la seguridad y privacidad de la información. Estas acciones incluyen la actualización de políticas y procedimientos, el ajuste de controles de seguridad, la formulación de planes de mejora, el refuerzo de la capacitación al personal y la actualización del mapa de riesgos de seguridad de la información.

La fase de actuar permite consolidar un enfoque de mejora continua, asegurando que el Modelo de Seguridad y Privacidad de la Información se mantenga actualizado, pertinente y coherente con los cambios normativos, tecnológicos y organizacionales del HOSPITAL SAN

VICENTE DE PAÚL DE MISTRATÓ.

Salidas (Resultados)

Como resultado de la aplicación del ciclo PHVA, el HOSPITAL SAN VICENTE DE PAÚL DE MISTRATÓ obtiene lineamientos institucionales claros para la seguridad y privacidad de la información, riesgos de seguridad gestionados, incidentes controlados y documentados, personal sensibilizado, sistemas de información protegidos y mayor confiabilidad en la información utilizada para la atención en salud y la gestión administrativa.

Estas salidas contribuyen directamente al fortalecimiento de la seguridad del paciente, la continuidad de la operación, el cumplimiento normativo y la confianza de la comunidad en la institución.

GESTIÓN DE ACTIVOS DE INFORMACIÓN

La E.S.E. HOSPITAL SAN VICENTE DE PAÚL DE MISTRATÓ reconoce los activos de información como elementos esenciales para el cumplimiento de su misión institucional y la adecuada prestación de los servicios de salud. La clasificación de los activos de información permite establecer el nivel de protección requerido para cada tipo de información, priorizar la aplicación de controles de seguridad y garantizar el cumplimiento de los principios de confidencialidad, integridad, disponibilidad y privacidad.

La clasificación de los activos de información se realiza considerando la naturaleza de la información, el impacto que tendría su pérdida, alteración, acceso no autorizado o indisponibilidad, así como las obligaciones legales y normativas aplicables. Este proceso facilita la gestión del riesgo, orienta la asignación de responsabilidades y asegura un tratamiento diferenciado de la información según su nivel de sensibilidad.

Información clasificada como pública

Corresponde a la información cuya divulgación no genera afectación a los derechos de los usuarios, funcionarios o terceros, ni compromete la operación institucional. Incluye documentos e información que, por disposición legal, pueden ser conocidos por cualquier persona. Este tipo de información debe mantenerse íntegra y disponible, garantizando su actualización y acceso oportuno.

Ejemplos de información pública incluyen informes de gestión, planes institucionales publicados, manuales generales, información contractual disponible en plataformas oficiales y datos estadísticos agregados que no permiten la identificación de personas. Aunque su nivel de confidencialidad es bajo, requiere controles que aseguren su integridad y disponibilidad, evitando alteraciones no autorizadas o pérdidas de información.

Información clasificada como de uso interno

Incluye la información generada para la gestión interna del hospital, cuyo acceso está restringido al talento humano autorizado y cuyo uso está directamente relacionado con la operación administrativa y asistencial. La divulgación no autorizada de esta información puede generar impactos operativos, administrativos o reputacionales, aunque no

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

necesariamente vulnera derechos fundamentales de los titulares de datos.
En esta categoría se encuentran documentos administrativos internos, procedimientos, actas de reuniones, informes de seguimiento, comunicaciones internas, reportes operativos y registros de apoyo a la gestión. Esta información requiere controles de acceso basados en roles, mecanismos de custodia adecuados y lineamientos claros para su almacenamiento y transmisión.

Información clasificada como confidencial
Comprende la información cuyo acceso está estrictamente limitado y cuya divulgación no autorizada puede generar consecuencias legales, administrativas o asistenciales para la entidad. Incluye información que, por su naturaleza, debe ser protegida para preservar la confianza institucional y el cumplimiento normativo.

En esta clasificación se ubican los datos personales de usuarios y funcionarios, la información financiera detallada, los registros de talento humano, contratos, procesos disciplinarios, información estratégica y los sistemas de información que soportan procesos críticos. Este tipo de información requiere controles reforzados de acceso, autenticación individual, trazabilidad de uso y mecanismos de almacenamiento seguro.

Información clasificada como sensible o crítica
Corresponde a la información que, por su naturaleza, está sujeta a reserva legal y cuyo tratamiento indebido puede afectar gravemente los derechos fundamentales de los titulares o la continuidad de la atención en salud. En el contexto del hospital, esta categoría incluye principalmente la historia clínica y toda la información relacionada con el estado de salud de los usuarios.

La información sensible o crítica requiere el más alto nivel de protección, garantizando acceso exclusivo al personal autorizado, uso únicamente para fines asistenciales, administrativos o legales debidamente justificados, y la implementación de controles técnicos, administrativos y físicos robustos. La pérdida, alteración o divulgación indebida de esta información constituye un incidente grave de seguridad y debe ser gestionada conforme a los procedimientos institucionales.

Criterios de clasificación de los activos de información
La clasificación de los activos de información se basa en criterios que permiten evaluar el impacto potencial de un incidente de seguridad. Se consideran, entre otros, la afectación a la continuidad del servicio de salud, el impacto legal y sancionatorio, la afectación a los derechos de los titulares de la información, el impacto financiero y el daño reputacional para la entidad.

Responsabilidad y actualización de la clasificación
Cada activo de información cuenta con un responsable designado, quien debe velar por su adecuada clasificación, uso y protección. La clasificación de los activos de información se revisa y actualiza de manera periódica o cuando se presentan cambios normativos, tecnológicos u organizacionales, garantizando que los controles de seguridad se mantengan acordes con la realidad institucional y los riesgos identificados.

Clasificación de activos de información

Activo de información	Tipo de información	Clasificación	Impacto ante pérdida o divulgación	Controles de seguridad aplicables	Nivel de protección	Responsable
Historia clínica física	Datos sensibles en salud	Sensible / Crítica	Afectación directa a derechos fundamentales del usuario, sanciones legales y riesgo para la seguridad del paciente	Acceso restringido, custodia física, control de préstamo, confidencialidad del personal	Muy alto	Coordinación Médica / SIAU / Facturación
Historia clínica electrónica	Datos sensibles en salud	Sensible / Crítica	Riesgo legal, asistencial y reputacional	Usuarios individuales, perfiles de acceso, trazabilidad, copias de seguridad	Muy alto	Sistemas / Coordinación Médica / Facturación
Sistema R-FAST	Información clínica y administrativa	Confidencial	Indisponibilidad del servicio, errores en atención y facturación	Control de accesos, respaldos periódicos, monitoreo de disponibilidad	Alto	Sistemas / Facturación
Sistema ANNARLABS	Información administrativa	Confidencial	Impacto operativo	Perfiles por rol, autenticación individual, copias de seguridad	Alto	Sistemas / Laboratorio
Base de datos de usuarios	Datos personales	Confidencial	Vulneración de habeas data,	Autorizaciones, control de accesos, almacenam	Alto	Facturación

