 <p>E.S.E. Hospital San Vicente Ramiriquí</p>	SISTEMA INTEGRADO DE GESTIÓN	
	POLITICA DE SEGURIDAD DIGITAL	Código: POL-SD-ES-DE-001
		Versión: 00
		Fecha: 16/10/2020
	Página: 1 de 14	


POLÍTICA SEGURIDAD DIGITAL Y SEGURIDAD DE LA INFORMACIÓN

**EMPRESA SOCIAL DEL ESTADO HOSPITAL
SAN VICENTE DE RAMIRIQUÍ**

**SANDRA VIVIANA SAMPAYO DIAZ
GERENTE**

NIT 891800644-9
www.hospitalramiriqui.gov.co

Carrera 3 No. 7 - 21 Barrio Libertador Ramiriquí - Boyacá
Conmutador: 3114802222
E-mail: gerencia@hospitalramiriqui.gov.co / secretaria@hospitalramiriqui.gov.co

	SISTEMA INTEGRADO DE GESTIÓN	
	POLITICA DE SEGURIDAD DIGITAL	Código: POL-SD-ES-DE-001
		Versión: 00
		Fecha: 16/10/2020
		Página: 2 de 14

CONTENIDO

INTRODUCCIÓN	3
1. JUSTIFICACIÓN	4
2. MARCO LEGAL.....	5
3. DEFINICIONES.....	7
4. OBJETIVOS	11
4.1. Objetivo General	11
4.2. Objetivos Específicos.....	11
5. ALCANCE DE LA POLÍTICA	12
6. POLÍTICA DE SEGURIDAD DIGITAL	12
7. CUMPLIMIENTO.....	12
8. IMPLEMENTACIÓN	13
9. SEGUIMIENTO.....	14

NIT 891800644-9

www.hospitalramiriqui.gov.co

Carrera 3 No. 7 - 21 Barrio Libertador Ramiriquí - Boyacá

Conmutador: 3114802222

E-mail: gerencia@hospitalramiriqui.gov.co / secretaria@hospitalramiriqui.gov.co

	SISTEMA INTEGRADO DE GESTIÓN	
	POLITICA DE SEGURIDAD DIGITAL	Código: POL-SD-ES-DE-001
		Versión: 00
		Fecha: 16/10/2020
	Página: 3 de 14	

INTRODUCCIÓN

La política de Seguridad digital hace parte de Modelo Integrado de Planeación y Gestión MIPG el cual fue adoptado mediante decreto 1499 de 1 de septiembre de 2017 y aplica a todas las entidades y organismos públicos, independientemente de la su naturaleza jurídica.

La Política de Seguridad digital de la Empresa Social del Estado Hospital San Vicente de Ramiriquí se implementa con el fin de proteger los activos de información de la institución y minimizar los riesgos que propicien delitos informáticos.

Por lo anteriormente expuesto se establece la política de Seguridad digital de la Empresa Social del Estado Hospital San Vicente de Ramiriquí en cumplimiento al Modelo Integrado de Planeación y gestión MIPG.

NIT 891800644-9

www.hospitalramiriqui.gov.co

Carrera 3 No. 7 - 21 Barrio Libertador Ramiriquí - Boyacá

Conmutador: 3114802222

E-mail: gerencia@hospitalramiriqui.gov.co / secretaria@hospitalramiriqui.gov.co

	SISTEMA INTEGRADO DE GESTIÓN	
	POLITICA DE SEGURIDAD DIGITAL	Código: POL-SD-ES-DE-001
		Versión: 00
		Fecha: 16/10/2020
	Página: 4 de 14	

1. JUSTIFICACIÓN

La Empresa Social del Estado Hospital San Vicente de Ramiriquí responde al cumplimiento de los lineamientos del decreto 1499 de 2017 con el que se busca el fortalecimiento organizacional de la gestión de la entidad.

En cumplimiento de la tercera dimensión establecida en el Modelo Integrado de Planeación y Gestión “Gestión con valores para resultados” y la implementación de la política que integra, se logra cumplir con el objetivo del MIPG” Agilizar, simplificar y flexibilizar la operación de las entidades para la generación de bienes y servicios que resuelvan efectivamente las necesidades de los ciudadanos” y “Facilitar y promover la efectiva participación ciudadana en la planeación, gestión y evaluación de las entidades públicas”.

Resulta fundamental la formulación e implementación de la Política de Seguridad Digital de Empresa Social del Estado Hospital San Vicente de Ramiriquí, con el fin de garantizar la protección de los activos de información de la entidad y a los ciudadanos asegurar la integridad, confiabilidad y disponibilidad de la información.


