

MANUAL DE SEGURIDAD DE LA INFORMACIÓN



Elaboró:

FAIVER TOVAR NOGALES

Lider Administración y Almacenamiento de la Información
Afiliado Participe Admisalud

MONICA VILLEGAS NOGUERA

Profesional Administrativa Administración y Almacenamiento de la Información
Afiliado Participe Admisalud

Revisó:

LUCY XIMENA IBARRA HERNÁNDEZ.

Subgerente Administrativa y Financiera

Aprobó:

CESAR EDMUNDO SARRIA PORRAS

Gerente

POPAYAN, 2021

Ch

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

MAN-SIS-01

Versión: 03

Página 2 de 21



Contenido

1	OBJETIVO.....	5
2	ALCANCE.....	5
3	BASE LEGAL.....	5
4	OBLIGACIONES.....	6
5	PRINCIPIOS BÁSICOS.....	6
	5.1. Confidencialidad.....	6
	5.2. Integridad:.....	6
	5.3. Disponibilidad.....	6
	5.4. Autenticidad:.....	6
	5.5. No repudio:.....	6
	5.6. Confiabilidad de la información: Es.....	7
	5.7. Sistemas de información:.....	7
	5.8. Sistema de gestión de la información:.....	7
	5.9. Usuario:.....	7
	5.10. Base de Datos:.....	7
	5.10. Dato sensible:.....	7
	5.11. Autorización:.....	7
	5.12. Tratamiento:.....	7
6	DEFINICIONES.....	7
	6.1. Activo de información:.....	7
	6.2. Backup o copia de seguridad:.....	7
	6.3. Control:.....	7
	6.4. Equipo de cómputo:.....	8
	6.5. Medio removible:.....	8
	6.6. Servicio.....	8
	6.7. Terceros:.....	8

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

MAN-SIS-01

Versión: 03

Página 3 de 21



7	SEGURIDAD FÍSICA Y AMBIENTAL	8
7.1.	Controles de acceso físico	8
7.2.	Protección y ubicación de equipos y repositorios de información.	8
7.3.	Mantenimiento del equipo	9
7.4.	Perdida, daño o traslado de equipos o repositorios de información	9
8	SEGURIDAD EN EL RECURSO HUMANO	9
8.1	Selección del personal	9
8.2	Durante la vigencia de la contratación:	10
8.3	Finalización de Vinculación Laboral o Cambio de Rol	10
9	CLASIFICACIÓN Y ORGANIZACIÓN DE LA INFORMACIÓN.....	10
9.1.	Para prevenir el deterioro de los archivos físicos se debe tener en cuenta las siguientes consideraciones:	11
9.2.	Conservación preventiva en espacios de archivo, en relación con las condiciones locativas.	12
10	ADQUISICIÓN, ACTUALIZACIÓN Y LICENCIAMIENTO DE SOFTWARE	13
11	USO RESPONSABLE DE ACTIVOS Y RECURSOS.....	14
11.1.	Intranet	14
11.2	Internet	14
11.3	Correo electrónico	14
11.4	Equipos, archivos, dispositivos removibles	14
11.5	Recursos Compartidos	15
12	CONTROL DE ACCESO A LA INFORMACIÓN	15
12.1	Acceso a la red cableada e inalámbrica	15
12.2.	Perfiles de Usuarios	16
12.3	Gestión de contraseñas	16
12.4	Procedimiento para asignación de claves de acceso	17
12.5	Transmisión del Dato:	18
13	GESTIÓN DE SEGURIDAD PARA TELECOMUNICACIONES E INFRAESTRUCTURA	19
13.1	Antivirus	19

Handwritten signature and initials.

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

MAN-SIS-01

Versión: 03

Página 4 de 21



HOSPITAL
UNIVERSITARIO
SAN JOSÉ

13.2	Protección perimetral	19
13.3	Copias de seguridad de configuraciones en servidores	19
13.4	Planes de contingencia	19
13.5	Monitoreo del uso de sistemas	20
14	CONTROL DE CAMBIOS	20

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

MAN-SIS-01

Versión: 03

Página 5 de 21



**HOSPITAL
UNIVERSITARIO
SAN JOSÉ**

1 OBJETIVO

Proveer una guía para proteger, preservar y administrar objetivamente los activos de información junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, confiabilidad, legalidad y no repudio de la información.