			sanciones legales	iento seguro		
Base de datos de talento humano	Datos personales	Confidencial	Afectación laboral y legal	Accesos restringidos, custodia documental, control de usuarios	Alto	Talento Humano
Nómina	Datos personales y financieros	Confidencial	Impacto financiero y reputacional	Restricción de acceso, respaldo de información, custodia documental	Alto	Talento Humano
Contratos y estudios previos	Información administrativa y contractual	Confidencial	Riesgo jurídico y financiero	Control documental, accesos por rol, archivo seguro	Medio – Alto	Jurídica / Contratación
Informes financieros	Información financiera	Confidencial	Impacto fiscal y de control	Acceso restringido, respaldo periódico	Medio – Alto	Financiera
Planes institucionales	Información institucional	Pública	Bajo impacto	Control de versiones, publicación oficial	Básico	Planeación / gerencia / control interno
Informes de gestión	Información institucional	Pública	Bajo impacto	Custodia documental, control de integridad	Básico	Planeación / gerencia / control interno / Líderes de procesos
Actas de comité	Información interna	Uso interno	Impacto administrativo	Acceso restringido al personal autorizado	Medio	Secretaría Técnica de cada comité
Correos institucionales	Información administrativa	Uso interno	Riesgo de fuga de información	Políticas de uso, control de accesos	Medio	Sistemas

Equipos de cómputo	Soporte de información	Confidencial	Pérdida de información institucional	Contraseñas, bloqueo, control de inventario	Medio – Alto	Sistemas
Dispositivos de almacenamiento	Soporte de información	Confidencial	Fuga o pérdida de información	Restricción de uso, cifrado, control físico	Alto	Sistemas

GESTIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La gestión de riesgos de seguridad y privacidad de la información se desarrolla de forma articulada con el mapa de riesgos institucional y el Sistema de Control Interno, permitiendo identificar amenazas, vulnerabilidades y eventos que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de la información. El hospital prioriza riesgos asociados a la operación asistencial, el manejo de historias clínicas y el uso de sistemas de información críticos.

Entre los principales riesgos identificados se encuentran el acceso no autorizado a historias clínicas, el uso de usuarios compartidos en sistemas externos, la pérdida de información por fallas técnicas, el robo o daño de equipos de cómputo, errores humanos en el registro de información clínica y la divulgación indebida de datos personales. Para cada riesgo se definen controles administrativos, técnicos y físicos, así como acciones de tratamiento que permiten reducir su probabilidad de ocurrencia o mitigar su impacto sobre la atención en salud.

Riesgo de seguridad	Activo de información	Vulnerabilidad identificada	Amenaza	Consecuencia institucional	Nivel de riesgo	Controles preventivos	Tratamiento del riesgo
Acceso indebido a información clínica	Historia clínica electrónica	Usuarios compartidos, contraseñas débiles	Uso no autorizado	Vulneración de derechos, sanciones legales, riesgo asistencial	Alto	Usuarios individuales, perfiles por rol	Eliminación de usuarios genéricos y fortalecimiento de autenticación
Divulgación no	Bases de datos	Falta de cultura de	Error human	Incumplimiento	Alto	Políticas de	Capacitación

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

autorizada de datos personales	de usuarios	seguridad	o	legal y daño reputacional		confidencialidad	periódica
Indisponibilidad de sistemas críticos	R-FAST, ANNAR LABS	Ausencia de plan de contingencia	Fallas técnicas	Interrupción de la atención en salud	Alto	Soporte técnico básico	Plan de contingencia tecnológica
Pérdida de información institucional	Servidores y equipos	Copias de seguridad incompletas	Fallas eléctricas o técnicas	Pérdida irreversible de información	Alto	Backups parciales	Automatización y verificación de respaldos
Alteración de registros clínicos	Historia clínica	Controles de edición débiles	Error humano	Riesgo asistencial y legal	Alto	Control de accesos	Trazabilidad y validación de registros
Robo o pérdida de equipos	Equipos de cómputo	Control físico limitado	Hurto	Fuga de información	Medio – Alto	Inventario de equipos	Bloqueo remoto y custodia
Incumplimiento normativo	Información institucional	Desactualización normativa	Falta de seguimiento	Sanciones de entes de control	Alto	Normativa vigente	Revisión normativa periódica

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La E.S.E. HOSPITAL SAN VICENTE DE PAÚL DE MISTRATÓ gestiona los incidentes de seguridad de la información mediante un enfoque preventivo, correctivo y de mejora continua, promoviendo una cultura de reporte no punitivo. Se consideran incidentes de seguridad eventos como el acceso no autorizado a sistemas de información, la pérdida o robo de equipos con información institucional, la divulgación accidental de datos personales, fallas en los sistemas que afecten la disponibilidad de la información, infecciones por software malicioso o errores en el manejo de historias clínicas.

La gestión de los incidentes contempla la identificación y reporte inmediato por parte de cualquier funcionario, el análisis de la causa raíz, la implementación de acciones correctivas y preventivas, y la documentación de lecciones aprendidas. Los incidentes relevantes son reportados a la Gerencia y articulados con los procesos de calidad, seguridad del paciente y control interno, garantizando una respuesta oportuna y la reducción de riesgos futuros.

Incidente de seguridad	Evento desencadenante	Nivel del incidente	Acción inmediata de contención	Análisis del incidente	Acciones correctivas	Registro y cierre	Responsable
Acceso no autorizado detectado	Alerta del sistema o auditoría	Crítico	Bloqueo inmediato del usuario	Revisión de trazabilidad y causa raíz	Ajuste de perfiles y credenciales	Formato de incidente y acta de cierre	Sistemas / Seguridad de la Información
Divulgación indebida de información	Reporte interno o queja	Alto	Contención de la información divulgada	Evaluación del impacto legal y asistencial	Reinducción y controles adicionales	Registro del incidente	Jurídica / control interno
Pérdida de información	Falla detectada	Crítico	Restauración de copia de seguridad	Análisis técnico	Mejora del esquema de backups	Informe técnico	Sistemas
Indisponibilidad del sistema	Caída del sistema	Alto	Activación de contingencia	Evaluación técnica	Ajuste de infraestructura	Registro del evento	Sistemas
Alteración de registros	Auditoría clínica	Alto	Corrección inmediata	Análisis de permisos y edición	Refuerzo de controles	Informe de incidente	Coordinación Médica
Robo o pérdida de equipo	Reporte del funcionario	Alto	Bloqueo del equipo y accesos	Evaluación de información comprometida	Fortalecimiento de custodia	Registro e inventario	Sistemas / control interno / gerencia
Infección por malware	Alerta antivirus	Alto	Aislamiento del equipo	Evaluación del alcance	Actualización de controles	Informe técnico	Sistemas

Incumplimiento de políticas	Auditoría interna	Medio	Retroalimentación inmediata	Análisis de causas	Capacitación y seguimiento	Registro de mejora	Talento Humano

PROTECCIÓN DE DATOS PERSONALES Y DATOS SENSIBLES

El hospital garantiza el tratamiento adecuado de los datos personales y datos sensibles conforme a la Ley 1581 de 2012, el Decreto 1377 de 2013 y la normativa del sector salud. Se identifican y documentan las bases de datos institucionales, se gestionan las autorizaciones de los titulares y se establecen mecanismos para atender los derechos de acceso, rectificación, actualización y supresión de la información.

