Introducción

EL INSTITUTO DISTRITAL DE CIENCIA BIOTECNOLOGÍA E INNOVACIÓN EN SALUD (IDCBIS), a través de la Dirección General que representa a la junta directiva, tiene la posición de proteger todos los activos de información que ha establecido e identificado el Instituto (las partes interesadas internas y externas, la información como tal, los procesos, las tecnologías de información y la comunicación: tecnologías, procesos y personas involucradas en éstas), y de esta manera apoya la implementación del **Modelo de Seguridad y Privacidad de la Información – MSPI**, por medio de la aprobación de las respectivas políticas, procesos, procedimientos e instructivos, orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad y a la continuidad de las operaciones del Instituto a través de la gestión de los activos y de los riesgos de seguridad y privacidad de la información; fomentando la creación de una cultura y conciencia de seguridad en los empleados, contratistas y terceros del **IDCBIS**, los cuales se encuentran fundamentados en la norma técnica colombiana NTC-ISO-27001:2013 a través de la asignación de responsabilidades generales y específicas para llevar a cabo la gestión de dicho modelo.

1. OBJETIVO

Establecer los principios rectores y directrices generales del Modelo de Seguridad y Privacidad de la Información – MSPI del **INSTITUTO DISTRITAL DE CIENCIA BIOTECNOLOGÍA E INNOVACIÓN EN SALUD (IDCBIS),** con el fin de garantizar la integridad, confidencialidad, disponibilidad y privacidad de la información institucional, en pro del fortalecimiento estratégico y organizacional del IDCBIS.

1.1 Objetivos Específicos

EL INSTITUTO DISTRITAL DE CIENCIA BIOTECNOLOGÍA E INNOVACIÓN EN SALUD (IDCBIS), a través de la Política de Seguridad y Privacidad de la información, busca propender que se mantengan los objetivos institucionales, por lo tanto, la política tiene lo siguientes objetivos:

- Definir, documentar, socializar y actualizar las políticas complementarias, lineamientos, roles, responsabilidades y controles para generar la seguridad y privacidad de la información de los procesos del IDCBIS alineada al Plan Estratégico de Tecnologías de la Información – PETI, por medio del liderazgo y

desarrollo del mismo y a la Norma Técnica Colombiana – NTC ISO/IEC 27001:2013.

- Promover una cultura de seguridad y privacidad de la información al interior del Instituto con el objetivo de generar confianza en los procesos y sus niveles de seguridad y fortalecer los planes de cultura y concientización en el Instituto.
- Promover el uso de buenas prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Cumplir con los principios fundamentales de seguridad confidencialidad, integridad y disponibilidad de la información y los lineamientos y/o controles de Seguridad y Privacidad de la Información definidos por el Instituto.
- Mejorar los procesos, procedimientos e instructivos en materia de seguridad de la información para todo el Instituto.
- Identificar, clasificar y actualizar los activos de información y sus riesgos asociados.
- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en el Instituto.

2. ALCANCE

Dar cumplimiento a los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC a través de Gobierno Digital, identificando el inventario de los activos de información, asegurando la gestión adecuada de la seguridad y privacidad, enfocado en la preservación de la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos del Instituto. La Política de Seguridad y Privacidad de la Información es de obligatorio cumplimiento y aplica a todos los empleados, contratistas, proveedores, terceros y demás grupos de interés que accedan a la información o que tengan vínculos laborales, contractuales con el Instituto, así como a todos los procesos del IDCBIS.

3. RESPONSABLE

El Grupo de Gestión de Tecnologías de la Información es el responsable de divulgar y hacer cumplir los lineamientos definidos en esta política, Es de su responsabilidad de a quienes delegue la ejecución de este proceso, cumpla con las indicaciones y formatos que se establecen en el presente documento

El cumplimiento de las políticas, lineamientos, procedimientos y guías de seguridad propenderá por los siguientes compromisos:

- El **IDCBIS** protegerá la información generada, procesada, transmitida y/o resguardada por los procesos y procedimientos en el cumplimiento de sus funciones**,** y de los activos de información que hacen parte de estos. con el fin de minimizar impactos negativos a el Instituto; para ello, es fundamental la aplicación

COPIA NO CONTROLADA

de controles de acuerdo con la clasificación de la información de su propiedad y/o en custodia.

