

	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PO-001
	PROCESO: GESTIÓN TECNOLOGIA DOCUMENTAL SUBPROCESO SISTEMAS DE INFORMACIÓN	VERSIÓN: 01 FECHA: 29/09/2023
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA: 1 de 11

1. INTRODUCCION

Con la definición de las políticas y estándares de seguridad informática se busca crear conciencia y establecer al interior del ESE Hospital San Vicente de Arauca una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le puedan llegar a afectar.

El Hospital San Vicente de Arauca ESE., entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

2. OBJETIVO GENERAL

Garantizar la confidencialidad, integridad y disponibilidad de la información identificando los riesgos que le puedan llegar a afectar y estableciendo estrategias que permitan disminuir su impacto en la seguridad y confidencialidad de la información.

3. OBJETIVO ESPECIFICOS

- Crear una cultura de apropiación de la seguridad y privacidad de la información en el Hospital San Vicente de Arauca ESE.
- Gestionar los riesgos de seguridad de la información a fin de mitigar los impactos negativos ante una eventual materialización de los mismos.
- Actualizar, definir e implementar acciones de la política de seguridad y privacidad de la información en el mapa de riesgo del proceso de Sistemas.

4. ALCANCE

Esta política es transversal a todos los procesos y procedimientos institucionales Hospital San Vicente de Arauca ESE, aplica a todos los usuarios internos y externos de la ESE. (Funcionarios, contratistas, consultores, pasantes, proveedores de bienes, entidades del Estado, entes de control) y otros terceros que desempeñen alguna actividad en las instalaciones del Hospital.

5. RESPONSABLE

Profesional de Sistemas del Hospital San Vicente de Arauca.

6. MARCO LEGAL Y NORMATIVO

- Ley 23 de 1982: Ley de propiedad intelectual y derechos de autor.

“Trabajando por la Salud del pueblo Araucano”

Calle 15 16-17 Esquina. PBX (097) – 8850030-Correo electrónico: contactenos@hospitalsanvicente.gov.co

Página Web: www.Hospitalsanvicente.gov.co- Facebook Hospital San Vicente Arauca- Twitter: @SanArauca-

YouTube: Hospital San Vicente de Arauca, Arauca / Colombia

	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PO-001
	PROCESO: GESTIÓN TECNOLOGIA DOCUMENTAL SUBPROCESO SISTEMAS DE INFORMACIÓN	VERSIÓN: 01
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	FECHA: 29/09/2023
		PÁGINA: 2 de 11

- Constitución Política de Colombia de 1991: Artículo 15 consagra que “Todas las personas tienen el derecho a su intimidad personal y familiar y a su buen nombre. De igual modo, tienen el derecho a conocer, actualizar y a rectificar las informaciones que hayan recogido sobre ellas en los bancos de datos y en los archivos de las entidades públicas y privadas”.
- Ley 527 de 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 594 de 2000: Reglamentada parcialmente por los Decretos Nacionales 4124 de 2004, 1100 de 2014. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
- Ley 603 DE 2000: Esta ley se refiere a la protección de los derechos de autor en Colombia. El software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.
- Ley 962 de 2005: Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas.
- Ley 1266 de 2008, Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Resolución 1995 de 1999: Normas para el Manejo de la Historia Clínica.
- Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Ley 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 2578 de 2012: Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye “El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles” entre otras disposiciones.
- Decreto 2609 de 2012: Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.
- Norma técnica colombiana NTC/ISO 27001:2013: Sistema de seguridad de la Información

“Trabajando por la Salud del pueblo Araucano”

	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PO-001
	PROCESO: GESTIÓN TECNOLOGIA DOCUMENTAL SUBPROCESO SISTEMAS DE INFORMACIÓN	VERSIÓN: 01 FECHA: 29/09/2023
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA: 3 de 11

- Norma ISO 27001: Sistemas de Gestión de la Seguridad de la Información.
- Ley 1712 DE 2014: Ley de Transparencia y del derecho de acceso a la información pública nacional.
- Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- CONPES 3854 de 2016: Política Nacional de Seguridad Digital.
- Decreto 612 de 2018: Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Decreto 1008 de 2018: Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015. Tiene como principio la seguridad de la información, que busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

7. TERMINOS Y DEFINICIONES

Política: Conjunto de normas internas que se diseñan para regular y delimitar las reglas de conducta dentro de una organización. Describen las responsabilidades tanto de los empresarios y altos cargos como de los empleados en todos los niveles jerárquicos.