Los datos sensibles, en especial los relacionados con la historia clínica, reciben un nivel de protección reforzado, limitando su acceso únicamente al personal autorizado y para fines estrictamente asistenciales, administrativos o legales. El incumplimiento de estas disposiciones constituye una falta grave y es objeto de las acciones disciplinarias correspondientes.

CONTROL DE ACCESOS Y USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

El acceso a los sistemas de información y a los activos tecnológicos del hospital se otorga de acuerdo con los perfiles funcionales y las responsabilidades asignadas a cada usuario. Se garantiza el uso de credenciales individuales, la actualización periódica de contraseñas y la revocatoria oportuna de accesos cuando se presentan cambios de rol, desvinculación laboral o finalización de contratos.

El uso adecuado de los sistemas de información implica la prohibición de compartir usuarios y contraseñas, la obligación de cerrar sesiones activas y el uso exclusivo de los recursos tecnológicos para fines institucionales. Estas medidas permiten asegurar la trazabilidad de las acciones realizadas y prevenir accesos indebidos o manipulaciones no autorizadas de la información.

CONTINUIDAD DE LA OPERACIÓN Y RESPALDO DE LA INFORMACIÓN

La disponibilidad de la información es esencial para garantizar la continuidad de la atención en salud. El hospital implementa políticas de respaldo periódico de la información crítica, asegurando la realización de copias de seguridad y la capacidad de restauración ante fallas técnicas, incidentes de seguridad o eventos de fuerza mayor. Estas acciones se articulan con el Plan de Emergencias y los planes de contingencia tecnológica, permitiendo mantener la operación asistencial incluso en escenarios adversos.

GOBERNANZA DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La seguridad y privacidad de la información en la E.S.E. HOSPITAL SAN VICENTE DE

PAÚL DE MISTRATÓ se gestionan bajo un esquema de gobernanza institucional que garantiza liderazgo directivo, asignación clara de responsabilidades y articulación con el Modelo Integrado de Planeación y Gestión – MIPG. La Gerencia asume la responsabilidad estratégica de aprobar políticas, planes y recursos asociados a la seguridad de la información, mientras que el responsable de Seguridad y Privacidad de la Información coordina la implementación operativa del Modelo de Seguridad y Privacidad de la Información – MSPI, realiza seguimiento al cumplimiento normativo y consolida los reportes institucionales.

Los líderes de proceso son responsables de la protección de la información generada y utilizada en sus áreas, asegurando la aplicación de controles y el reporte oportuno de incidentes. El área de Sistemas apoya la implementación de controles técnicos, la administración de accesos y la continuidad de los servicios tecnológicos. Esta estructura de gobernanza se articula con el Comité Institucional de Gestión y Desempeño, el Sistema de Control Interno y los procesos de calidad, permitiendo la toma de decisiones informadas y el seguimiento periódico al desempeño del sistema de seguridad de la información.

SENSIBILIZACIÓN, CAPACITACIÓN Y CULTURA DE SEGURIDAD DE LA INFORMACIÓN

El fortalecimiento de la cultura de seguridad de la información se logra mediante procesos permanentes de sensibilización y capacitación dirigidos a todo el talento humano. El hospital desarrolla actividades de inducción, reinducción y formación periódica en temas como protección de datos personales, manejo seguro de la información, reporte de incidentes y buenas prácticas digitales. Estas acciones buscan reducir los errores humanos, fortalecer el compromiso institucional y promover el cumplimiento de los lineamientos establecidos.

CAPÍTULO 3
CONTEXTUALIZACIÓN DE PROCESOS Y SUBPROCESOS EN EL HOSPITAL

SUBPROCESO CONTINGENCIA RECUPERACION Y RETORNO A LA NORMALIDAD

Objetivo

Definir las actividades que permiten implementar el plan de contingencia, recuperación y retorno a la normalidad de la plataforma de información de la E.S.E Hospital San Vicente de Paúl Mistrató, cuando se materialice algún tipo de desastre, que anule las operaciones de los recursos informáticos y/o servicios de la Institución.

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

Alcance

Inicia con la identificación del tipo de desastre materializado y finaliza con la elaboración de un informe final, donde se evidencien las afectaciones, acciones tomadas y resultados.

Responsabilidades

Área de sistemas y Comunicaciones: Debe identificar el tipo de desastre materializado, debe informar inmediatamente a la Alta gerencia de la E.S.E Hospital San Vicente de Paúl Mistrató, sobre la materialización del desastre y los daños preliminares identificados. Deberá definir el tiempo de recuperación del servicio en condiciones de operación limitada y el tiempo máximo de recuperación en condiciones de operación plena. Debe elaborar un informe final, donde se evidencien las afectaciones, acciones tomadas y resultados.

El área de sistemas debe poner en práctica, inmediatamente, el Plan de Contingencia, Recuperación y Retorno a la Normalidad.

Las diferentes áreas de la E.S.E Hospital San Vicente de Paúl Mistrató se encargan de elaborar el plan de continuidad de cada proceso a su cargo en caso de presentarse alguna contingencia, es decir, cada una (y en conjunto) definen las acciones que deben ejecutar en sus procesos para garantizar que la E.S.E Hospital San Vicente de Paúl Mistrató sigue prestando sus servicios mientras el Área de TIC está ejecutando la recuperación o el restablecimiento de los servicios de TIC.

SUBPROCESO COPIA DE RESPALDO DE LA INFORMACION

Objetivo

Definir las actividades que permiten realizar las copias de respaldo, de los recursos informáticos y sistemas de información de la E.S.E HOSPITAL SAN VICENTE DE PAÚL MISTRATÓ, garantizando con esto la preservación de la disponibilidad de los datos generados, procesados y custodiados por la Institución.

Alcance

Inicia con la identificación de la información institucional que necesita ser respaldada con copias de seguridad y los respectivos tiempos de ejecución de la tarea y finaliza con la actividad de verificación del espacio de almacenamiento, definido para las copias de respaldo.

Responsabilidades

Líder de sistemas y líderes de procesos administrativo asistencial:

- Definir con los Propietarios y/o Custodios de la información, qué documentos y/o sistemas de información deben estar incluidos en la tarea de copia de respaldo y los tiempos de realización de la actividad.
- Definir el lugar donde se almacenará la copia de respaldo (servidor), la partición, la estructura de los directorios, entre otras condiciones. Definir el método de realización de la actividad de copia de respaldo.

