PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

OBJETIVO

.

ALCANCE DEL DOCUMENTO

.

MARCO NORMATIVO

NORMATIVIDAD	CONTENIDO
CONPES 3854 de 2016	Política Nacional de Seguridad Digital
Norma internacional ISO 31000:2018	Sistemas de gestión del riego
Norma internacional ISO 27000:2013	Seguridad de la información
Ley Estatutaria 1581 de 2012	Protección de datos personales
Ley 1266 de 2008	Disposiciones generales de habeas data y se regula el manejo de la información
Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5	Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2020
Manual para la Implementación de la Política de Gobierno Digital	Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019
Modelo de Seguridad y privacidad de la información - MSP	Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información,

	Arquitectura y Servicios Ciudadanos Digitales
Decreto 767 de 2022	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, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 88 de 2022	Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea
Decreto 338 de 2022	Por el cual se adiciona el Titulo 21 a la parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones

ESTADO ACTUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Hospital Infantil Concejo de Medellín no ha realizado el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información de la Política Nacional de Gobierno Digital.

DESARROLLO

El Hospital Infantil Concejo de Medellín adopta en su modelo de procesos, el proceso de Seguridad y Privacidad de la Información en el nivel estratégico que permite garantizar continuamente la seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios en la entidad, por medio de la definición de políticas, programas, lineamientos, estrategias y actividades.

Política general de seguridad y privacidad de la información

Las directivas de La Corporación Hospital Infantil Concejo de Medellín, 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.

Para La Corporación Hospital Infantil Concejo de Medellín, la protección de la información

busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad para, sus **los funcionarios, contratistas, terceros y partes interesadas**, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del Sistema General de Seguridad de la Información (SGSI) estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus usuarios, terceros y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los **funcionarios, contratistas, terceros y partes interesadas de** La Corporación Hospital Infantil Concejo de Medellín
- Garantizar la continuidad del negocio frente a incidentes.
- La Corporación Hospital Infantil Concejo de Medellín ha decidido **definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Objetivo

Con el fin de minimizar la materialización del riesgo frente a los activos de información La Corporación Hospital Infantil Concejo de Medellín se han establecido los siguientes objetivos del SGSI, así:

- Crear una cultura de Seguridad de la Información mediante las sensibilizaciones y capacitaciones en cuanto a las mejores prácticas para evitar la materialización de riesgos asociados al SGSI.

- Identificar mediante una adecuada evaluación del riesgo, el valor de la información, así como las vulnerabilidades y las amenazas a las que está expuestas.
- Dar un tratamiento efectivo a los incidentes de seguridad, con el fin de identificar sus causas y realizar las acciones correctivas.

- Implementar y mantener el Sistema de Gestión de Seguridad de la Información promoviendo la mejora continua

- Proteger los activos de información mediante la implementación de políticas, procedimientos y controles de seguridad necesarios y suficientes de acuerdo con el análisis de riesgo.

- Gestionar los riesgos de seguridad de la información de manera que estén dentro de los niveles de aceptación definidos por La Corporación Hospital Infantil Concejo de Medellín.

Alcance/Aplicabilidad

Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de **los funcionarios, contratistas, terceros y partes interesadas.**

Principios que soportan el Modelo de SGSI

- Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de **los funcionarios, contratistas, terceros y partes interesadas.**
- La Corporación Hospital Infantil Concejo de Medellín **protegerá la información** generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos **otorgados a terceros** (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- La Corporación Hospital Infantil Concejo de Medellín **protegerá la información** creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un **uso incorrecto** de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La Corporación Hospital Infantil Concejo de Medellín **protegerá su información** de las amenazas originadas por parte **del personal**.
- La Corporación Hospital Infantil Concejo de Medellín **protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos**.

- La Corporación Hospital Infantil Concejo de Medellín **controlará la operación** de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La Corporación Hospital Infantil Concejo de Medellín **implementará control de acceso** a la información, sistemas y recursos de red.
- La Corporación Hospital Infantil Concejo de Medellín garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La Corporación Hospital Infantil Concejo de Medellín garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La Corporación Hospital Infantil Concejo de Medellín **garantizará la disponibilidad** de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La Corporación Hospital Infantil Concejo de Medellín garantizará el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas.**

Cumplimiento

Todos los **funcionarios, contratistas, terceros y partes interesadas** de la entidad que en el ejercicio de sus funciones utilicen información y servicios TI La Corporación Hospital Infantil Concejo de Medellín deben cumplir con el 100% de la política. El incumplimiento de la política de seguridad y privacidad de la información de La Corporación Hospital Infantil Concejo de Medellín traerá consigo consecuencias legales de acuerdo a la normativa vigente.