2 ALCANCE

Este manual aplica para directivos, funcionarios y terceros de todos los procesos gerenciales, administrativos, de apoyo diagnóstico y terapéutico, asistenciales y es responsabilidad de todos y cada uno de ellos cumplir, promover e implementar las acciones necesarias tendientes a proteger, preservar y administrar los activos de información del Hospital Universitario San José de Popayán E.S.E.

3 BASE LEGAL

- Ley 100 de 1993 - Por la cual se crea el sistema de seguridad social integral y se dictan otras disposiciones.
- Ley 594 de 2000 "Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones" artículo 16.
- Ley 1437 de 2011, Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. En sus artículos 58 y 59.
- Resolución 123 de 2012 - Por la cual se modifica el artículo 2 de la Resolución 1445 de 2006 y se adopta el Manual de Estándares de Acreditación Ambulatorios y Hospitalarios.
- Decreto 2578 de 2012 - Por medio del cual se reglamenta el Sistema Nacional de Archivos.
- Decreto 1377 de 2013. Reglamenta parcialmente la ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto Único Reglamentario 1074 de 2015. Artículo 2.2.2.25.3.1 políticas de tratamiento de la información.

44
74

MANUAL DE SEGURIDAD DE LA INFORMACIÓN	MAN-SIS-01	
	Versión: 03	Página 6 de 21



De acuerdo a lo establecido por la Organización Internacional para la estandarización (ISO, por sus siglas en inglés) en sus estándares relacionados a continuación, tomados como referencia para este manual:

- Norma ISO 27001:2005: Define cómo organizar la seguridad de la información en cualquier tipo de organización
- Norma ISO 27002:2005: Recomendaciones de las mejores prácticas en la gestión de la seguridad de la información

4 OBLIGACIONES

Es compromiso de todos los clientes internos conocer y dar a conocer el Manual de Seguridad de la Información y es su deber cumplir y respetar las disposiciones en él contenidas para el desarrollo de cualquier actividad relacionada con manejo de la información dentro de la institución.

5 PRINCIPIOS BÁSICOS

Este manual de Seguridad de la Información provee una guía para garantizar que la información institucional cumpla con los siguientes principios:

- 5.1. Confidencialidad:** Se garantiza que la información sea accesible sólo a aquellas personas que estén autorizadas para tener acceso a ella.
- 5.2. Integridad:** Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- 5.3. Disponibilidad:** Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
- 5.4. Autenticidad:** Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- 5.5. No repudio:** Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

14

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

MAN-SIS-01

Versión: 03

Página 7 de 21



5.6. Confiabilidad de la información: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

5.7. Sistemas de Información: Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

5.8. Sistema de gestión de la información: Sistema que permite la definición, establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora continua de la información.

5.9. Usuario: Quien usa ordinariamente la información o es destinatario de la misma.

5.10. Base de Datos: Conjunto organizado de datos personales que sea objeto de tratamiento.

5.10. Dato sensible: Aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación.

5.11. Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

5.12. Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

6 DEFINICIONES

6.1. Activo de información: Representa los datos de la organización, información que tiene valor para los procesos del Hospital, independientemente de su ubicación: puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil para el Hospital Universitario San José de Popayán E.S.E.

6.2. Backup o copia de seguridad: Es una copia de respaldo de la información

6.3. Control: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, y que puede ser de carácter administrativo, técnico o legal.

44
H
8

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

MAN-SIS-01

Versión: 03

Página 8 de 21



HOSPITAL
UNIVERSITARIO
SAN JOSÉ

6.4. Equipo de cómputo: Es un dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

6.5. Medio removible: Es un medio que permite llevar o transportar información desde un computador a otro. Los medios removibles incluyen cintas, diskettes, discos duros removibles, CDs, DVDs, unidades de almacenamiento USB.

6.6. Servicio: Es cualquier acto o desempeño que una persona puede ofrecer a otra, que es esencialmente intangible y que no conlleva ninguna propiedad.