Propietarios y/o Custodios de la información:

- Definir en conjunto con el área de sistemas y Comunicaciones, qué documentos y/o sistemas de información deben estar incluidos en la tarea de copia de respaldo y los tiempos de realización de la actividad.

Profesional de Infraestructura TI:

- Programar la tarea de copia de respaldo, en la herramienta definida y aprobada para tal fin.
- Ejecutar la tarea de copia de respaldo manual, de acuerdo a los lineamientos definidos por el área.
- Verificar que la copia de respaldo realizada se almacenó en el servidor apropiado, en la partición adecuada y en la carpeta definida para tal fin.

SUBPROCESO RESTAURACION DE INFORMACION

Objetivo

Definir las actividades que permiten realizar una correcta restauración de la información recolectada, procesada y custodiada por el área de Informática, permitiendo identificar cualquier novedad, relacionada con la integridad de los datos institucionales, almacenados en las copias de respaldo existentes.

Alcance

Inicia con la definición de la frecuencia de ejecución de las actividades de restauración de la información institucional y finaliza con la actividad de informar los resultados obtenidos.

Responsabilidades

Profesional de área de sistemas y Comunicaciones:

- Definir la frecuencia de ejecución de las actividades de restauración de la información.
- Seleccionar la(s) copia(s) de respaldo a restaurar.

- Seleccionar el personal del área, que será el responsable de ejecutar la tarea de restauración.

Personal seleccionado:

- Restaurar la información de las copias de respaldo almacenadas, de acuerdo a los lineamientos internos del área.
- Realizar una actividad de comprobación o verificación de la información restaurada.
- Informar al Profesional de Gestión de Informática y Comunicaciones, las novedades identificadas, al concluir la tarea.

SUBPROCESO CREACION DE USUARIOS EN LAS PLATAFORMAS DE INFORMACION HSVP

Objetivo

Definir las actividades que permiten cumplir con la creación de las cuentas de acceso a los sistemas de información de la E.S.E HOSPITAL SAN VICENTE DE PAÚL MISTRATÓ, fortaleciendo con esto la preservación, confidencialidad, integridad y disponibilidad de la información de la institución.

Alcance

Inicia con el registro de los usuarios en el área facturación y finaliza con la actividad de informar en el área solicitante de la cuenta sobre la creación y configuración en todas y cada una de las herramientas disponibles y que el usuario pueda y deba tener acceso mediante las credenciales de identificación de la cuenta asignada. Esta cuenta tendrá todos los detalles relacionados como nombre de usuario, contraseña, rol, permisos y privilegios otorgados con el fin de cumplir a cabalidad los procesos y procedimientos al interior de la E.S.E HOSPITAL SAN VICENTE DE PAÚL MISTRATÓ.

Responsabilidades Profesional de Gestión Humana:

- Oficializar el ingreso de personal en el área de facturación.
- Si es necesario, solicitar la creación o actualización de credenciales del correo electrónico en el área de sistemas
- Solicitar la creación de cuentas del usuario en R-FAST o ANNARLAB ETC. Donde debe especificar los permisos, privilegios, roles y/o perfil del usuario, e informar a los líderes de las áreas la creación de los mismos.

Personal del área de sistemas

- Crea usuario con los permisos requeridos
- El área de sistemas y facturación deben custodiar Usuario y Clave.

SUBPROCESO INTERCAMBIO DE INFORMACION DIGITAL

Objetivo

Definir las actividades que permiten cumplir con las solicitudes de intercambio de información institucional con terceros, garantizando niveles óptimos de preservación de la confidencialidad e integridad de la información durante la tarea.

Alcance

Inicia con la identificación del nivel de autorización de acceso, del tercero, a la información institucional y finaliza con el intercambio de información.

Responsabilidades

Del Propietario, Custodio de la Información, o Empleado Público:

- Identificar si el solicitante de la información tiene el nivel de autorización de acceso suficiente.
- Identificar la clasificación de la información, solicitada por el tercero.
- Identificar el método de intercambio de información.
- Informar a sistemas y Comunicaciones, sobre la solicitud de intercambio de información institucional con un tercero (cuando la misma sea información Pública Clasificada o Reservada). Procede con el intercambio de información.

Del Profesional de sistemas de información:

- Verificar que el método de intercambio de información cumple con los requisitos de seguridad óptimos.
- Garantizar la preservación de la confidencialidad e integridad de la información a intercambiar con el tercero.
- Notificar al propietario de la información, custodio de la información, o servidor público, sobre el resultado de la verificación del método de intercambio y dar el visto bueno.

SUBPROCESO INTERCAMBIO INFORMACION FISICA

Objetivo

Definir las actividades que permiten cumplir con las solicitudes de intercambio de información institucional con terceros, garantizando niveles óptimos de preservación de la confidencialidad e integridad de la información durante la tarea.

Alcance

Inicia con la identificación del nivel de acceso a la información que posee el solicitante y finaliza con el envío de la documentación, a su respectivo destinatario.

Responsabilidades

Del Propietario, Custodio de la información, auxiliar de correspondencia o empleado público:

- Identificar si el solicitante de la información tiene el nivel de autorización de acceso adecuado.
- Identificar la clasificación de la información, solicitada por el tercero.
- Implementar controles de seguridad para el transporte y entrega de la documentación clasificada como Pública Clasificada o Reservada.
- Consultar el procedimiento "Recepción y Radicación de Comunicaciones Oficiales Externas Recibidas, y Enviadas", para llevar esta actividad.

Del Profesional o Técnico de Correspondencia:

- Implementar controles de seguridad para el transporte y entrega de la documentación clasificada como Pública Clasificada o Reservada.
- Radicar la información en el archivo administrativo con el visto bueno de la gerencia. Requerido Para llevar a cabo esta actividad.
- Gestionar la actividad de envío de la documentación, a su respectivo destinatario.

SUBPROCESO CONTROL DE DOCUMENTOS

Objetivo

Establecer mecanismos para el control de los documentos en la E.S.E Hospital San Vicente de Paúl Mistrató

Alcance

Inicia con el requerimiento de elaboración, modificación o eliminación de la documentación de los Sistemas de Gestión y termina con el ingreso del documento al listado de información documental respectivo y la publicación en el sitio web institucional.

Responsabilidades Del Administrador de la Documentación:

Revisar, editar, registrar, distribuir, divulgar, controlar y en general administrar la documentación original que conforman los Sistemas de Gestión, así como el control de los cambios de dicha documentación. Los Sistemas de Gestión de la E.S.E HOSPITAL SAN

VICENTE DE PAÚL MISTRATÓ son:

- Sistema de Gestión de Calidad
- Sistema de Seguridad de la Información.
- Sistema de Seguridad y Salud en el Trabajo.
- Sistema de Gestión Ambiental.
- Sistema de Gestión Documental.
- Modelo de Seguridad y Privacidad de la Información (Gobierno en Línea).