Información: conjunto organizado de datos relevantes para uno o más sujetos que extraen de él un conocimiento.

Sistemas de información: conjunto de datos y procedimientos que interactúan entre sí y ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales y las particularidades de cada organización.

Activos Informáticos: Son los recursos tecnológicos (hardware y software) de la información y la comunicación (TIC) que emplea para gestionar la información que maneja.

Hardware: Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

Software: Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

“Trabajando por la Salud del pueblo Araucano”

	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PO-001
	PROCESO: GESTIÓN TECNOLOGIA DOCUMENTAL SUBPROCESO SISTEMAS DE INFORMACIÓN	VERSIÓN: 01 FECHA: 29/09/2023
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA: 4 de 11

Buzón de correo: Un buzón de correo también se denomina cuenta de e-mail. El buzón de correo electrónico recoge todos los correos electrónicos que el usuario ha enviado y recibido desde y hacia su dirección de correo electrónico.

E-mail: Es un mensaje digital que se transmite mediante una red informática.

Aplicación: Es un software que ha sido diseñado para cubrir una necesidad o realizar una tarea concreta dentro de un dispositivo electrónico como una tablet, un Smartphone o un computador.

Red: Conjunto de dispositivos que se encuentran interconectados entre sí a través de un medio, estos intercambian información y comparten recursos.

Firma Digital: Es un sello de autenticación electrónico cifrado en información digital, como mensajes de correo, macros o documentos electrónicos.

Antivirus: Es un tipo de software que se utiliza para evitar, buscar, detectar y eliminar virus de una computadora.

Virus: Un virus es un tipo de malware – un programa perjudicial creado por piratas informáticos que puede infectar tu computadora o dispositivo en varias formas.

Dirección IP: Es una dirección única que identifica a un dispositivo en internet o en una red local.

Periféricos: Son los dispositivos a través de los cuales el ordenador se comunica con el mundo exterior tales como: impresoras, teclados, mouse, escáner, entre otros.

Regulador de voltaje: Dispositivo mantener el voltaje estable en una línea eléctrica para evitar daños y fallas en los equipos energizados.

UPS: dispositivo que gracias a sus baterías y demás elementos encargados de almacenar energía, puede proporcionar o suministrar energía eléctrica durante algún apagón eléctrico por un tiempo limitado.

Data center: Centro de Procesamiento de los Datos. Un lugar en el que se albergan todos los recursos necesarios para el procesamiento de los datos de una organización.

Switch: dispositivo informático que permite interconectar dispositivos a través de una red de área local o red LAN.

“Trabajando por la Salud del pueblo Araucano”

	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PO-001
	PROCESO: GESTIÓN TECNOLOGIA DOCUMENTAL SUBPROCESO SISTEMAS DE INFORMACIÓN	VERSIÓN: 01 FECHA: 29/09/2023
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA: 5 de 11

LAN: Una red de área local conecta dispositivos dentro de una proximidad relativamente cercana.

Bitácora: Registro oficial de eventos durante un periodo de tiempo en particular.

Internet: red de computadoras interconectadas entre sí a nivel mundial con el objetivo de hacer común información de acceso público.

Streaming: Tecnología que permite ver y oír contenidos que se transmiten desde internet u otra red sin tener que descargar previamente los datos al dispositivo desde el que se visualiza y oye el archivo.

8. CONDICIONES GENERALES

8.1 PRINCIPIOS DE SEGURIDAD QUE SOPORTAN EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE NOMBRE DE LA ENTIDAD

Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios y proveedores de la entidad o terceros.

El Hospital San Vicente de Arauca protegerá la información generada, procesada o resguardada por los procesos de la entidad, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes).