- El **I IDCBIS** protegerá su información de las amenazas internas y/o externas por parte del personal custodio, responsable, usuario de esta y/o personas ajenas a al Instituto.
- El **IDCBIS** protegerá las instalaciones de procesamiento de datos e información y la infraestructura tecnológica que soporta sus procesos estratégicos, misionales y de apoyo.
- El **IDCBIS** controlará la operación de sus procesos estratégicos, misionales y de apoyo; garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- El **IDCBIS** implementará controles de acceso a la información, sistemas y recursos de red.
- El **I IDCBIS** verificará que la seguridad sea una pieza integral del ciclo de vida de los sistemas de información.
- El **IDCBIS** revisará a través de una adecuada gestión los eventos y/o incidentes de seguridad las debilidades asociadas con los sistemas de información, logrando una mejora efectiva de su modelo de seguridad y privacidad de la información.
- El **IDCBIS** verificará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas. El incumplimiento a la Política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de esta, incluyendo lo establecido en las normas que corresponden al Gobierno Nacional y territorial en cuanto a Seguridad, Privacidad de la Información y Gobierno Digital se refiere.
- El **IDCBIS**comunicará a sus colaboradores y a la ciudadanía en general la implementación y gestión de la presente política.

4. DEFINICIONES (1)

Activo de información: Es todo aquel recurso tangible o intangible que tenga valor o importancia para la organización, de acuerdo con la tipificación definida.

Confidencialidad: Consiste en garantizar que el activo de información no esté disponible o sea divulgado por personas, entidades o procesos **NO** autorizados.

Integridad: Consiste en asegurar o salvaguardar que el activo de información cuente con las propiedades de: exactitud, precisión, consistencia, confiabilidad y totalidad.

Disponibilidad: Consiste en garantizar que el activo de información esté accesible y utilizable en el momento oportuno que se requiera bajo la demanda de personas, entidades o procesos.

SGSI: Sistema de Gestión de Seguridad de la Información.

COPIA NO CONTROLADA

MSPI: Modelo de Seguridad y Privacidad de la Información.

Seguridad Digital: El CONPES de Seguridad Digital es una herramienta para que todos los colombianos cuenten con un ambiente digital seguro, para ello las entidades del Estado y las empresas privadas deben implementar acciones para que los ciudadanos realicen, sin temor alguno, compras a través de internet, transacciones en línea entre otros a través de políticas y procedimientos de seguridad de la información.

5. PRINCIPIOS

Los principios que adopta el IDCBIS para orientar la ejecución de la Política de Seguridad y Privacidad de la Información son:

Seguridad de la información: el IDCBIS considera importante definir las medidas preventivas y de reacción del individuo, la organización y las tecnologías, para proteger la información y salvaguardar la confidencialidad, autenticidad, integridad y disponibilidad.

Confidencialidad: se debe garantizar que los datos que están guardados en el sistema no se divulguen a otras entidades o individuos que no están autorizados para acceder a esa información

Integridad: se debe garantizar que toda información recogida sea exacta y no haya sido modificada a no ser que algún usuario autorizado lo haya hecho por orden expresa.

Disponibilidad: toda la información que se encuentre almacenada en el sistema tiene que estar siempre a disposición de los usuarios autorizados en cualquier momento que ellos necesiten acceder a ella.

6. DESARROLLO DE LA POLÍTICA

6.1 Generalidades Del Sistemas Gestión de Seguridad de la Información

6.1.1 Política del Sistema de Gestión de Seguridad de la Información

EL INSTITUTO DISTRITAL DE CIENCIA BIOTECNOLOGÍA E INNOVACIÓN EN SALUD (IDCBIS), en el marco de su misión y entendiendo la importancia de una adecuada gestión de la información, se compromete a realizar las acciones pertinentes y de carácter obligatorio para conservar la integridad, confidencialidad, disponibilidad y privacidad de sus activos de información, los cuales soportan los procesos del Instituto, estableciendo así, el **Sistema de Gestión de Seguridad de la Información - SGSI**, el cual realiza la gestión integral de riesgos e incidentes, fortalece la cultura de seguridad en los colaboradores y propende por la continuidad del negocio. Lo anterior, enmarcado

COPIA NO CONTROLADA

en el cumplimiento de los requisitos legales, regulatorios y en concordancia con la misión y visión del Instituto.

6.2 Alcance del Sistema de Gestión de Seguridad de la Información

La implementación del Sistema de Gestión de Seguridad de la Información y la presente política del **INSTITUTO DISTRITAL DE CIENCIA BIOTECNOLOGÍA E INNOVACIÓN EN SALUD (IDCBIS),** aplica para todos los procesos y es de obligatorio complimiento para los empleados, contratistas, proveedores, que tengan vínculos laborales o contractuales con el Instituto.

Para dar cumplimiento se debe asegurar la divulgación e implementación de la política, manual, procedimientos, guías e instructivos, garantizando el seguimiento y mejora de estos en todos los procesos del Instituto.