Roles involucrados en la gestión de la seguridad de la información

Usuarios

Los usuarios La Corporación Hospital Infantil Concejo de Medellín son todos los funcionarios, contratistas y terceros del Hospital y tienen las siguientes responsabilidades:

- Cumplir con las políticas del Sistema de Gestión de seguridad de la Información.
- Reportar incidentes de seguridad que atenten contra la confidencialidad, integridad o disponibilidad de la información o evidencien un incumplimiento de las políticas de seguridad del Sistema de Gestión de seguridad de la Información.
- Participar activamente de las campañas de sensibilización en el Sistema de Gestión de seguridad de la Información.

- Participar de las actividades para la identificación de activos y riesgos de seguridad de la información.
- Apoyar el desarrollo de las auditorías internas y externas al Sistema de Gestión de seguridad de la Información.

Responsable de Responder a las consultas sobre incidentes de seguridad.

- Revisar y evaluar los indicadores de gestión correspondientes a la atención de incidentes de seguridad para poder ser presentados a la alta dirección.
- Convocar la participación de otros funcionarios de la entidad cuando el incidente lo amerite (Comunicaciones, Gestión de Talento Humano, Gestión Jurídica, Tecnología, Representante de las Directivas para el Sistema de Gestión de seguridad de la Información, etc.).
- Revisar el cumplimiento de los procedimientos y mejores prácticas en gestión de incidentes y recomendar, si lo amerita, la aplicación de planes de contingencia y/o continuidad.
- Revisar todos los incidentes de seguridad y los aspectos contractuales que aplican para el outsourcing de la Mesa de Servicios.

Agente del primer punto de contacto.

- Accesos no autorizados a los sistemas de información.
- Uso indebido de los recursos informáticos de la Entidad.
- Divulgación de información a quien no tiene derecho a conocerla.
- Uso de la información con el fin de obtener beneficio propio o de terceros.
- Hacer pública la información sin la debida autorización.
- Realización de copias no autorizadas de software.
- Descargar software a través de Internet sin la debida autorización
- Intentar modificar, reubicar o sustraer equipos de cómputo, software, información o periféricos sin la debida autorización. Transgredir o burlar los mecanismos de autenticación u otros sistemas de seguridad. Enviar cualquier comunicación electrónica fraudulenta.
- Enviar cualquier comunicación electrónica fraudulenta.
- Violación de cualquier ley o regulación nacional respecto al uso de sistemas de información.
- Robo de información sensible.
- Robo y pérdida de equipos de cómputo con información sensible.
- Denegación de servicio sobre equipos de la red, afectando la operación diaria de la Entidad.
- Denegación de servicio por el ingreso y propagación de virus que explotan vulnerabilidades.

- Amenazas a través de diferentes medios de comunicación (por ejemplo, correo electrónico) que generen un impacto directo sobre la seguridad de la información.
- Cambios o modificaciones en registros de bases de datos sin previa autorización.
- Generación o distribución de código malicioso.
- Fallas en los sistemas de información y pérdidas de servicio.
- Otros eventos y/o vulnerabilidades relacionadas con la seguridad de la información

Administrador de los sistemas de seguridad.

- Configurar y mantener los activos informáticos relacionados con la gestión de la seguridad de la información, por ejemplo, equipo de firewall, sistemas de prevención de intrusos (IPS), enrutadores de frontera, sistemas de gestión y monitoreo, consola de despliegue de políticas de seguridad, etc.
- Debe ser notificado por el Agente del primer punto de contacto sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar el incidente de seguridad.
- Debe documentar y notificar al Agente del primer punto de contacto y al CSSI sobre el incidente y la solución de este.
- Generar los reportes de eventos de seguridad que sean solicitados.
- Realizar los ajustes necesarios sobre los sistemas de seguridad que gestione.

Sitio de contacto

seguridaddigital@corporacionhicm.org

Portafolio de proyectos

Iniciativas	Proyecto	Indicador
Fortalecimiento de las capacidades institucionales para la seguridad y Privacidad de la Información	Fortalecimiento del Modelo de gestión de seguridad y privacidad de la información	Porcentaje de Incidentes del SPI monitoreados
	Fortalecimiento del plan de Continuidad de la operación de los servicios de la entidad	Porcentaje de efectividad de las pruebas programadas de las estrategias del plan de continuidad
	Implementación del Programa Integral de Gestión de Datos Personales	Porcentaje de bases de datos reportadas a la Superintendencia de Industria y Comercio
	Seguimiento y monitoreo de las actividades definidas en el Plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información	Porcentaje de eficacia del plan de tratamiento de riesgos

PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Plan de implementación de Seguridad y Privacidad de la Información se ejecuta de acuerdo con el siguiente cronograma.