NIT 891800644-9

www.hospitalramiriqui.gov.co

Carrera 3 No. 7 - 21 Barrio Libertador Ramiriquí - Boyacá

Conmutador: 3114802222

E-mail: gerencia@hospitalramiriqui.gov.co / secretaria@hospitalramiriqui.gov.co

	SISTEMA INTEGRADO DE GESTIÓN	
	POLITICA DE SEGURIDAD DIGITAL	Código: POL-SD-ES-DE-001
		Versión: 00
		Fecha: 16/10/2020
	Página: 5 de 14	

2.MARCO LEGAL

Ley 599 DE 2000: Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa.

ISO/IEC 27001:2005: Es la evolución certificable del código de buenas prácticas ISO 17799. Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.

ISO 27002:2005: Esta norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar e implantar o mantener sistemas de gestión de la seguridad de la información.

Ley 1341 DE 2009: Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

Ley 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, 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.

Decreto 2693 de 2012: Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y


NIT 891800644-9

www.hospitalramiriqui.gov.co

Carrera 3 No. 7 - 21 Barrio Libertador Ramiriquí - Boyacá

Conmutador: 3114802222

E-mail: gerencia@hospitalramiriqui.gov.co / secretaria@hospitalramiriqui.gov.co

 <p>E.S.E. Hospital San Vicente Ramiriquí</p>	SISTEMA INTEGRADO DE GESTIÓN	
	POLITICA DE SEGURIDAD DIGITAL	Código: POL-SD-ES-DE-001
		Versión: 00
		Fecha: 16/10/2020
	Página: 6 de 14	

las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

Decreto 1499 de 2017 Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015


NIT 891800644-9

www.hospitalramiriqui.gov.co

Carrera 3 No. 7 - 21 Barrio Libertador Ramiriquí - Boyacá

Conmutador: 3114802222

E-mail: gerencia@hospitalramiriqui.gov.co / secretaria@hospitalramiriqui.gov.co

	SISTEMA INTEGRADO DE GESTIÓN	
	POLITICA DE SEGURIDAD DIGITAL	Código: POL-SD-ES-DE-001
		Versión: 00
		Fecha: 16/10/2020
	Página: 7 de 14	

3. DEFINICIONES

Activo de información: es todo aquello que en la entidad es considerado importante o de alta validez para la misma ya que puede contener información importante como son las bases de datos con usuarios, contraseñas, números de cuentas, etc.

Amenaza cibernética: aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado.

Ataque cibernético: acción organizada o premeditada de una o más agentes para causar daño o problemas a un sistema a través del Ciberespacio.

Backup: Es una copia de seguridad o el proceso de copia de seguridad. Backup se refiere a la copia y archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.

Ciber defensa: es el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales.

Ciber espionaje: es el acto o práctica de obtener secretos sin el permiso del dueño de la información (personal, sensible, propietaria o de naturaleza clasificada) para ventaja personal, económica, política o militar en el Ciberespacio, a través del uso de técnicas malintencionadas.


Ciberterrorismo: es el uso del Ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o estado trayendo como consecuencia una violación a la voluntad de las personas.

Cibercrimen (delito cibernético): conjunto de actividades ilegales asociadas con el uso de las Tecnologías de la Información y las Comunicaciones, como fin o como medio.

Ciberlavado: es el uso del Ciberespacio, en cualquiera de sus formas, para dar apariencia de legalidad a bienes obtenidos ilícitamente o para ocultar dicha ilicitud ante las autoridades.

NIT 891800644-9
www.hospitalramiriqui.gov.co

Carrera 3 No. 7 - 21 Barrio Libertador Ramiriquí - Boyacá
 Conmutador: 3114802222
 E-mail: gerencia@hospitalramiriqui.gov.co / secretaria@hospitalramiriqui.gov.co

	SISTEMA INTEGRADO DE GESTIÓN	
	POLITICA DE SEGURIDAD DIGITAL	Código: POL-SD-ES-DE-001
		Versión: 00
		Fecha: 16/10/2020
	Página: 8 de 14	

Ciberseguridad: es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio.

Confidencialidad: la información no se pone a disponibilidad si se revela a individuos, entidades o procesos no autorizados.

Copias de respaldo: es un acopia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de pérdida.

Dato: es una representación simbólica (numérica, alfabética, algorítmica, especial etc) de un atributo o variable cuantitativa o cualitativa.

Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Entorno digital: Ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web.


Entorno digital abierto: entorno digital en el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica.

Gestión de Riesgos de seguridad: es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades.