6.7. Terceros: Se entiende por tercero a toda persona, jurídica o natural, como proveedores, contratistas o clientes, que tengan una relación directa con el Hospital.

7 SEGURIDAD FÍSICA Y AMBIENTAL

7.1. Controles de acceso físico

- En la institución se cuenta con acceso restringido al personal no autorizado en áreas de almacenamiento de información y dispositivos que permitan gestión de la información, servidores, archivos, centros de cableado, a través de manejo de contraseñas, definición de roles y perfiles de usuario en el sistema de información y seguridad física para controlar el acceso a los archivos de la Historia Clínica que aún se almacenan en físico.
- Cualquier persona que tenga acceso a las instalaciones de la institución, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la institución, de acuerdo a lo establecido en el procedimiento de control de acceso de equipos e información el cual está en proceso de revisión y aprobación.
- Debe ser notificada al área responsable de la seguridad cuando se detecte una posible violación de acceso a cualquiera de estas instalaciones, con el fin de determinar el motivo de la falla y realizar su inmediata corrección.

7.2. Protección y ubicación de equipos y repositorios de información.

- Solo usuarios autorizados pueden tener acceso a los equipos y su información, pero estos no deben mover o reubicar los equipos de cómputo o de

184

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

MAN-SIS-01

Versión: 03

Página 9 de 21



telecomunicaciones, instalar o desinstalar dispositivos, sin la autorización o supervisión del área de Sistemas de Información.

- Cualquier medio físico de información no debe ser manipulado sin la previa autorización del área encargada de la custodia de dicha información, con el fin de sustraer o adicionar información que no corresponda ser almacenada en dicho medio.

7.3. Mantenimiento del equipo

- Solo personal autorizado y con el conocimiento adecuado puede realizar mantenimientos preventivos o correctivos sobre los equipos.
- En caso del mantenimiento correctivo de los equipos de cómputo este se hará previa notificación del área que lo requiera, de acuerdo al procedimiento de Soporte Técnico a equipos de cómputo e impresoras.

7.4. Pérdida, daño o traslado de equipos o repositorios de información

Todo evento relacionado con un equipo o repositorio que contenga información útil para la institución debe ser notificado al área encargada de su custodia.

- Documentos oficiales (Archivo y correspondencia)
- Historias clínicas (Estadística)
- Medios electrónicos (Oficina de Sistemas de Información)

8 SEGURIDAD EN EL RECURSO HUMANO

Todos los funcionarios del Hospital Universitario San José de Popayán E.S.E. y terceros que realicen actividades dentro de la institución, deben ser cuidadosos de no divulgar información confidencial por canales no autorizados, en lugares públicos, en conversaciones o situaciones que pongan en riesgo la seguridad y el buen nombre de la institución.

8.1 Selección del personal

Ningún funcionario que se encuentre en periodo de prueba o preselección de acuerdo a lo dispuesto por la oficina de talento humano del hospital, debe tener acceso a información sensible para los intereses de la institución o en todo caso el

MANUAL DE SEGURIDAD DE LA INFORMACIÓN	MAN-SIS-01	
	Versión: 03	Página 10 de 21



funcionario será responsable de la misma, bajo supervisión de la persona encargada de su inducción.

8.2 Durante la vigencia de la contratación: Todos los funcionarios y aquellos terceros que laboren directamente en el Hospital Universitario San José de Popayán E.S.E., deben acogerse al presente manual, así como los términos de uso adecuado de los recursos de información que le son entregados, previo a la entrega de éstos recursos, y teniendo en cuenta que estos términos y responsabilidades son extensibles fuera de la Institución.

8.3 Finalización de Vinculación Laboral o Cambio de Rol: El Jefe directo del funcionario o el Responsable del tercero, son los encargados de asegurar que todos los activos propios de la organización sean devueltos y en coordinación con el Centro de Cómputo se garantice que los accesos físicos y lógicos sean eliminados y la información pertinente sea transferida.

En caso que un funcionario o tercero tenga un cambio de funciones o de actividades, se deben seguir los mismos procedimientos donde se asegure la entrega de activos, la reasignación de los accesos físicos y lógicos, la transferencia de información y la posterior entrega de los mismos de acuerdo a su nuevo rol.