De los Líderes de los Procesos: Generar y solicitar creación o cambios a documentos actuales, implementar los documentos del proceso a cargo, controlar los documentos externos o de otros procesos que interactúen con su gestión y socializar con su personal a cargo la documentación vigente. Recoger copias obsoletas, si se trata de documentos a modificar o eliminar

Del Representante de la Dirección: Aprobar los documentos de los sistemas de gestión y controlar los documentos externos o de otros procesos que interactúen con su gestión.

Solicitud de copia de la historia clínica.

Solamente se entregará copia del contenido de la historia clínica, en los siguientes casos:

a. Al titular de la historia clínica, previa identificación.
b. A los padres, en representación de menores de edad, previa demostración del parentesco.
c. A terceros con autorización firmada y autenticada del titular.
d. A las autoridades competentes, específicamente reglamentadas en la resolución 1995 de 1999.

Parágrafo: El costo de las copias estará a cargo del solicitante, excepto por requerimientos legales.

Ingreso y salida de las historias clínicas.

Toda historia clínica que sea solicitada por un servicio, profesionales de la salud, encargados de facturación o personal administrativo debe estar acorde con el procedimiento establecido en la institución.

Búsqueda de las historias clínicas.

El personal del archivo propenderá por la búsqueda y suministro oportuno de las historias solicitadas previamente por los diferentes servicios, según lo estipulado en el procedimiento.

Será prioritaria la búsqueda de las Historias Clínicas requeridas para los procedimientos de auditoría, entes de control y atención oportuna al paciente.

Parágrafo: Cuando no se encuentre una historia clínica, debe atenderse al usuario diligenciando los registros clínicos requeridos y debe reportarse como historia clínica perdida en el registro según manual de procedimientos, y posteriormente debe realizarse la consolidación de la historia clínica si esta se encuentra y de encontrarse se debe colocar la fecha de aparición de la misma en el registro de historias clínicas perdidas.

Informes.
El funcionario de archivo clínico es el responsable de mantener actualizado el formato de historias clínicas perdidas y entradas y salidas de las historias clínicas.

Archivo administrativo

a. El acceso al archivo administrativo es restringido, el ingreso es solo para la persona encargada de esta área y auxiliares o practicantes autorizados por la administración para desempeñar labores de apoyo con previa inducción.
b. Toda la documentación que se entregue en el archivo administrativo será almacenada en una base de datos o cuaderno de registro con la fecha y nombre del documento que se entrega para asegurar continuidad y oportunidad en el acceso a dicha información.
c. Para solicitar un documento conservado en el archivo administrativo, se debe contar con la autorización de la administración o de la gerencia en caso tal de que lo amerite, si es un funcionario de la institución debe hacer el requerimiento al archivo administrativo para que le sea entregado el documento.

Hardware y software

a. El mantenimiento de los activos informáticos debe ser permanente, tanto componentes como soporte técnico, migración a nuevas necesidades y tecnologías.
b. Las interfaces deben facilitar el acceso a los servicios, de modo que se puedan utilizar de una forma rutinaria sin esfuerzo y deben prevenir los errores del usuario.
c. Todos los equipos de la institución estarán asegurados.
d. Se harán auditorias semestrales para verificar que el sistema y los equipos no tenga copias ilegales o piratas.
e. Se restringirá el acceso de disco externos y/o memorias USB
f. Se restringirán los permisos a los equipos para evitar descargas de virus o programas ilegales.
g. Se implementarán barreras protectoras en los equipos como el Firewall, el Proxy, los dominios, entre otros softwares expertos en brindar seguridad a la información.
h. Se harán capacitaciones al personal sobre el manejo y uso de las herramientas informáticas.
i. Los aplicativos que se instalen en la institución deben sincronizarse con la fecha y hora correcta.

j. El uso de los equipos es para uso exclusivo de los funcionarios de la institución.
k. No exponer los equipos al sol o al agua para evitar su deterioro o daño permanente.
l. Los equipos son para uso únicamente de cumplimiento de las funciones de cada funcionario.
m. Para trasladar un equipo de un lugar a otro se debe contar con la autorización del personal de sistemas.
n. No se deberán instalar programas sin la debida autorización.
o. Los Software utilizados por la E.S.E Hospital San Vicente de Paúl Mistrató son de uso interno y sólo para ser utilizado en los procesos administrativo-asistenciales de nuestra institución.
p. No se debe entregar datos o reproducir total o parcialmente la información a personas ajenas de la E.S.E Hospital San Vicente de Paúl Mistrató o que no sean parte del proceso administrativo correspondiente.
q. El correo electrónico, internet e intranet son de uso exclusivo labores relacionadas con nuestras tareas o funciones de nuestra área, queda prohibido el uso para otros fines.
r. Se prohíbe la descarga de archivos, transmisión o almacenamiento que pudiera ser considerado pornográfico, difamatoria, racista, videos, música o que atente contra las buenas costumbres o principios, excepto que el trabajo lo amerite.

Manejo apropiado de las impresiones

a. Las impresoras solo podrán ser utilizadas para imprimir documentos requeridos por la institución.
b. Retirar los documentos que se envían a imprimir.
c. Todo documento que quede en la impresora al final del día debe ser eliminado.
d. En caso del mal funcionamiento en una impresora, o que está siendo mal utilizada, deberá informar al área de sistemas de la E.S.E HOSPITAL SAN VICENTE DE PAÚL MISTRATÓ.
e. Cada área será la responsable de mantener los suministros correspondientes.
f. El material impreso que contenga información sensible no debe ser descuidado en áreas abiertas, debe ser removido de las impresoras sin demora.

Manejo apropiado de contraseña

a. Nunca guarde sus contraseñas, en ningún tipo de papel, agenda, que este a disposición de terceros etc.
b. Las contraseñas se deben mantener confidenciales en todo momento.
c. No compartir las contraseñas con otros usuarios.
d. Cambiar la contraseña si piensa que alguien más la conoce y si ha tratado de dar mal uso de ella.
e. Selecciona contraseñas que no sean fáciles de predecir.
f. Nunca grabe su contraseña en una tecla de función o en un comando de caracteres pre- definido.

g. Cambie sus contraseñas regularmente.
h. No utilizar la opción de almacenar contraseñas en Internet.
i. No utilizar contraseña con números telefónicos, nombre de familia etc.

