

“Por la cual se adopta la Política de Seguridad y Privacidad de la Información del Instituto Distrital de Recreación y Deporte”

LA DIRECTORA GENERAL DEL INSTITUTO DISTRITAL DE RECREACIÓN Y DEPORTE

En uso de sus facultades legales, en especial las que le confiere el artículo 6° del Acuerdo 4 de 1978 *“Por el cual se crea el Instituto Distrital para la Recreación y el Deporte”*, el artículo 3° de la Resolución 006 de 2017 *“Por la cual se modifica la estructura organizacional y las funciones de las dependencias del Instituto Distrital de Recreación y Deporte, y se dictan otras disposiciones”*, y

CONSIDERANDO

Que la Constitución Política de Colombia en su artículo 15 establece que *“Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas (...)”* y en ese mismo sentido, el artículo 74 prevé que *“Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la Ley. El secreto profesional es inviolable.”*

Que la Ley 1273 del 05 de enero de 2009 *“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”*, crea un nuevo bien jurídico tutelado denominado *“De la protección de la información y los datos”*, preservando integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

Que la Ley Estatutaria 1581 del 17 de octubre de 2012, *“Por la cual se dictan disposiciones generales para la protección de datos personales”*, tiene como objeto *“(...) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma”* (artículo 1), estableciendo, además, las disposiciones generales para la protección de datos personales.

Que la Ley Estatutaria 1712 del 06 de marzo de 2014 *“Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”*, reglamentada parcialmente por el Decreto 103 del 20 de enero de 2015, tiene por objeto *“(...) regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información”* (artículo 1).

Que en el marco del Decreto Nacional 2573 del 12 de diciembre de 2014, *“Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones”* establece los lineamientos generales de Gobierno en Línea.

Que el Decreto 1078 del 26 de mayo de 2015 *“Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”* dispone en el artículo 2.2.17.1.2 que las entidades que conforman la administración pública

“Por la cual se adopta la Política de Seguridad y Privacidad de la Información del Instituto Distrital de Recreación y Deporte”

serán sujetos obligados para el cumplimiento de las políticas y los lineamientos de la Estrategia de Gobierno en Línea, estableciendo en su artículo 2.2.9.1.2.1 como uno de sus habilitadores transversales de la Política de Gobierno Digital, el de la Seguridad y privacidad de la Información, comprendido por las acciones transversales a los componentes de TIC para Servicios, TIC para el Gobierno Abierto y TIC para la Gestión, tendientes a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada. Así mismo y en su artículo 2.2.17.5.6 prevé que la seguridad y privacidad de la información, comprende la seguridad digital y los requerimientos necesarios para garantizar la continuidad en la prestación de los servicios digitales.

Que el Decreto Nacional 1499 del 11 de septiembre 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”*, definió las bases del nuevo Sistema Integrado de Gestión, estableció el Modelo Integrado de Planeación y de Gestión para implementar dicho sistema, e hizo énfasis en que dentro de las políticas de gestión y de desempeño institucional se encuentran, según el artículo 2.2.22.2.1, numerales 11 y 12, las Políticas de Gobierno Digital y de Seguridad Digital, con las cuales debe alinearse la Política de Seguridad y Privacidad de la Información.

Que mediante Documento CONPES 3995 de 2020 - Política Nacional de Confianza y Seguridad Digital, se establecen medidas para desarrollar la confianza digital a través de la mejora de la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

Que el Decreto Distrital 807 del 24 de Diciembre de 2019 *“Por medio del cual se reglamenta el Sistema de Gestión en el Distrito Capital y se dictan otras disposiciones”*, establece en su artículo 8, la creación de los Comités Instituciones de Gestión y Desempeño, definiendo la institucionalidad para la implementación del Modelo Integrado de Planeación y de Gestión (MIPG) como *“(…) el conjunto de instancias que de manera coordinada establecen las reglas, condiciones, políticas y metodologías que facilitan la implementación, evaluación y seguimiento del modelo”*.