Hardware : Se puede definir como el conjunto de los componentes que conforman la parte material (física) de una computadora

NIT 891800644-9
www.hospitalramiriqui.gov.co

Carrera 3 No. 7 - 21 Barrio Libertador Ramiriquí - Boyacá
 Conmutador: 3114802222
 E-mail: gerencia@hospitalramiriqui.gov.co / secretaria@hospitalramiriqui.gov.co

	SISTEMA INTEGRADO DE GESTIÓN	
	POLITICA DE SEGURIDAD DIGITAL	Código: POL-SD-ES-DE-001
		Versión: 00
		Fecha: 16/10/2020
	Página: 9 de 14	

Incidente digital: evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el entorno digital y que genera impactos sobre los objetivos.

Integridad: mantenimiento de la exactitud y complejidad de la información y sus métodos de proceso.

Información: es un conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje

Múltiples partes interesadas: el Gobierno nacional y los territoriales, las organizaciones públicas y privadas, la Fuerza Pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil, quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales, y quienes pueden ejercer distintos roles y tener distintas responsabilidades.

Planes de Contingencia: los procedimientos alternativos a la operación normal en una organización, cuyo objetivo principal es permitir el continuo funcionamiento y desarrollo normal de sus operaciones, preparándose para superar cualquier eventualidad ante accidentes de origen interno o externo, que ocasionen pérdidas importantes de información. Estos deben prepararse de cara a futuros sucesos.

Resiliencia: es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido


Responsabilidad: las múltiples partes interesadas deben asumir la responsabilidad de la gestión del riesgo de seguridad digital.

Riesgo: es el efecto de incertidumbre sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas.

Riesgo de seguridad digital: es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital.

NIT 891800644-9
www.hospitalramiriqui.gov.co

Carrera 3 No. 7 - 21 Barrio Libertador Ramiriquí - Boyacá
 Conmutador: 3114802222
 E-mail: gerencia@hospitalramiriqui.gov.co / secretaria@hospitalramiriqui.gov.co

 <p>E.S.E. Hospital San Vicente Ramiriquí</p>	SISTEMA INTEGRADO DE GESTIÓN	
	POLITICA DE SEGURIDAD DIGITAL	Código: POL-SD-ES-DE-001
		Versión: 00
		Fecha: 16/10/2020
	Página: 10 de 14	

Software: Se define como el conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora o de igual manera se define como la parte no tangible dentro de un sistema

Seguridad digital: es la situación de normalidad y de tranquilidad en el entorno digital (cibespacio), derivada de la realización de los fines esenciales del Estado mediante:

La gestión del riesgo de seguridad digital;

La implementación efectiva de medidas de ciberseguridad;

el uso efectivo de las capacidades de ciber defensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

Servidor: es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

Vulnerabilidad: Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan.

NIT 891800644-9

www.hospitalramiriqui.gov.co

Carrera 3 No. 7 - 21 Barrio Libertador Ramiriquí - Boyacá

Conmutador: 3114802222

E-mail: gerencia@hospitalramiriqui.gov.co / secretaria@hospitalramiriqui.gov.co

	SISTEMA INTEGRADO DE GESTIÓN	
	POLITICA DE SEGURIDAD DIGITAL	Código: POL-SD-ES-DE-001
		Versión: 00
		Fecha: 16/10/2020
	Página: 11 de 14	

4.OBJETIVOS

4.1. Objetivo General

Fortalecer la capacidad de la entidad para identificar, gestionar, mitigar los riesgos de seguridad digital en las actividades que desarrolla diariamente la entidad en la generación de información.

4.2. Objetivos Específicos

Establecer las directrices internas de la administración de la Empresa Social del Estado Hospital San Vicente de Ramiriquí relacionadas con el cumplimiento de la política de seguridad.

Fortalecer la seguridad digital en las actividades a desarrollar por el equipo de trabajo de la entidad.

Crear condiciones de identificación de los riesgos de seguridad digital para mitigarlos.


NIT 891800644-9

www.hospitalramiriqui.gov.co

Carrera 3 No. 7 - 21 Barrio Libertador Ramiriquí - Boyacá

Conmutador: 3114802222

E-mail: gerencia@hospitalramiriqui.gov.co / secretaria@hospitalramiriqui.gov.co

	SISTEMA INTEGRADO DE GESTIÓN	
	POLITICA DE SEGURIDAD DIGITAL	Código: POL-SD-ES-DE-001
		Versión: 00
		Fecha: 16/10/2020
	Página: 12 de 14	

5. ALCANCE DE LA POLÍTICA

La política de Seguridad Digital de la Empresa Social del Estado Hospital San Vicente de Ramiriquí aplica a todo el personal de planta, contratistas, estudiantes y terceros vinculados a la entidad, permitiendo identificar, gestionar y mitigar los riesgos de seguridad digital, en cumplimiento a las directrices del Modelo Integrado de Planeación y Gestión MIPG.