Manejo apropiado de control de Virus

a. El sistema de actualizaciones y detección diaria es automatizado en la consola de antivirus.
b. Se debe comunicar de cualquier infección por virus que no fue eliminada por el antivirus al área de sistemas.
c. Los usuarios no podrán bajo ninguna circunstancia desinstalar el producto de antivirus existente en su equipo.
d. Los dispositivos extraíbles antes de ser usados deben realizar scanner con el antivirus.
e. En la medida de lo posible se restringe el uso de dispositivos extraíbles

Manejo de cuentas de sistemas

a. Toda cuenta de acceso que se requiera modificar deberá ser solicitada a través de los administradores de los sistemas de información o en la opción de cambio de contraseña.
b. El procedimiento de creación de cuentas debe ser canalizado por el coordinador del área.
c. La cuenta de red es la que utilizará cada usuario para conectarse a su equipo PC, esta debe ser solicitada por el coordinador del área.
d. La cuenta de usuario software R-FAST debe ser solicita por el líder del área.
e. La eliminación de cuentas se realizará de forma formal, por el área de recurso humano cuando el funcionario no tenga vínculo laboral con la institución o cuando este lo requieran, pero en situaciones especiales como suspensiones del personal, podrá ser enviado un correo por parte del jefe solicitando el bloqueo temporal de las cuentas del funcionario en cuestión formalizando a la brevedad.

Manejo de acceso a internet

a. El acceso a internet se encuentra protegido por filtros para disminuir sitios peligros que contenga código malicioso o que se encuentren ajenos al servicio, permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus.
b. No navegar por sitios no confiables.
c. Queda prohibido el uso de sitios de radios online.
d. Queda prohibido el uso de intercambio de archivos (Ares, emule, Torrents, Limewire, etc.).
e. Queda prohibido el uso de sitios de chat (Messenger, chat, etc.).
f. Queda prohibido el uso de internet para actividades ilícitas.
g. Queda prohibido la descarga que no cumpla con la normativa vigente de copyright y similar.
h. Se prohíbe el acceso a los sitios o páginas Web que contengan materiales

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

amenazadores, pornográficos, racistas, sexistas o cualquier otro que degrade la calidad del ser humano, salvo aquellas requeridas por la naturaleza de las funciones institucionales del usuario.

i. No compartir sus claves para ingresar a sitios que lo requiera como Bancos, Correo, etc.
j. No permitir que el navegador de internet recuerde la contraseña automáticamente.
k. Está Prohibido participar en juegos de entretenimiento en línea.
l. Si no está navegando por internet, cierre todas las ventanas abiertas.
m. Cualquier archivo que se reciba o descargue de internet deberá revisarse con el antivirus para asegurar que no tenga virus.
n. El área de Informática tiene la facultad de suspender el servicio de navegación en internet bajo circunstancias que así lo requiera (Virus, mal uso de internet, tráfico sospechoso, etc.).
o. Si requiere navegar en algún sitio bloqueado enviar correo a informatica@hsvpmistrato.gov.co, para su evaluación.

Manejo de correo electrónico

a. El área de informática cuenta con filtros para identificar y bloquear correos no deseados (Spam o Virus), archivos infectados o maliciosos.
b. El Correo electrónico es de uso exclusivo para las labores de nuestras funciones de la E.S.E Hospital San Vicente de Paúl Mistrató y queda restringido el uso para otros fines.
c. Se prohíbe expresamente el envío de archivos, transmisión o almacenamiento de cualquier información que pudiera ser considerada pornográfica, difamatoria, racista, música, videos, etc., o que atente contra las buenas costumbres o principios.
d. Todo correo ajeno que no pertenezca al dominio HSVP, no se entrega soporte o algún tipo de estabilidad.
e. La contraseña del correo debe ser cambiada periódicamente.
f. No dar click en link sospechosos llegados por correos electrónicos (bancos, tiendas, etc.).
g. No completar datos personales en correos electrónicos sospechosos.
h. Eliminar correo no deseado (spam o sospechoso).
i. Evitar descargar archivos sospechosos
j. No enviar correo que su tamaño se ha superior a 10MB.

Manejo de redes sociales

El área de sistemas bloqueará todo tipo de sitio relacionado con redes sociales, permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus, si algún funcionario por motivos de trabajo requiera acceder a ello, el coordinador o líder de área debe enviar la solicitud formal a informática, especificando los siguientes datos:

1. Nombre del funcionario
2. IP del equipo
3. Motivo

Cabe destacar que cualquier foto subida o comentario en Facebook, X (antes Twitter) o en alguna red social es responsabilidad exclusiva del que la emite.

Manejo de software

a. Queda prohibida la instalación que no cumpla con las instrucciones del Área de Sistemas de Información.
b. Los usuarios no deben instalar ni descargar aplicaciones que podrían provocar alguna vulnerabilidad o inestabilidad en los servicios.
c. Toda solicitud debe ser canalizada al correo informatica@hsvpmistrato.gov.co

Manejo de dispositivos móviles

Para garantizar la seguridad y estabilidad de la red y los dispositivos móviles, se describen algunos concejos y manejo adecuado, de los dispositivos móviles.net:

a. Los teléfonos móviles o tabletas de la E.S.E Hospital San Vicente de Paúl Mistrató se han adquirido específicamente para facilitar el desarrollo de actividades laborales relacionadas con la entidad y el uso para propósitos personales debe ser ocasional, racional y no debe obstaculizar las actividades laborales.
b. En caso de licencia o vacaciones del funcionario, el teléfono móvil o tableta debe quedar a disposición del área a la cual fue asignado.
c. La instalación, configuración, modificación o eliminación de software aplicativo sobre los dispositivos móviles es responsabilidad exclusiva del área de Informática.
d. No descargar ningún software que no se encuentre licenciado o que indique claramente que es de licencia libre.
e. Las actualizaciones de sistemas operativos de los dispositivos móviles, debe ser coordinado con el área de sistemas, que es la responsable de realizar las actualizaciones.
f. Se debe mantener desactivada la red Bluetooth, Infrarrojos, etc., en caso de que no esté siendo utilizada.
g. Es responsabilidad de cada funcionario hacer copias de seguridad de la información almacenada en el teléfono móvil, si no está seguro del proceso debe comunicarse con el Área de sistemas.
h. Es responsabilidad del funcionario reportar inmediatamente al Área de almacén, cualquier daño o pérdida del dispositivo móvil que le ha sido asignado.
i. Se debe solicitar al área de sistemas la configuración y acceso a los correos de la E.S.E Hospital San Vicente de Paúl Mistrató, a los teléfonos móviles donde exista servicio disponible y que pertenezcan a la institución.
j. No insertar tarjetas de memoria sin haber comprobado previamente que están

libres de virus o de algún tipo de código malicioso.

k. No acceder a los enlaces no solicitados a través de SMS/MMS/Email podría ser código malicioso.