El Hospital Universitario San José de Popayán E.S.E. a través de la dependencia correspondiente, se encargará de informar a las áreas implicadas, los procesos de vinculación, desvinculación, traslados o reubicación realizados; así como el bloqueo al acceso a los diferentes sistemas de información.

9 CLASIFICACIÓN Y ORGANIZACIÓN DE LA INFORMACIÓN

- Para asegurar que los activos de información reciben el nivel de protección adecuado, el proceso de Administración y Almacenamiento de la Información es responsable de definir la metodología de clasificación de activos de información, estos se deben clasificar según la necesidad, las prioridades y el grado de protección esperado en el manejo de los mismos, de acuerdo al procedimiento de realización de copias de seguridad institucional, el cual se actualizará en este aspecto.

- De igual forma, en la institución están identificados los medios de almacenamiento aceptados dentro de la institución de acuerdo a la disposición del proceso de

4/11

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

MAN-SIS-01

Versión: 03

Página 11 de 21



Gestión Documental, así como del proceso de Administración y Almacenamiento de la Información

- La clasificación y la organización de la información en medio físico, electrónico o digital desde la producción hasta la disposición final de los documentos, debe hacerse aplicando los instrumentos archivísticos estandarizados como son las Tablas de Retención Documental y las Tablas de Valoración Documental.
- Para la consulta de los documentos desde los archivos de gestión, central e histórico de debe contar con los inventarios documentales actualizados, lo que nos permitirá la consulta de la información eficiente, eficaz y confiable, garantizando la continuidad de la función pública.

9.1. Para prevenir el deterioro de los archivos físicos se debe tener en cuenta las siguientes consideraciones:

- Se debe tener las manos limpias al momento de la manipulación para evitar dejar manchas sobre los folios o las carpetas.
- Las personas que manejen los archivos deben contar con elementos de protección personal como son guantes, tapabocas y batas.
- Cuando el documento se somete a largas jornadas de manipulación, es necesaria la limpieza rigurosa de las manos y fosas nasales.
- Al hacer consulta de los documentos, se debe tener cuidado al pasar las hojas, debido a que la manipulación inadecuada puede generar deterioros. El momento de la apertura de las carpetas es muy importante, debido a que el esfuerzo físico al que se somete el documento lo hace vulnerable a sufrir rasgaduras.
- Cuando se lleve a cabo la consulta o se esté conformando un expediente, no se debe estar cerca de alimentos o bebidas para evitar el riesgo de derrame sobre la documentación.
- En los depósitos de archivos o espacios donde reposan archivos, únicamente debe almacenarse documentos, pues estos se pueden contaminar y causar deterioro, así como afectar la salud de quienes los manipulan o consulta.
- La adecuada manipulación es muy importante para la conservación de la integridad de los documentos y las unidades de almacenamiento, sin embargo, el paso del tiempo y la frecuente consulta puede ir creando desgaste en las carpetas,

Handwritten signatures and initials in the bottom right corner.

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

MAN-SIS-01

Versión: 03

Página 12 de 21



por tanto, se recomienda que si hay evidencia de deterioro, rasgaduras o falta de estabilidad de la unidades de conservación, se reemplacen por carpetas nuevas y así evitar el deterioro de los documentos.

- Para la manipulación de los archivos que se encuentren con riesgo biológico se debe proceder de acuerdo a la "Norma de Bioseguridad y Seguridad y salud en el trabajo para manipulación de documentos con biodeterioro en el documento" y al "Sistema - Integrado de Conservación de Documentos".
- Los documentos producidos o recibidos en los diferentes procesos de la entidad deben, estar almacenados en archivadores metálicos y en estantería que cumpla con las normas básicas de estabilidad, además se debe garantizar el mantenimiento periódico del inmobiliario.
- Unidades de Conservación: se debe garantizar que las unidades de conservación, como son cajas, carpetas y fundas plásticas deberán contemplar especificaciones técnicas dadas para el soporte documental por el Acuerdo 049 de 2000 y la norma GTC 5397 DE 2005.