8.2 DEBERES

Hay que tener en cuenta que: La ley 734 de 2002 en su artículo 48, considera una falta gravísima lo siguiente: “Artículo 48. Faltas gravísimas. Son faltas gravísimas las siguientes: Causar daño a los equipos estatales de informática, alterar, falsificar, introducir, borrar, ocultar o desaparecer información en cualquiera de los sistemas de información oficial contenida en ellos o en los que se almacene o guarde la misma, o permitir el acceso a ella a personas no autorizadas.”

Estas políticas de seguridad informática establecidas en el presente documento son la base fundamental para la protección de los activos informáticos y de toda la información de la institución.

Se establecen entonces los siguientes deberes que deberán ser acogidos por todos los usuarios internos y externos de la ESE. (Funcionarios, contratistas, consultores, pasantes, proveedores de bienes, entidades del Estado, entes de

“Trabajando por la Salud del pueblo Araucano”

Calle 15 16-17 Esquina. PBX (097) – 8850030-Correo electrónico: contactenos@hospitalsanvicente.gov.co

Página Web: www.Hospitalsanvicente.gov.co- Facebook Hospital San Vicente Arauca- Twitter: @SanArauca- YouTube: Hospital San Vicente de Arauca, Arauca / Colombia

	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PO-001
	PROCESO: GESTIÓN TECNOLOGIA DOCUMENTAL SUBPROCESO SISTEMAS DE INFORMACIÓN	VERSIÓN: 01 FECHA: 29/09/2023
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA: 6 de 11

control) y otros terceros que desempeñen alguna actividad en las instalaciones de la entidad:

- Todos los usuarios internos y externos de la ESE. (, funcionarios, contratistas, consultores, pasantes, proveedores de bienes, entidades del Estado, entes de control) y otros terceros que desempeñen alguna actividad en las instalaciones del Hospital debe aceptar las Políticas de confidencialidad de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el Política General De Seguridad Y Privacidad De La Información.
- Los accesos a las páginas Web a través de los navegadores deben sujetarse a las normas que previamente se manifiestan por la oficina de sistemas.
- La historia clínica es un documento privado, sometido a reserva, que únicamente puede revelarse a un tercero previa autorización del paciente o en los casos previstos por la ley. Las personas pueden exigir que su historia clínica sea tratada de manera confidencial y reservada.
- No está permitido el uso del correo personal. Los correos institucionales deben ser para uso exclusivo de las actividades de la ESE Hospital San Vicente de Arauca.
- Los mensajes y la información contenida en los buzones de correo son de propiedad del Hospital.
- Cualquier aplicación, archivo desconocido o sospechoso ya sea en correos electrónicos o en los archivos del equipo del usuario no deberán ser abierto y deberá ser reportado al área de Sistemas, que procederá a examinar y determinar si la aplicación o archivo es potencialmente peligrosa para el equipo o la red de la entidad.
- No está permitido extraer información por ningún medio y bajo sin autorización manifiesta del líder del área a quien corresponda dicha información.
- Atender todas lo dispuesto en la Ley 527 de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

8.3 GESTION DE ACTIVOS

- Los equipos informáticos deben ser ubicados en espacios y conexión eléctrica adecuados que garanticen su buen funcionamiento y no exposición a ambientes de calor y/o humedad que puedan afectar su rendimiento y su vida útil.
- La protección física de los equipos corresponde a quienes en un principio se le asigna, y corresponde notificar los movimientos en caso de que existan, a la oficina de sistemas.
- El área de sistemas debe tener debidamente registrados todos los equipos propiedad del hospital y deberá estar paqueteado y relacionado en el inventario del área y a cargo del funcionario al cual se ha asignado.

“Trabajando por la Salud del pueblo Araucano”

Calle 15 16-17 Esquina. PBX (097) – 8850030-Correo electrónico: contactenos@hospitalsanvicente.gov.co
Página Web: www.Hospitalsanvicente.gov.co- Facebook Hospital San Vicente Arauca- Twitter: @SanArauca-
YouTube: Hospital San Vicente de Arauca, Arauca / Colombia

	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PO-001
	PROCESO: GESTIÓN TECNOLOGIA DOCUMENTAL SUBPROCESO SISTEMAS DE INFORMACIÓN	VERSIÓN: 01
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	FECHA: 29/09/2023
		PÁGINA: 7 de 11

- Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
- Todo equipo informático conectado a la red del hospital debe contar con los elementos mínimos de protección (antivirus) debidamente licenciados y actualizados. En los casos en que el usuario inhabilite esta funcionalidad será responsable por los daños causados.
- Cualquier traslado o reubicación de los equipos deben ser realizados solo por el personal del área de sistemas previa solicitud del funcionario quien tenga a cargo dicho elemento.
- Todos los empleados y usuarios de partes externas deben devolver todos los activos de la Entidad que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
- Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
- Toda persona (funcionario, contratista o tercero) que utilice los recursos informáticos, tiene la responsabilidad de velar por su integridad, confidencialidad y disponibilidad de la información como lo señala el Código Único Disciplinario (Ley 734 de 2002) Art. 34 Num. 22: “Son deberes de todo servidor público: Responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización.”

8.4 ACCESO A LA INFORMACIÓN Y CONTROL DE USUARIOS

- Todas los funcionarios, contratistas y/o terceros autorizados que laboran en el hospital deberán ingresar con nombres de usuario y claves que serán asignados por el área de sistemas previa autorización escrita del líder de área informando en que módulos va a trabajar, repositorios de información a los cuales tendrá acceso y cuáles son las funciones asignadas. La contraseña asignada por defecto para el caso del software institucional Dinámica Gerencial deberá ser cambiada por el usuario al momento de ingresar por primera vez a la aplicación.
- Los usuarios deberán renovar periódicamente su clave de acceso al sistema. Estas claves deberán ser único conocimiento del usuario y esta terminante mente prohibido acceder a servicios informáticos utilizando cuentas, claves, contraseñas de otros usuarios. Aún con la autorización expresa del usuario propietario de la misma. En caso de olvido de la contraseña se debe solicitar a la oficina de sistemas la restauración de la misma.
- No se permiten accesos de trabajo remoto sin autorización del área de sistemas. Toda cuenta de acceso al sistema, a la red y direcciones IP, será asignada por la oficina de Sistemas previa solicitud por escrito.

“Trabajando por la Salud del pueblo Araucano”

	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PO-001
	PROCESO: GESTIÓN TECNOLOGIA DOCUMENTAL SUBPROCESO SISTEMAS DE INFORMACIÓN	VERSIÓN: 01
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	FECHA: 29/09/2023
		PÁGINA: 8 de 11

- Los accesos a los servicios bancarios vía web a nombre de la ESE Hospital San Vicente de Arauca, solamente podrán ser utilizados por el jefe de tesorería y únicamente en el equipo que este tenga asignado.
- Las usuarios y contraseñas de acceso a las plataformas web externas al hospital son se salvaguarda de los líderes de cada proceso.
- Cuando un funcionario, contratista o tercero se desvincule del Hospital San Vicente de Arauca ESE, el área de sistemas procederá a desactivar sus cuentas de usuario antes de formalizar su retiro, previa solicitud del área de talento humano si se trata de un funcionario de planta o de la subdirección administrativa si es el caso de un contratista o tercero.
- Las cuentas de usuario que sean otorgadas a terceros (personas que no sean empleados del Hospital) deberán ser autorizadas por la dirección. Estas cuentas expiraran en el término de 30 días. En caso de ser necesario extender su uso se deberá contar nuevamente con autorización de la Dirección.

8.5 USO DE EQUIPOS DE CÓMPUTO

- Los usuarios no pueden cambiar las configuraciones tanto de hardware como software. En caso de requerirlo solo lo puede hacer personal del área de sistemas previa solicitud del líder del proceso o servicio.
- No se permite la descargar descarga y/o instalación de aplicaciones. En caso de requerirse solo lo hará el personal del área de sistemas.
- Tanto los equipos de cómputo como demás periféricos así como las herramientas software son de uso exclusivo del Hospital San Vicente de Arauca y deben ser utilizadas exclusivamente en pro del desarrollo de sus funciones y responsabilidades establecidas por y para la ESE.
- Los equipos deben estar conectados a una red eléctrica regulada o en su defecto a reguladores de voltaje y en los servidores deben usarse fuentes de poder interrumpibles (UPS).
- Los equipos no podrán salir del Hospital sin previa autorización escrita del Jefe inmediato y visto bueno del líder del área de sistemas y visto bueno de almacén.
- Para la asignación de equipos nuevos se debe hacer la solicitud por escrito a el área de sistemas con el visto bueno del Jefe inmediato, se procede a entregar el computador mediante acta, con el respectivo visto bueno de suministros para el paqueteo del activo e ingreso al inventario de sistemas; previa entrega del equipo a reemplazar por parte del solicitante, en caso de reemplazo.
- Se deben procurar medidas de protección (como el uso de vigilancia privada, cerradura con llave y cámaras de video con grabación continua) para equipos en aras de disminuir riesgos de robo, destrucción o uso inadecuado.
- Todo el personal que labora en la entidad deberá está comprometido a cumplir las siguientes normas básicas en aras del cuidado de los equipos suministrados para la ejecución de sus funciones y tareas:

“Trabajando por la Salud del pueblo Araucano”

	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PO-001
	PROCESO: GESTIÓN TECNOLOGIA DOCUMENTAL SUBPROCESO SISTEMAS DE INFORMACIÓN	VERSIÓN: 01 FECHA: 29/09/2023
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA: 9 de 11

- No ingerir, ni dejar alimentos y/o bebidas cerca y/o encima de los equipos.
- Procurar siempre una buena la ventilación de los equipos (no colocar papeles u otros objetos cerca o sobre de las ranuras de ventilación)
- Mantener alejados de la CPU, monitor y pantalla todo elemento electromagnético como imágenes.
- No ubicar los equipos de cómputo en el piso o lugares inestables y/o expuestos a ser golpeados de manera accidental o involuntaria.
- Trasladar ni cambiar de ubicación los equipos y/o periféricos. Cualquier traslado o reubicación de los equipos deben ser realizados solo por el personal del área de sistemas previa solicitud del funcionario quien tenga a cargo dicho elemento.
- No abrir las carcasas de los equipos de cómputo y/o periféricos, en caso de ser necesario, solo lo podrá hacer el personal del área de sistemas.
- Mantener limpios los equipos de cómputo y periféricos (teclado, monitor, mouse, escáneres e impresoras) mediante limpieza externa.
- Procurar mantener los cables en buen estado, organizados y debidamente conectados; no debe de existir ningún tipo de tensión, evitando el doblado de los mismos.
- No conectar aparatos con motor eléctrico como ventiladores u otros aparatos en los mismos enchufes de los equipos de cómputo.

8.6 USO Y ADMINISTRACION DE REDES

- Los cambios en servidores y equipos de red del Hospital, así como la instalación de nuevo software, el cambio de direcciones IP, la reconfiguración de routers y switches, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Lo anterior con el fin de evitar problemas que puedan causar interrupción de las comunicaciones, caída de la red, acceso de servicio a información confidencial.
- Los servidores de red y los equipos de comunicación serán ubicados en centros de cómputo apropiados, protegidos contra daños y robo; y con las condiciones de infraestructura física, ambientales y eléctricas necesarias para su correcto funcionamiento.
- El área de sistemas deberá contar con una Bitácora de acceso al Data center restringiendo el acceso solo a personal autorizado.

8.6.1 MANEJO DE COPIAS DE SEGURIDAD

- El Hospital debe contar con un procedimiento claro y documentado de manejo de copias de seguridad y salvaguarda de la información.
- La entidad deberá dejar registro pruebas de restauración de copias de seguridad mediante actas.
- El Hospital debe contar con una bitácora dl registro de copias de seguridad realizadas y de restauraciones de la misma.

“Trabajando por la Salud del pueblo Araucano”

Calle 15 16-17 Esquina. PBX (097) – 8850030-Correo electrónico: contactenos@hospitalsanvicente.gov.co

Página Web: www.Hospitalsanvicente.gov.co- Facebook Hospital San Vicente Arauca- Twitter: @SanArauca-

YouTube: Hospital San Vicente de Arauca, Arauca / Colombia

	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PO-001
	PROCESO: GESTIÓN TECNOLOGIA DOCUMENTAL SUBPROCESO SISTEMAS DE INFORMACIÓN	VERSIÓN: 01 FECHA: 29/09/2023
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA: 10 de 11