Que, en cumplimiento de lo previsto en el referido Decreto Distrital, mediante la Resolución No. 265 del 31 de agosto de 2020, se crea el Comité Institucional de Gestión y Desempeño del Instituto Distrital de Recreación y Deportes IDR, como la instancia encargada de orientar, articular y ejecutar las acciones y estrategias para la correcta implementación, operación, desarrollo, evaluación y seguimiento del Modelo Integrado de Planeación y Gestión, la cual fue modificada por la Resolución No. 538 del 15 de julio de 2021 *“Por la cual se modifica el artículo 13 de la Resolución 265 de 2020 que crea el Comité Institucional de Gestión y Desempeño del Instituto Distrital de Recreación y Deporte, IDR”*.

Que mediante Resolución No. 500 del 10 de marzo de 2021 el Ministerio de Tecnologías de la Información y las Comunicaciones, establece los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital; así como los lineamientos y estándares para la estrategia de seguridad digital, precisando en su artículo 5 numeral 1 que, la estrategia de seguridad digital debe *“ser aprobada a través de un acto administrativo de carácter general”*.

“Por la cual se adopta la Política de Seguridad y Privacidad de la Información del Instituto Distrital de Recreación y Deporte”

Que para lograr el buen uso y seguridad de los activos de información, que maneja la entidad tanto en formato físico como digital, el Instituto Distrital de Recreación y Deporte, requiere la definición e implementación de una política de seguridad digital que indique los lineamientos frente a la seguridad y privacidad de la información, que permita realizar un buen uso de la misma; así como mitigar los riesgos sobre su confidencialidad, disponibilidad e integridad.

Que, en mérito de lo expuesto,

RESUELVE

ARTÍCULO 1. Adoptar la Política de Seguridad y Privacidad de la Información y Seguridad Digital del Instituto Distrital de Recreación y Deporte IDRD; así como los procesos, procedimientos y documentos técnicos que lo soporten, debidamente revisados y aprobados por la Oficina Asesora de Planeación, con el fin de mantener la disponibilidad, integridad y confidencialidad de la información, en concordancia con la normatividad vigente.

ARTÍCULO 2. Definiciones: Para efectos de la presente resolución, se adoptan las siguientes definiciones

- *Política de Seguridad y Privacidad de la Información.* Es la declaración general que representa la posición del Instituto Distrital de Recreación y Deporte IDRD respecto a la protección de los activos de información (los funcionarios, contratistas y terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos del Instituto y apoyan la implementación del Modelo de Privacidad y Seguridad de la información, mediante la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.
- *Activos de Información.* En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal. (MSPI min tic)
- *Seguridad Digital.* Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la gestión del riesgo de seguridad digital y la implementación efectiva de medidas de ciberseguridad y ciberdefensa
- *Confidencialidad.* La información debe ser accesible sólo para las personas autorizadas.
- *Disponibilidad.* La información y los servicios deben estar disponibles cuando se le requiera.
- *Integridad.* La información y sus métodos de procesamiento deben ser completos y exactos.
- *Información.* Datos relacionados que tienen valor para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades

“Por la cual se adopta la Política de Seguridad y Privacidad de la Información del Instituto Distrital de Recreación y Deporte”

de la entidad y, en consecuencia, necesita una protección adecuada (ISO/IEC 27001:2013).

- *Sistema de Gestión de Seguridad de la Información SGSI:* Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- *Modelo de Seguridad y Privacidad de la Información – MSPI.* Se refiere al mecanismo que conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

ARTÍCULO 3. Componentes de la Política. La Política de Seguridad y Privacidad de la Información y Seguridad Digital está conformada por estándares (técnicos y generales de seguridad de la información), procesos y procedimientos, estructura organizacional y mecanismos de verificación y control. Para garantizar que los riesgos de seguridad de la información y los riesgos de ciberseguridad sean conocidos, gestionados y mitigados de forma documentada, sistemática, estructurada, repetible, eficiente y adaptable a los cambios que se produzcan en los riesgos, el entorno y las tecnologías¹.