9.2. Conservación preventiva en espacios de archivo, en relación con las condiciones locativas.

- Las unidades de conservación y almacenamiento: El Hospital debe considerar que las áreas destinadas a depósitos de archivos serán espacios que garanticen la conservación documental.
- Conservación preventiva: En espacios de archivos, en relación con las condiciones locativas se debe garantizar que las áreas destinadas a depósito de archivos o en las oficinas donde se conservan los archivos de Gestión, garanticen la conservación del documental, ya que es parte de la memoria institucional e histórica del Hospital.
- Ubicación: el área de Archivo Central debe estar ubicada en un lugar donde se garantice la estabilidad estructural en la construcciones (placas, pisos deben estar dimensionadas para soportar una carga mínima de 1200k/m²).
- Condiciones Ambientales: Las condiciones para las áreas de almacenamiento se refiere específicamente a la humedad relativa y la temperatura (De acuerdo con la clase, las características y las técnicas de soportes), la contaminación atmosférica, iluminación ventilación, carga de polvo y material particulado y carga microbiana. Esto teniendo en cuenta el Manual de Construcción y Adecuación de los Espacios para Archivos del Archivo General de la Nación.

46

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

MAN-SIS-01

Versión: 03

Página 13 de 21



- **Mantenimiento:** En los espacios de archivos del Hospital debe considerarse tanto el mantenimiento relacionando con las características arquitectónicas de las construcciones, como aquellas condiciones propias de su ubicación, con el fin de tomar las acciones pertinentes que contribuyan de manera efectiva a la conservación preventiva de los acervos documentales propios de los archivos de gestión, central e histórico del Hospital; para lo cual se debe tener en cuenta el Protocolo de limpieza para espacios de archivos.
- Debe hacerse periódicamente inspecciones y el mantenimiento preventivo como mínimo dos veces al año (Ver Manual de Construcción y Adecuación para Espacios de Archivos del AGN)
- Así mismo el mantenimiento preventivo debe garantizar la limpieza de instalaciones, estanterías y unidades de conservación de los Archivos del Hospital aplicando el Protocolo de limpieza para espacios de Archivos., el cual debe contar con una programación de limpieza frecuente cada 15 días para superficies , estantería y demás objetos y para las unidades de conservación (carpetas y documentos)cada mes.
- **Prevención de Desastres:** Considerando la importancia de los archivos como memoria institucional y patrimonio documental, la prevención de desastres forma parte fundamental para lograr la permanencia, conservación y consulta de los acervos documentales no importa su medio. Así el Hospital debe plantear el mapa de riesgos con el propósito de realizar acciones tendientes a la mitigación del riesgo latente.

10 ADQUISICIÓN, ACTUALIZACIÓN Y LICENCIAMIENTO DE SOFTWARE

La institución adquiere software libre, licenciado y actualizaciones para prevenir vulnerabilidades y mantener los aplicativos actualizados de acuerdo a la normatividad vigente.

H2
H2
H2

11 USO RESPONSABLE DE ACTIVOS Y RECURSOS

11.1. Intranet

El acceso a la intranet del Hospital Universitario San José de Popayán E.S.E. es exclusivo de funcionarios que realizan actividades en los procesos administrativos y asistenciales de la institución y la información en ella contenida es de su interés.

11.2 Internet

- El acceso a internet del Hospital Universitario San José de Popayán está restringido al personal que labora en las áreas administrativas y asistenciales de la institución de acuerdo a la disposición del administrador de red del hospital.

- Así mismo se realiza el control de acceso a los contenidos encontrados en la web, de tal forma que existe un listado de sitios excluidos sin excepción y sitios con permisos parciales, los cuales deberán estar referenciados, para un buen uso de este recurso.

11.3 Correo electrónico

- Los correos electrónicos institucionales asignados a cada dependencia o funcionario en ejercicio de sus funciones es para uso exclusivo de comunicaciones oficiales y en ningún caso para temas personales.

- Está prohibido el uso del correo electrónico para inscripciones a concursos, redes sociales o cualquier otro tipo de actividad que no tenga relación directa con las funciones asignadas y que contenga información que se considere de importancia para el Hospital Universitario San José de Popayán.

- Cada usuario responsable de las cuentas de correo institucionales debe revisar, responder y eliminar los correos no deseados o que no se requieran para liberar espacio en el servidor.