Manejo computadores portátiles

Para garantizar la seguridad y estabilidad de la red de la E.S.E Hospital San Vicente de Paúl Mistrató, se describen algunos concejos y manejo adecuado.

a. Todo computador portátil debe ser incorporado al dominio de la red de la E.S.E Hospital San Vicente de Paúl Mistrató.
b. Los computadores portátiles de la E.S.E Hospital San Vicente de Paúl Mistrató se han adquirido específicamente para facilitar el desarrollo de actividades laborales, su uso debe estar relacionado con las actividades del área a la cual ha sido asignado y el uso para propósitos personales debe ser ocasional, racional y no debe obstaculizar las actividades laborales.
c. Los equipos portátiles deben permanecer en las instalaciones de la E.S.E Hospital San Vicente de Paúl Mistrató, durante los días y horarios hábiles de trabajo, pueden salir de las instalaciones, solo en el caso de utilizarlo en labores de la entidad.
d. En caso de licencia o vacaciones del funcionario, el equipo portátil debe quedar a disposición del área a la cual fue asignado, si el coordinador del área autoriza puede ser utilizado en el periodo de licencia o vacaciones.
e. La instalación, configuración, modificación o eliminación de software aplicativo sobre los equipos portátiles es responsabilidad exclusiva del área de sistemas.
f. El área de sistemas tiene la potestad para remover, sin notificar al funcionario, cualquier software que no esté autorizado
g. La configuración, eliminación, modificación o cambio de sistema operativo es de responsabilidad del área de sistemas.
h. La configuración e instalación de hardware de los equipos portátiles, es responsabilidad exclusiva del área de sistemas de la ESE o el área de soporte, según corresponda.
i. Se debe mantener desactivada la red inalámbrica en caso de que no esté siendo utilizada.
j. Es responsabilidad de cada funcionario hacer copias de seguridad de la información almacenada en el equipo portátil, si no está seguro del proceso debe comunicarse con el Área de Soporte.
k. Es responsabilidad del funcionario reportar inmediatamente al Área activos fijos, cualquier daño o pérdida del dispositivo móvil que le ha sido asignado.
l. No insertar tarjetas de memoria sin haber comprobado previamente que están libres de virus o de algún tipo de código malicioso.

Software Administrativo Hospitalario R-FAST

Es un sistema de información está compuesto por módulos que integran todas las áreas de la E.S.E Hospital San Vicente de Paúl Mistrató, públicas y privadas y de todos los niveles de atención, es decir, que a partir del acto médico afecta las demás unidades funcionales y

su correspondiente resultado en el área administrativa.

R-FAST garantiza la seguridad de la información y seguridad por usuario con su correspondiente clave de acceso donde autoriza o restringe las actividades dentro de la plataforma de información. R-FAST cuenta con un registro de transacciones que permite identificar a los usuarios que utilizaron el sistema de información, el día, la hora y la transacción realizada, para efectuar actividades de seguimiento y auditoría.

Repositorio Institucional de Documentos

La institución contará con un Repositorio Institucional Virtual, el cual podrá operar mediante plataforma en la nube y/o carpeta compartida en el servidor institucional con acceso remoto controlado.

Este repositorio será el medio oficial para la custodia y consulta de:

- Manuales
- Procedimientos
- Protocolos
- Guías
- Formatos
- Planes, programas y políticas
- Documentos de apoyo a los Sistemas de Gestión

Se dispondrá de una matriz maestra de control documental que incluirá el nombre del documento, código, versión, fecha de actualización, proceso responsable, estado (vigente u obsoleto) y enlace directo al archivo.
Niveles de acceso:

- Edición: Exclusiva del Líder de Calidad
- Consulta: Funcionarios y contratistas, únicamente para lectura y descarga

No se permitirá la modificación directa de documentos por parte de otros usuarios, garantizando la integridad y custodia de la información.

Responsabilidades del personal de sistemas

a. Se harán auditorias trimestrales para identificar la vulnerabilidad del sistema de información y el grado de capacitación operativa y técnica de los funcionarios.
b. Se harán evaluaciones al fluido eléctrico, las conexiones y los cables para evitar eventos adversos en el sistema de información.
c. Todos los equipos entrarán en el inventario de la institución.
d. Todos los funcionarios de la institución contarán con herramientas informáticas de trabajo en buen estado si así lo requiere su labor.
e. A cada usuario de la institución se le deben conceder los accesos necesarios para el cumplimiento de sus funciones.
f. Es responsabilidad del área de sistemas instalar todo el software de la

institución.

g. Realizar Copias de respaldo todos los días a las 7:00 Pm de todos y cada uno de los servidores (Servidor de Correo, servidor de base de datos R-FAST - ANNARLAB,), donde se garantice fiel copia de la información que repose sobre estos equipos del área de sistemas. Dicha información se guarda en discos duros externos.

Actualmente también se guarda una copia de seguridad diaria en la NAS de los servidores antes mencionados y de la información que en ellos reposa.

CAPÍTULO 4
IMPLEMENTACIÓN

PLAN DE IMPLEMENTACIÓN (CRONOGRAMA GENERAL)

- **Primer trimestre:** Diagnóstico detallado y adopción normativa.
- **Segundo trimestre:** Implementación de controles y comité.
- **Tercer trimestre:** Capacitación y ajustes técnicos.
- **Cuarto trimestre:** Evaluación, seguimiento y mejora.

RECURSOS Y PRESUPUESTO

Las actividades del presente plan se ejecutarán con recursos propios de la institución, priorizando acciones de alto impacto y bajo costo, y gestionando apoyos técnicos cuando sea necesario.

ESTRATEGIAS POR EJECUTAR PARA CUMPLIR EL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – VIGENCIA 2026

Actividad programada	Meta o producto	Responsable	Fecha programada
Socializar el Plan de Seguridad y Privacidad de la Información con el personal de la E.S.E., asegurando la comprensión de sus lineamientos, responsabilidades y obligaciones frente al manejo de la información.	Alcanzar el 100% del personal institucional informado y sensibilizado sobre el Plan de Seguridad y Privacidad de la Información.	Líder de sistemas	Febrero de 2026
Desarrollar jornadas de	Lograr que el 100%	Líder de	Abril de 2026

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

capacitación orientadas al conocimiento y apropiación de la normativa vigente en materia de seguridad de la información, protección de datos personales y confidencialidad.	del personal reciba capacitación sobre las normativas aplicables y los deberes institucionales en seguridad y privacidad de la información.	sistemas	
Replicar de manera permanente la información relacionada con seguridad y privacidad de la información a través de los canales institucionales de comunicación, con mensajes preventivos y educativos.	Garantizar el 100% de difusión de la información a través de correo institucional, redes internas y otros medios definidos por la E.S.E.	Líder de sistemas	Junio de 2026
Evaluar el nivel de conocimiento del personal frente a los lineamientos de seguridad y privacidad de la información mediante instrumentos de medición definidos por la entidad.	Alcanzar un nivel mínimo del 70% de conocimiento del personal evaluado sobre seguridad y privacidad de la información.	Líder de sistemas	Agosto de 2026
Verificar de manera periódica la ejecución y disponibilidad de las copias de respaldo de la información contenida en los sistemas de información institucionales.	Asegurar el 100% de copias de respaldo actualizadas de las bases de datos de los sistemas de información de la E.S.E.	Líder de sistemas	Diario durante 2026
Revisar y actualizar de forma permanente los usuarios creados en las plataformas tecnológicas de la entidad, garantizando la gestión adecuada de accesos y perfiles.	Mantener el 100% de usuarios activos y retirados correctamente gestionados en las plataformas institucionales.	Líder de sistemas	Seguimiento semanal y a demanda durante 2026

Realizar seguimiento periódico a los riesgos y controles de seguridad digital definidos en el Mapa de Riesgos Institucional, verificando su efectividad y cumplimiento.	Ejecutar el seguimiento bimestral al 100% de los riesgos y controles de seguridad digital identificados en el Mapa de Riesgos Institucional.	Líder de sistemas con el apoyo técnico del área de Planeación	Bimestral durante 2026

SEGUIMIENTO, INDICADORES Y MEJORA CONTINUA

El desempeño del Plan de Seguridad y Privacidad de la Información se evalúa mediante indicadores que permiten medir su efectividad y orientar la toma de decisiones. El seguimiento es realizado de manera periódica y los resultados son reportados a la Gerencia y a las instancias de control institucional.