6. POLÍTICA DE SEGURIDAD DIGITAL

La Empresa Social del Estado Hospital San Vicente de Ramiriquí en aras de garantizar la seguridad digital con el fin de contrarrestar las amenazas informáticas que puedan afectar significativamente el desarrollo de la prestación del servicio en la entidad.


7. CUMPLIMIENTO

Todas las personas cubiertas por el alcance de la política se espera que se adhieran en un 100%. La cual será objeto de socialización y evaluación aplicando mecanismos de mejoramiento continuo que involucren participación, compromiso y adaptación.

La Política de Seguridad digital de la Empresa Social del Estado Hospital San Vicente de Ramiriquí será de obligatorio cumplimiento para todos los servidores públicos de planta, contratistas, estudiantes y terceros.

NIT 891800644-9
www.hospitalramiriqui.gov.co

Carrera 3 No. 7 - 21 Barrio Libertador Ramiriquí - Boyacá
 Conmutador: 3114802222
 E-mail: gerencia@hospitalramiriqui.gov.co / secretaria@hospitalramiriqui.gov.co

 <p>E.S.E. Hospital San Vicente Ramiriquí</p>	SISTEMA INTEGRADO DE GESTIÓN	
	POLITICA DE SEGURIDAD DIGITAL	Código: POL-SD-ES-DE-001
		Versión: 00
		Fecha: 16/10/2020
	Página: 13 de 14	

8. IMPLEMENTACIÓN

A continuación, se presentan las estrategias a implementar para dar cumplimiento a la política de Seguridad digital:

1. A partir de los resultados de FURAG, identificar y documentar las debilidades y fortalezas de la implementación de la política.
2. Asignar responsabilidades frente a la seguridad de la información.
3. Verificar que la seguridad es parte integral del ciclo de vida de los sistemas de información.
4. Proteger la información creada, procesada, transmitida o resguardada por los diferentes procesos de la entidad.
5. Todo usuario de los recursos de las TIC, no debe visitar sitios restringidos de manera explícita o implícita o sitios que afecten la productividad de la institución.
6. Minimizar el uso de dispositivos extraíbles para compartir archivos haciendo uso del recurso de internet de la entidad.
7. La entidad debe procurar porque sus funcionarios participen en las jornadas de capacitación del MINTIC y participar en las jornadas de fortalecimiento de capacidades de seguridad digital.
8. Elaborar el mapa de riesgo de seguridad digital.
9. Establecer roles y responsabilidades específicos respecto de la seguridad digital.
10. Establecer competencias de formación necesaria a todo el personal de la entidad.

NIT 891800644-9

www.hospitalramiriqui.gov.co

Carrera 3 No. 7 - 21 Barrio Libertador Ramiriquí - Boyacá

Conmutador: 3114802222

E-mail: gerencia@hospitalramiriqui.gov.co / secretaria@hospitalramiriqui.gov.co

	SISTEMA INTEGRADO DE GESTIÓN	
	POLITICA DE SEGURIDAD DIGITAL	Código: POL-SD-ES-DE-001
		Versión: 00
		Fecha: 16/10/2020
	Página: 14 de 14	

9. SEGUIMIENTO

El comité de Gestión y Desempeño de la Empresa Social de Estado Hospital San Vicente de Ramiriquí, establecerá el sistema de seguimiento y evaluación de la implementación de la política de seguridad digital para garantizar su cumplimiento por parte del personal del planta, contratistas y terceros vinculados a la entidad en el ejercicio de sus funciones.

VALIDACION DEL DOCUMENTO		
ELABORÓ	REVISÓ	APROBÓ
FIRMA: NOMBRE: CARLOS ENRIQUE CORTES PULIDO CARGO: PROFESIONAL UNIVERSITARIO	FIRMA: NOMBRE: COMITÉ CARGO: GESTIÓN Y DESEMPEÑO	FIRMA: NOMBRE: COMITÉ CARGO: GESTION Y DESEMPEÑO

CONTROL DE CAMBIOS		
CAMBIO REALIZADO	FECHA DE CAMBIO	VERSIÓN

NIT 891800644-9
www.hospitalramiriqui.gov.co

Carrera 3 No. 7 - 21 Barrio Libertador Ramiriquí - Boyacá
 Conmutador: 3114802222
 E-mail: gerencia@hospitalramiriqui.gov.co / secretaria@hospitalramiriqui.gov.co