11.4 Equipos, archivos, dispositivos removibles

- Es responsabilidad de cada funcionario dar un uso adecuado a los equipos, archivos y demás mecanismos para el procesamiento de información que son entregados por parte del Hospital Universitario San José de Popayán, evitando la manipulación indebida de los mismos.

44

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

MAN-SIS-01

Versión: 03

Página 15 de 21



- Se encuentra prohibido el uso de dispositivos removibles como memoria USB, discos duros en las áreas asistenciales del Hospital Universitario San José de Popayán.
- Es responsabilidad de cada funcionario el correcto transporte y salvaguarda de dispositivos removibles que no son proporcionados por el hospital, dado que no son en todo caso una herramienta recomendable para el almacenamiento de información.
- El hospital como medida de seguridad bloqueara el uso de dispositivos removibles o memorias USB para evitar el mal uso de estas con fines diferentes a los legalmente contemplados por la institución.

11.5 Recursos Compartidos

- El uso de recursos compartidos como carpetas publicas sin configuración de seguridad, solo está permitido para información que no es relevante para la institución o que por su nivel de importancia no tiene altos niveles de confidencialidad.
- Los recursos compartidos se encuentran habilitados y aceptados a través de protocolo de transferencia de archivos ftp, con las medidas de seguridad que se consideren desde el área de sistemas de información.

12 CONTROL DE ACCESO A LA INFORMACIÓN

12.1 Acceso a la red cableada e inalámbrica

- Los equipos de cómputo propiedad del Hospital Universitario San José, cuentan con acceso a la red cableada de la institución previa configuración.
- A la red inalámbrica del Hospital Universitario San José tiene acceso todo personal o tercero que requiera una conexión a la información contenida en los dispositivos de la institución, previa autorización y configuración del área de sistemas de información.
- No tienen acceso a la red inalámbrica los dispositivos móviles celulares.

HE

HU

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

MAN-SIS-01

Versión: 03

Página 16 de 21



12.2. Perfiles de Usuarios

- Desde el proceso de Administración y Almacenamiento de la información está definido un esquema de perfiles de acceso a la información de acuerdo al rol que desempeña cada empleado dentro de la institución.
- Para los documentos físicos almacenados de propiedad del Hospital Universitario San José de Popayán también están definidos unos niveles de acceso de acuerdo a las funciones dentro de la institución; el área de estadística y archivo es la responsable de la salvaguarda de los soportes físicos de historia clínica y documental respectivamente.
- Para los documentos físicos almacenados en los archivos de Gestión, Central e Histórico de propiedad del Hospital Universitario San José de Popayán también están definidos unos niveles de acceso de acuerdo a las funciones dentro de la institución, adhiriéndose a los procedimientos estandarizados para la consulta y préstamos de los mismos.

12.3 Gestión de contraseñas

- Las contraseñas asignadas para gestión de servicios informáticos y servidores deben cambiarse cada 30 días; la contraseña del usuario SQL para acceso a la Base de Datos se cambiará cada 6 meses, las contraseñas deben ser robustas, con combinación de letras mayúsculas y minúsculas, números y caracteres especiales.
- Estas contraseñas son almacenadas en un archivo seguro, no compartido y es gestionado y actualizado por el coordinador del área de sistemas de información.
- Las cuentas de usuario en los equipos para uso de los clientes internos tienen permisos de administración, los equipos tienen un nombre registrado en el dominio que corresponde al área de servicio, las contraseñas para los equipos se conforman por 8 caracteres alfanuméricos que corresponden a la letra inicial del servicio en mayúscula, seguida de los números del uno al seis y el símbolo asterisco.
- La contraseña de los usuarios de los principales sistemas es única, administrada desde dinámica gerencial hospitalaria, la cual debe ser cambiada cada 3 meses. Las contraseñas por defecto deben ser cambiadas al primer ingreso.