Indicadores de seguridad de la información

Componente del Plan	Indicador	Descripción del indicador	Fórmula de cálculo	Meta	Periodicidad	Responsable
Gestión del Plan	Porcentaje de ejecución del Plan de Seguridad y Privacidad de la Información	Mide el grado de cumplimiento de las actividades programadas en el plan durante la vigencia.	(Actividades ejecutadas / Actividades programadas) × 100	≥ 90 %	Semestral	Área de sistemas/ Planeación
Sensibilización y capacitación	Porcentaje de personal capacitado en seguridad y privacidad de la información	Evalúa el nivel de cobertura de las jornadas de capacitación y socialización del plan y la normativa aplicable.	(Número de funcionarios capacitados / Total de funcionarios) × 100	≥ 90 %	Anual	Talento Humano / Área de sistemas/

Cultura de seguridad	Nivel de conocimiento del personal en seguridad de la información	Mide el nivel de apropiación de los lineamientos de seguridad y privacidad por parte del personal.	(funcionarios que alcanzan el nivel mínimo / Total evaluados) × 100	≥ 70 %	Anual	Área de sistemas/
Gestión de riesgos	Porcentaje de riesgos de seguridad de la información con tratamiento definido	Evalúa la cobertura del tratamiento de riesgos identificados en el mapa institucional.	(Riesgos con controles definidos / Total riesgos identificados) × 100	100 %	Anual	Planeación / Área de sistemas
Controles de seguridad	Nivel de implementación de controles de seguridad de la información	Mide el grado de implementación de los controles técnicos y administrativos definidos en el plan.	(Controles implementados / Controles definidos) × 100	≥ 90 %	Semestral	Area de sistemas
Gestión de accesos	Porcentaje de revisión de usuarios y perfiles de acceso	Evalúa la gestión adecuada de usuarios activos, retirados y perfiles en los sistemas institucionales.	(Usuarios revisados / Total de usuarios) × 100	100 %	Mensual	Area de sistemas
Respaldo de la información	Cumplimiento del plan de copias	Verifica la ejecución y disponibilidad de las	(Respaldos realizados / Respaldos	100 %	Diario / Mensual	Area de sistemas

	de seguridad	copias de respaldo de la información institucional.	programados) × 100			
Continuidad y recuperación	Número de pruebas de restauración realizadas	Mide la ejecución de pruebas de recuperación de la información para garantizar la continuidad del servicio.	Conteo de pruebas realizadas	≥ 2 por año	Semestral	Area de sistemas
Gestión de incidentes	Porcentaje de incidentes de seguridad atendidos conforme al procedimiento	Evalúa la capacidad de respuesta frente a incidentes de seguridad de la información.	(Incidentes atendidos / Incidentes reportados) × 100	100 %	Trimestral	Área de sistemas/
Confidencialidad	Porcentaje de personal con Acuerdo de Confidencialidad firmado	Mide el cumplimiento de la suscripción del acuerdo de confidencialidad por parte del personal.	(Acuerdos firmados / Total de personal) × 100	100 %	Anual	Talento Humano
Monitoreo y auditoría	Porcentaje de auditorías ejecutadas en seguridad	Evalúa el cumplimiento del programa de auditorías relacionada	(Auditorías ejecutadas / Auditorías programadas) × 100	100 %	Anual	Control Interno

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

	de la información	s con seguridad y privacidad de la información				
Mejora continua	Porcentaje de acciones de mejora cerradas	Mide la efectividad del plan de mejora derivado de auditorías, monitoreo e incidentes.	(Acciones cerradas / Acciones formuladas) × 100	≥ 90 %	Semestral	Responsables de proceso

RESPONSABLES DEL PLAN

Rol / Cargo	Responsabilidad dentro del Plan
Gerente de la E.S.E.	Aprobar el PLAN DE SEGURIDAD Y PRIVACIDAD 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 Planeación	Articular el plan con el MIPG, la gestión del riesgo institucional 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 y privacidad 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

BIBLIOGRAFÍA

- Congreso de la República de Colombia. (1991). *Constitución Política de Colombia*.
- *Congreso de la República de Colombia. (1993). Ley 87 de 1993. Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado.*
- *Congreso de la República de Colombia. (1999). Resolución 1995 de 1999. Por la cual se establecen normas para el manejo de la historia clínica. Ministerio de Salud.*
- *Congreso de la República de Colombia. (2000). Ley 594 de 2000. Ley General de Archivos.*
- *Congreso de la República de Colombia. (2009). Ley 1273 de 2009. Por medio de la cual se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos".*
- *Congreso de la República de Colombia. (2011). Ley 1438 de 2011. Por medio de la cual se reforma el Sistema General de Seguridad Social en Salud.*
- *Congreso de la República de Colombia. (2012). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.*
- *Presidencia de la República de Colombia. (2013). Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.*
- *Congreso de la República de Colombia. (2014). Ley 1712 de 2014. Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.*
- *Ministerio de Tecnologías de la Información y las Comunicaciones. (2015). Decreto 1078 de 2015. Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.*
- *Presidencia de la República de Colombia. (2017). Decreto 1499 de 2017. Por medio del cual se adopta el Modelo Integrado de Planeación y Gestión – MIPG.*
- *Ministerio de Tecnologías de la Información y las Comunicaciones. (Vigente). Modelo de Seguridad y Privacidad de la Información – MSPI. Lineamientos para entidades públicas.*
- *Departamento Administrativo de la Función Pública. (Vigente). Guía para la implementación del Modelo Integrado de Planeación y Gestión – MIPG.*
- *Ministerio de Salud y Protección Social. (Vigente). Lineamientos para la gestión de la información clínica y la historia clínica en las Instituciones Prestadoras de Servicios de Salud.*
- *E.S.E. HOSPITAL SAN VICENTE DE PAÚL DE MISTRATÓ. (2025). Plan de Seguridad y Privacidad de la Información. Documento institucional.*
- *E.S.E. HOSPITAL SAN VICENTE DE PAÚL DE MISTRATÓ. (Vigente). Políticas institucionales de seguridad de la información, control interno y gestión documental.*