ARTÍCULO 4. Ámbito de Aplicación. La Política de Seguridad y Privacidad de la Información y Seguridad Digital, aplica a:

1. Toda la infraestructura tecnológica y sistemas de información que soportan la misionalidad de la Entidad.
2. Todas las sedes físicas del IDR; así como los parques y escenarios administrados por el instituto.
3. Todos los niveles, dependencias y áreas del IDR.
4. Todos los procesos y procedimientos del IDR.
5. Todos los activos de información, esto es, toda la información creada, procesada o utilizada por la entidad, sin importar el medio, formato, presentación o lugar en la cual se encuentre.
6. Todas las personas vinculadas al IDR, funcionarios, contratistas, proveedores, personal que labore en las instalaciones del instituto vinculado con un proveedor u operadores; entes de control; terceros que en cumplimiento de sus funciones y las del Instituto, compartan, utilicen, recolecten, procesen, intercambien o consulten su información de forma interna o externa, independientemente de su ubicación; y la ciudadanía en general.

ARTÍCULO 5. Objetivos. La Política de Seguridad y Privacidad de la información, tiene los siguientes objetivos:

1. Brindar soporte tecnológico a los procesos misionales, estratégicos y de apoyo del Instituto.
2. Cumplir con los principios de seguridad de la información.
3. Cumplir con los principios de la función administrativa.
4. Mantener la confianza de los funcionarios, contratistas y terceros.

¹ ISO 27000:2013

“Por la cual se adopta la Política de Seguridad y Privacidad de la Información del Instituto Distrital de Recreación y Deporte”

5. Apoyar la innovación tecnológica.
6. Implementar el Modelo de Privacidad y Seguridad de la Información (MPSI).
7. Proteger los activos de información.
8. Establecer las políticas, procedimientos e instructivos en materia de seguridad digital y de la información.
9. Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas, terceros, practicantes y usuarios del Instituto Distrital de Recreación y Deporte IDR.
10. Garantizar la continuidad del negocio frente a incidentes.

ARTÍCULO 7.- Principios. Se establecen los siguientes principios de seguridad de la información, que soportan el Sistema de Gestión de Seguridad de la Información:

1. **Mejora Continua.** Se refiere a que el IDRD definirá, implementará y mejorará de forma continua, el Modelo de Seguridad y Privacidad de la Información, a través de lineamientos claros alineados a los procesos misionales, y a los requerimientos regulatorios originados principalmente por MINTIC y la Alta Consejería Distrital de TIC. De igual manera el IDRD, 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.
2. **Responsabilidad.** Se refiere a que las responsabilidades frente a la seguridad de la información, serán definidas por el IDRD, compartidas, publicadas y aceptadas por sus funcionarios, contratistas y terceros. Así mismo, el IDRD garantizará que la seguridad digital y de la información sea parte integral del ciclo de vida de los sistemas de información y propenderá por el cumplimiento de las obligaciones legales, regulatorias y contractuales relacionadas con seguridad de la información.
3. **Confidencialidad.** Se refiere a que el IDRD protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos y sistemas de información y además controlará la operación de sus procesos estratégicos, misionales y de apoyo, garantizando la seguridad de los recursos tecnológicos y las redes de datos. La protección de la información, se realizará de acuerdo con los riesgos establecidos en la matriz del proceso de gestión de TIC y la aplicación de controles de acuerdo con la clasificación de la información de propiedad del Instituto o bajo su custodia.
4. **Integridad.** Se refiere a que el IDRD protegerá la información generada, procesada, transmitida o resguardada por los procesos estratégicos, misionales y de apoyo, además de los activos de información que hacen parte de estos, con el fin de minimizar los impactos financieros, operativos o legales derivados de su uso incorrecto.
5. **Disponibilidad.** Se refiere a que el IDRD implementará controles de acceso a la información, sistemas y recursos de red y garantizará la disponibilidad de los sistemas de información que soportan los procesos estratégicos, misionales y de apoyo; así como la continuidad de su operación basado en el impacto que pueden generar eventos que atenten contra la seguridad de la información.