6.3 Objetivos del Sistema de Gestión de Seguridad de la Información

1. Identificar, clasificar, valorar y mantener actualizados los activos de información del Instituto
2. Gestionar los riesgos de Seguridad y Privacidad de la información que afecten la confidencialidad, integridad, disponibilidad y privacidad de la información institucional.
3. Gestionar los incidentes y eventos de seguridad y privacidad que pongan en riesgo la confidencialidad, disponibilidad, integridad y privacidad de los activos de información del Instituto de manera oportuna con el fin de minimizar su impacto y propagación.
4. Promover e implementar estrategias para establecer una cultura y apropiación en temas de Seguridad y Privacidad de la información en todos los colaboradores del Instituto.
5. Establecer, implementar y mejorar el plan de continuidad del negocio del **INSTITUTO DISTRITAL DE CIENCIA BIOTECNOLOGÍA E INNOVACIÓN EN SALUD (IDCBIS),** para los procesos y/o actividades críticas del Instituto.

6.4 Compromiso de la Dirección

La Dirección General y el Grupo de Tecnologías de la Información, se comprometen y responsabilizan con la asignación y comunicación de las funciones, obligaciones y responsabilidades de todos los empleados, contratistas, proveedores, terceros y demás grupos de interés que accedan a la información o que tengan vínculos laborales, contractuales con el Instituto, así como a todos los procesos del IDCBIS, en materia de seguridad y privacidad de la información, apalancando así el establecimiento, implementación, operación, seguimiento, mantenimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información – MSPI y de la Política de Gobierno Digital, basado en la NTC-ISO-IEC 27001:2013 y el cual define un conjunto de políticas,

COPIA NO CONTROLADA

procedimientos, guías y formatos con los lineamientos y buenas prácticas para mantener la confidencialidad, integridad, disponibilidad y privacidad de la información del Instituto.

6.5 Responsabilidades del Sistema de Gestión de Seguridad de la Información

La Dirección del IDCBIS es la instancia donde se deben tratar los temas de privacidad, seguridad digital y de la información del **INSTITUTO DISTRITAL DE CIENCIA BIOTECNOLOGÍA E INNOVACIÓN EN SALUD (IDCBIS).**

Se establece que el Grupo de Tecnologías de la Información, en el ámbito de sus competencias, definirá y liderará la gestión, adopción, implementación, operación, seguimiento, cumplimiento, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la información - SGSI del Instituto, contemplando los recursos necesarios para que las Políticas de Seguridad y Privacidad de la Información y de Protección de Datos Personales se integren a todos los procesos del **INSTITUTO DISTRITAL DE CIENCIA BIOTECNOLOGÍA E INNOVACIÓN EN SALUD (IDCBIS),** para el logro de este propósito es necesaria la participación de los diferentes actores.

Adicionalmente, todos los empleados, contratistas y terceros que tengan vínculos laborales o contractuales con el Instituto, están obligados a cumplir con las políticas, procedimientos, guías, lineamientos y demás instrumentos relacionados con el SGSI, reportando además cualquier tipo de anomalía, evento o incidente que ponga en riesgo la seguridad y privacidad de la información.

CONTROLADA

7. VIGENCIA

La presente política entrará en vigencia a partir de la fecha de aprobación por la Dirección del **INSTITUTO DISTRITAL DE CIENCIA BIOTECNOLOGÍA E INNOVACIÓN EN SALUD (IDCBIS)**, su publicación será objeto de revisión anualmente o cuando el Instituto lo considere necesario; en los escenarios de posibles cambios de entorno interno, externo y/o cuando sea solicitado por normativa legal colombiana.

8. BIBLIOGRAFIA

Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). (2013). Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la Seguridad de la Información (SGSI). Requisitos (NTC-ISO/IEC 27001.

9. NORMATIVIDAD

- Norma Técnica Colombiana ISO 27001- 2013 modelo de seguridad y privacidad de la información
- Guía Técnica Colombiana GTC-ISO/IEC 27002:2015 Código de práctica para controles de seguridad de la información

Documento no válido en medio impreso sin la identificación de “COPIA CONTROLADA”. La información de este documento es de carácter confidencial y de propiedad del IDCBIS. Su reproducción y uso requiere autorización de Gestión y Aseguramiento de Calidad.

- Ley 1273 de 5 de enero de 2009 del “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

- Ley Estatutaria 1581 de octubre 12 de 2012” Por el cual se dictan disposiciones generales para la protección de datos personales”.

- Decreto 1377 del 27 de junio de 2013 (derogado Parcialmente por el Decreto 1081 de 2015) “Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales”.

10. CONTROL DE CAMBIOS

VERSIÓN	FECHA DE APROBACIÓN	RAZÓN DE LA ACTUALIZACIÓN
01	26/02/2021	Generación de nuevo documento
02	04/05/2023	Se realiza actualización de la política dando alcance al Sistema de Gestión de Seguridad y Privacidad de la Información fundamentado en la norma técnica colombiana NTC-ISO-27001:2013.

COPIA NO CONTROLADA

Documento no válido en medio impreso sin la identificación de “COPIA CONTROLADA”. La información de este documento es de carácter confidencial y de propiedad del IDCBIS. Su reproducción y uso requiere autorización de Gestión y Aseguramiento de Calidad.