Gestión	Actividades	Tareas	Responsable	Fechas
Seguridad de la Información Privacidad y Datos Personales Seguridad Digital Seguridad de Datos				
Activos de Información	Definir lineamientos para el levantamiento de activos de información	Actualizar la metodología o la documentación de la gestión de levantamiento de activos de información, en el caso que aplique		
	Levantamiento Activos de Información	Socializar la metodología de activos de Información.		
		Validar activos de información en el instrumento levantado en la vigencia anterior		
		Identificar nuevos activos de información en cada dependencia		
		Revisar los instrumentos de activos de Información y realimentar a las áreas con las modificaciones		
		Realizar correcciones a los instrumentos de activos de		

		Información, Cambios físicos de la ubicación de activos de información		
		Actualización del inventario de activos de información por alguna de las siguientes novedades: Actualizaciones al proceso al que pertenece el activo, Adición de actividades al proceso, Inclusión de un nuevo activo, Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados, Materialización de riesgos que cambien la criticidad del activo	**Gestores de cada proceso**	
	Publicación de activos de información	Validar y aceptar los activos de información para su publicación en la web por cada líder de proceso		
		Consolidar el inventario de activos de Información.		
		Publicar el consolidado de activos de información		
	Registros activos de información ley 1712	Actualizar el instrumento de Registro Activos de Información con el insumo del inventario de activos de Información.		
		Publicación del Registro Activos de Información en la sección de transparencia y en el portal de datos abiertos de la entidad o aquel que lo sustituya		
Gestión de Riesgos	**Actualización de lineamientos de riesgos**	Apoyar cuando se requiera la actualización de la política, metodología y lineamientos de la gestión de riesgos		
	Sensibilización	Socialización de lineamientos y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información y Seguridad Digital		
	Identificación de	Contexto, Identificación,		

	Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información y Seguridad Digital		
	Aceptación de Riesgos Identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento		
	Publicación	**Publicación de Mapa de Riesgos**		
	Seguimiento Fase de Tratamiento	Seguimiento implementación de controles y planes de tratamiento de riesgos los identificados (verificación de evidencias)		
	Mejoramiento	Identificación de oportunidades de mejora acorde al seguimiento de la ejecución de los controles y de los planes de tratamiento		
	Monitoreo y Revisión	Medición, presentación y reporte de indicadores		
Gestión de Incidentes de Seguridad y Privacidad dela información	Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	Revisión, actualización y publicación cuando se requiera el procedimiento de incidentes de seguridad de la información basado en la norma ISO 27035	Encargado de la Gestión de Incidentes de Seguridad de la Información	
		Socializar cuando se requiera el procedimiento	Encargado de la Gestión de Incidentes de Seguridad de la Información	
	Encargado de la Gestión de Incidentes de	Seguimiento a los incidentes de seguridad de la información	Encargado de la Gestión	

	Seguridad de la Información		de Incidentes de Seguridad de la Información	
	CSIRT	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno	Encargado de la Gestión de Incidentes de Seguridad de la Información	
	Eventos/vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SGS	Encargado de la Gestión de Incidentes de Seguridad de la Información	
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Actualizar la documentación del Plan de Cambio, Cultura y Apropiación de Seguridad y Privacidad de la Información y Seguridad Digital, en el caso que aplique	Encargado de la Gestión de Incidentes de Seguridad de la Información	
	Ejecutar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Implementar las estrategias del Plan de Cambio, Cultura y Apropiación de Seguridad y Privacidad de la Información y Seguridad Digital	Encargado de la Gestión de Incidentes de Seguridad de la Información	

Plan de continuidad del Negocio	Documentación del Análisis de Impacto de la Operación	Actualización del Análisis de Impacto del Negocio Publicación del Análisis de Impacto del Negocio		
	Documentación de Valoración de Riesgos de Interrupción	Actualización del documento Valoración de Riesgos de interrupción para el plan de continuidad de la operación. Publicación Valoración de Riesgos de interrupción		
	Documentación de Estrategias de Continuidad	Actualización del documento Estrategias de Continuidad de la Operación Publicación Estrategias de Continuidad de la Operación		
	Documentación del Plan de continuidad de la Operación	Crear Documentación del Plan de continuidad de la Operación Aprobación del Plan de continuidad de la Operación		
Oportunidades de mejoras SGS	Reporte del estado de las Acciones Correctivas, correcciones y Oportunidades de Mejora	Generar reporte del estado actual de las AC y OM. Solicitar y/o realizar el cargue del análisis de causas y plan de tratamiento según sea requerido.		
	Realizar seguimiento a las oportunidades de mejora producto de revisiones internas y externas a los Procesos	Hacer seguimiento a las observaciones o recomendaciones dejadas a los acompañamientos realizados a los Proceso		
Planeación	Revisión Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información	Actualizar cuando se requiera las Políticas, Resoluciones, y la documentación estratégica del procesos de Seguridad y privacidad de la Información		
		Actualizar el Plan de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos		
Gobierno Digital	**Gobierno Digital**	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la		

		Información.		
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.		
		Revisar el avance de implementación del Plan de Seguridad Digital en la Entidad.		
		Reuniones de Socialización de los avances de la implementación del plan de Seguridad Digital y la Estrategia del Modelo de Seguridad y Privacidad de la información		