HA

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

MAN-SIS-01

Versión: 03

Página 17 de 21



12.4 Procedimiento para asignación de claves de acceso

- Los usuarios deberán solicitar en la oficina de Talento Humano el formato de Hoja de Ruta para iniciar el proceso de ingreso y asignación de claves a los diferentes aplicativos.
- Una vez autorizado el ingreso por talento humano, se procede a crear los usuarios y contraseñas al aplicativo institucional Dinámica Gerencial Hospitalaria .Net y demás aplicativos auxiliares según necesidad.
- Con el documento del nuevo usuario se procede a crear el usuario en Dinámica Gerencial Hospitalaria .Net; si es médico, enfermero, auxiliar de enfermería, bacteriólogo, terapeuta, etc.
- Se define como usuario el número del documento y la contraseña de ingreso debe tener mínimo 8 caracteres entre números, letras y un carácter especial.
- Se configuran las opciones: días de caducidad de la contraseña a 30 días y 6 fallos de contraseña; además de chequear el control respectivo cuando el usuario es de tipo asistencial (médicos y enfermeras).
- Se crea el usuario con los códigos definidos así: Médicos especialistas (ME), Médicos Generales (MG), Enfermeras (ENF), Auxiliares de Enfermería (AUX), Bacteriólogo (BC), Facturadores (FAC), Fonoaudiólogo (FN), Fisioterapeuta (FS), Psicólogo (PS).
- Se captura la firma que aparecerá en los folios de la historia clínica electrónica al personal médico y de enfermería.
- Se crea como tercero el usuario para efectos contables.
- Se autoriza el uso de los respectivos diseños de historias clínicas, según el área donde vaya a laborar el médico o enfermera.
- Se asignan los turnos al personal de enfermería que labora por sistema de turnos.
- Se autorizan los almacenes dependiendo de los servicios donde vaya a laborar el personal médico o de enfermería.
- Se autorizan las áreas de servicio dependiendo de los servicios donde vaya a laborar el personal médico o de enfermería.

Handwritten signatures and initials in the bottom right corner.

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

MAN-SIS-01

Versión: 03

Página 18 de 21



12.5 Transmisión del Dato:

Un sistema de comunicación de datos tiene como objetivo el transmitir información desde una fuente a un destinatario a través de una canal.

- El emisor o transmisor debe convertir la señal a un formato que sea reconocible por el canal.
- El canal conecta al emisor (E) y receptor (R) y puede ser cualquier medio de transmisión (fibra óptica, cable coaxial, aire,...).
- El receptor acepta la señal del canal y la procesa para permitir que el usuario final la comprenda

Se denomina red de transmisión de datos al conjunto formado por los equipos y los medios físicos y lógicos que permiten la comunicación de información entre diferentes usuarios a cualquier distancia que se encuentren. Estas redes pueden ser de ámbito local (LAN) o de ámbito global (WAN).

El Hospital Universitario San José de Popayán, se cuenta con una infraestructura de red LAN certificada con cableado categoría 6A la cual es administrada y gestionada por el área de Administración y Almacenamiento de la Información, el acceso a la red y la gestión de usuarios de red se realiza desde un servidor de dominio por medio de la herramienta ACTIVE DIRECTORY (directorio activo) de Windows server, que nos permite crear los usuarios para el inicio de sesión de los mismos en la red.

Dentro de los servicios de red establecidos en el Hospital para los usuarios se tiene: acceso de red local, acceso remoto, archivos, impresión, correo electrónico, plataformas de información estratégica, internet y backups.

La habilitación de las redes y prestación de servicios de red se tramitará únicamente en el proceso de administración y almacenamiento de la información de la institución.

Toda estación de trabajo conectada a la red de datos institucional (red de transmisión) transmite a través del canal LAN la información en tiempo real en los aplicativos misionales como en aquellas plataformas de MINSALUD necesarias para el desempeño de las actividades propias de la Institución. Esta información llega a los servidores institucionales de manera oportuna, confiable y veraz, cuyos niveles de seguridad y de gestión del riesgo garantizan la permanencia del dato y la prevención en su manipulación no autorizada y/o ataques informáticos.

44

13 GESTIÓN DE SEGURIDAD PARA TELECOMUNICACIONES E INFRAESTRUCTURA

13.1 Antivirus

Todo equipo de propiedad del Hospital Universitario San José de Popayán tiene instalado el antivirus adquirido y licenciado para la institución, el cual es administrado desde el servidor central con las configuraciones definidas por el administrador del sistema, por ejemplo bloqueo de memorias, tiempos de actualización, mensajes de alerta, filtros aplicables, etc.

