

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DIGITAL	Código: PO-01-DIR-GIC-011
		Versión: 02
		Aprobación: 13/0/2024

Elaboró:	Revisó:	Aprobó:
Alcides Castro Patiño Ingeniero de sistemas	Cristina López Alzate Asesora Externa de Calidad	Olga Cecilia Mejía Jaramillo Directora ejecutiva
Fecha: 12/07/2024	Fecha: 12/07/2024	Fecha: 13/07/2024

1. Descripción de la política.	La Corporación Hospital Infantil Concejo de Medellín se compromete a garantizar la seguridad, confidencialidad, oportunidad, accesibilidad y disponibilidad de los activos informáticos definiendo controles que permitan mitigar los riesgos de pérdida de información, delitos informáticos como el uso indebido de información, interceptación, robo o suplantación de identidad y otros riesgos a los que estén expuestos los dispositivos al conectarse a la red del hospital o al interactuar con otros dispositivos, generando confiabilidad y validez de los datos de usuarios, servidores, proveedores y partes interesadas, en pro de la mejora del servicio y cumplimiento legal.
2. Marco normativo.	<ul style="list-style-type: none"> • Decreto 103 de 2015 • Decreto 1494 de 2015 • Ley 1712 de 2014 • Decreto 2573 de 2014 • Decreto 1377 de 2013 • Decreto 2693 de 2012 • Ley 1581 de 2012 • Ley 1474 de 2011 • Decreto 4632 de 2011
3. Campo de aplicación.	Esta política es de obligatorio cumplimiento y aplicación para todo el equipo multidisciplinario de la Corporación Hospital Infantil Concejo de Medellín.
4. Estrategias.	<ul style="list-style-type: none"> • Definir e implementar Plan de Seguridad y privacidad de la información que incluya la seguridad digital, soportado en lineamientos claros acordes a las necesidades y a la normatividad. • Desarrollar e implementar controles de seguridad.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DIGITAL	Código: PO-01-DIR-GIC-011
		Versión: 02
		Aprobación: 13/0/2024

	<ul style="list-style-type: none"> • Brindar capacitación en seguridad de la información y seguridad digital, a los colaboradores. • Implementar mecanismos y herramientas que permitan prevenir, atender, controlar y regular los incidentes o emergencias digitales para afrontar las amenazas y los riesgos que atentan contra la seguridad digital. • Adoptar una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información e infraestructura implementando estrategias de mejoramiento continuo. • Elaborar procedimientos de acuerdo a la normatividad que permitan minimizar los riesgos asociados con seguridad digital, validando y monitoreando con frecuencia los riesgos • Gestionar los incidentes de seguridad digital y en caso de ser necesario dar aviso a autoridades competentes, de acuerdo con las normas legales establecida. • Generar campaña de comunicaciones de los principales riesgos de seguridad de la información. • Fomentar buenas prácticas de seguridad en los servidores sobre la intervención de riesgos. 	
5. Implementación y evaluación.	DESPLIEGUE:	SEGUIMIENTO Y EVALUACIÓN (INDICADORES):
	Medios de comunicación de la Corporación (cartelera, página web). Despliegue institucional. Comités internos.	Proporción de incidentes relacionados con seguridad digital <ul style="list-style-type: none"> • Proporción de incidentes relacionados con seguridad digital gestionados

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DIGITAL	Código: PO-01-DIR-GIC-011
		Versión: 02
		Aprobación: 13/0/2024

CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO	RESPONSABLE
02	13/07/2024	Se modifican componentes de la política, se modifica el contenido de la política, se incorporan estrategias, marco normativo y campo de aplicación.	Ingeniero de sistemas