8.6.2 USO DE INTERNET

- La asignación de acceso a Internet a los equipos de la entidad debe ser solicitada por el líder de área a la oficina de sistemas justificando la necesidad e informando los sitios a los cuales requiere acceso.
- El Área de sistemas se encargará de administrar el servicio de internet, y se debe, controlar o bloquear páginas según su criterio y que no son necesarias para el desempeño de las funciones de los usuarios, esto con el fin de disminuir riesgos para la seguridad de la información en el Hospital.
- El servicio de internet no debe ser usado para fines personales, y está prohibido instalar o utilizar herramientas de descargas de archivos, así como ingresar páginas para adultos y/o sexo explícito o a páginas de entretenimiento (Streaming).
- Está terminantemente prohibido el ingreso a páginas de apuestas en línea, minado de criptomonedas y trading.
- Toda información publicada en la página institucional del Hospital debe ser acorde a la normatividad y por solicitud del área interesada, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).

9. PLAN DE ACCIÓN

Formato en Excel Plan de Acción

10. BIBLIOGRAFÍA

Procedimientos de seguridad de la información

[https://www.mintic.gov.co/gestionti/615/articles5482_G3_Procedimiento de Seguridad.pdf](https://www.mintic.gov.co/gestionti/615/articles5482_G3_Procedimiento_de_Seguridad.pdf)

Guía para la gestión y clasificación de activos de información

[https://www.mintic.gov.co/gestionti/615/articles5482_G5_Gestion Clasicacion.pdf](https://www.mintic.gov.co/gestionti/615/articles5482_G5_Gestion_Clasicacion.pdf)

Plan de capacitación, sensibilización y comunicación de seguridad de la información

[https://www.mintic.gov.co/gestionti/615/articles5482_G14_Plan comunicacion sensibilizacion.pdf](https://www.mintic.gov.co/gestionti/615/articles5482_G14_Plan_comunicacion_sensibilizacion.pdf)

Modelo de seguridad y privacidad de la información

[https://www.mintic.gov.co/gestionti/615/articles5482_Modelo de Seguridad Privacidad.pdf](https://www.mintic.gov.co/gestionti/615/articles5482_Modelo_de_Seguridad_Privacidad.pdf)

“Trabajando por la Salud del pueblo Araucano”

Calle 15 16-17 Esquina. PBX (097) – 8850030-Correo electrónico: contactenos@hospitalsanvicente.gov.co

Página Web: www.Hospitalsanvicente.gov.co- Facebook Hospital San Vicente Arauca- Twitter: @SanArauca-

YouTube: Hospital San Vicente de Arauca, Arauca / Colombia

	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PO-001
	PROCESO: GESTIÓN TECNOLOGIA DOCUMENTAL SUBPROCESO SISTEMAS DE INFORMACIÓN	VERSIÓN: 01
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	FECHA: 29/09/2023
		PÁGINA: 11 de 11

CONTROL DE DOCUMENTO

Este documento debe reposar en el proceso de Gestión de Sistemas de Información

CONTROL DE DOCUMENTO				
VERSION	FECHA APROBACIÓN			MOTIVO
	DÍA	MES	AÑO	
01	02	10	2023	Creación del documento

ELABORÓ/ACTUALIZO FIRMA:	REVISO FIRMA:	VIABILIZÓ: FIRMA:	APROBO: FIRMA:
Freddy Cabrera	Sara Eddy Maldonado Ana Isabel Cely Abril	Claudia Genara Pérez	Comité institucional de gestión y desempeño
Líder del proceso de Sistemas de Información	Líder del proceso de Gestión y Garantía de la Calidad Profesional de apoyo del proceso Gestión y Garantía de la calidad	Subdirección Administrativa	CARGO: Acta de Comité No. 005 del 2023
29/09/2023	29/09/2023	29/09/2023	02 de octubre del 2023

“Trabajando por la Salud del pueblo Araucano”

Calle 15 16-17 Esquina. PBX (097) – 8850030- Correo electrónico: contactenos@hospitalsanvicente.gov.co
Página Web: www.Hospitalsanvicente.gov.co- Facebook Hospital San Vicente Arauca- Twitter: @SanArauca-
YouTube: Hospital San Vicente de Arauca, Arauca / Colombia