13.2 Protección perimetral

El acceso a la red interna del Hospital Universitario San José de Popayán está protegida por cortafuegos, que permita proteger la información de la institución de accesos no autorizados, desde la red interna como desde redes externas (Internet).

13.3 Copias de seguridad de configuraciones en servidores

Las copias de seguridad de las configuraciones básicas y de información almacenada en los principales servidores y la información de interés de la institución se realizan de acuerdo al procedimiento de realización de copias de seguridad, y respecto a las copias de seguridad de las estaciones de trabajo de los diferentes procesos y servicios estará a cargo del coordinador del proceso y/o usuario final del equipo para lo cual se deberá solicitar a través de la mesa de ayuda o el mecanismo que lo reemplace el apoyo técnico del proceso de Sistemas de Información.

13.4 Planes de contingencia

La institución cuenta con un procedimiento de contingencia de la información el cual contempla un anexo que dispone del plan de contingencia para las diferentes eventualidades como:

- Recuperación en caso de interrupción de la infraestructura tecnológica.
- Recuperación en caso de falla de equipos electrónico y hardware.
- Recuperación de datos ante fallas de ordenadores portátiles.
- Recuperación en caso de daño debido a fuego o líquidos.
- Recuperación en caso de acción de virus.
- Recuperación en caso de robo de datos

En este procedimiento se planean y ejecutan las tareas destinadas a asegurar la persistencia de la información que se genera en el Hospital, a restituir rápidamente los sistemas de información institucionales ante la eventual presencia de siniestros que los paralicen parcial o totalmente y a prevenir la pérdida de información.

Handwritten signatures and initials in the bottom right corner.

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

MAN-SIS-01

Versión: 03

Página 20 de 21



13.5 Monitoreo del uso de sistemas

- El área de sistemas de información del Hospital Universitario San José de Popayán realiza monitoreo continuo o aleatorio a todos los sistemas administrados por el mismo y verifica el tipo de contenido e información que se está generando desde los distintos procesos de la institución.
- Para el monitoreo de la calidad de la información se ejecuta el procedimiento de gestión y minería de datos.
- Para medir la efectividad de las medidas adoptadas con el fin de garantizar la seguridad y confidencialidad de la información, están definidos los siguientes indicadores:

Número de casos reportados y confirmados de pérdida de información.

Número de caídas reportadas del sistema de información.

Cantidad de bits transmitidos en la Institución mensualmente

14 CONTROL DE CAMBIOS

Código	Versión	Fecha	Descripción del Cambio
MAN-GI-01	0-1	28/07/2015 27/06/2017	Creación de documento
MAN-SIS-01	2	16/12/2020	Modificación de código y ajustes de actividades
MAN-SIS-01	3	Octubre de 2021	Actualización e inclusión de transmisión del dato

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

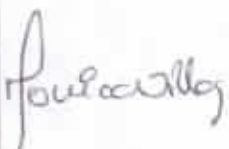
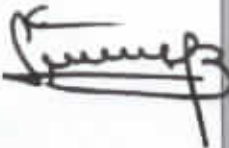
MAN-SIS-01

Versión: 03

Página 21 de 21



**HOSPITAL
UNIVERSITARIO
SAN JOSE**
UNIVERSIDAD NACIONAL CARRERAS DE CIENCIAS DE LA SALUD

Elaboró	Faiver Tovar Nogales Mónica Villegas Noguera	Revisó	Lucy Ximena Ibarra Hernández.	Aprobó	Cesar Edmundo Samia Porras
Cargo	Lider Administración y Almacenamiento de la Información Afiliado Participe Admisalud Profesional Administrativa Administración y Almacenamiento de la Información Afiliado Participe Admisalud	Cargo	Subgerente Administrativa	Cargo	Gerente
Firma	 	Firma		Firma	
Fecha		Fecha		Fecha	11 NOV 2021
GESTION DOCUMENTAL					
Nombre:	Hulber Enrique Acosta	Cargo:	Profesional Universitario. Oficina Asesora de Planeación - Afiliado Admisalud	Firma:	