ARTICULO 8. Oficial de Seguridad y Privacidad de la Información. El Subdirector Administrativo y Financiero será el Oficial de Seguridad y Privacidad de la Información en el IDRD, para lo cual liderará la implementación, seguimiento y mejoramiento de la *Política de Seguridad y Privacidad de la Información* (MPSI), lo que incluye actividades tales como: brindar asesoría sobre el manejo de la información de la entidad, coordinar la gestión de

“Por la cual se adopta la Política de Seguridad y Privacidad de la Información del Instituto Distrital de Recreación y Deporte”

riesgos de seguridad digital y de la información, apoyar la identificación de controles y reportar el avance en la implementación del sistema al Comité Institucional de Gestión y Desempeño del Instituto Distrital de Recreación y Deporte.

ARTICULO 9. Principales actividades del Oficial de Seguridad y Privacidad de la información. El Oficial de Seguridad de la información, en coordinación con el Área de Sistemas del IDR, se encargará de:

- Definir las herramientas, técnicas, controles y demás actividades requeridas para implementar el Modelo de Seguridad y Privacidad de la Información – MSPI–
- Identificar la brecha existente entre el Modelo de Seguridad y Privacidad de la Información - MSPI–MINTIC, y la situación actual del IDR para propender por el mejoramiento del sistema y la disminución de las brechas detectadas.
- Aplicar la metodología PHVA (Planear, Hacer, Verificar y Actuar) para implementar el Modelo de Seguridad y Privacidad de la Información – MSPI–, garantizando la continuidad del modelo en el Instituto.
- Trabajar de manera integrada con todas las dependencias y áreas del IDR, con el fin de avanzar en la implementación y adecuado funcionamiento del Modelo de Seguridad y Privacidad de la Información – MSPI–.
- Registrar las lecciones aprendidas respecto de la implementación y funcionamiento del Modelo de Seguridad y Privacidad de la Información – MSPI–, en pro de la mejora continua del mismo, al interior del Instituto.
- Medir y actualizar los indicadores de gestión del Modelo de Seguridad y Privacidad de la Información – MSPI- en el IDR.

ARTICULO 10. Políticas y Controles. De acuerdo con lo establecido en el Modelo de Seguridad y Privacidad de la Información (MSPI), el IDR a través del documento denominado: *“Manual De Políticas de Seguridad Digital y de la Información”*, adoptado en la entidad, en virtud de la Ley de Transparencia, realizará la especificación y actualización de las políticas y controles relacionados con la seguridad y privacidad de la información; así como la definición y ajustes necesarios respecto de los responsables de su ejecución y control.

ARTÍCULO 11. Revisión de la Política. La Política de Seguridad y Privacidad de la Información será revisada por el Oficial de Seguridad y Privacidad de la Información en coordinación con el Área de Sistemas del IDR, con una periodicidad mínima anual, mediante el diligenciamiento del autodiagnóstico de implementación del MSPI, o cuando se considere pertinente por cambios normativos, necesidades del servicio o riesgos de seguridad detectados que así lo ameriten.

Artículo 12. Tratamiento de riesgos de seguridad digital: Todos los líderes de procesos del IDR, acompañados por el Oficial de Seguridad de la Información, deben realizar la identificación, clasificación y tratamiento de riesgos de seguridad digital, que puedan comprometer las operaciones de la entidad y amenazar la seguridad de la información de acuerdo con lo definido en la Política de Administración de Riesgos de la entidad. El reporte de las evidencias de los controles definidos para la mitigación de los riesgos se realizará de acuerdo como lo que establezca la Oficina Asesora de Planeación.

ARTÍCULO 13. Cumplimiento y Sanciones. Todos los funcionarios, contratistas, proveedores, operadores, entes de control, terceros y ciudadanía en general (artículo 4 Núm. 6. de la presente resolución) deben cumplir la Política de Seguridad y Privacidad de la Información y Seguridad Digital y sus políticas específicas; así como los procesos y

“Por la cual se adopta la Política de Seguridad y Privacidad de la Información del Instituto Distrital de Recreación y Deporte”

procedimientos en los cuales se soporte y que se encuentran asociados al proceso de gestión de TIC.

El incumplimiento de la Política de Seguridad y Privacidad de la Información y Seguridad Digital y de sus políticas específicas, así como la violación a los procesos y procedimientos en que se soporten, pone en riesgo la continuidad y operación de los servicios de la entidad y por ende el cumplimiento de la misión institucional, lo cual generará las investigaciones a las que haya lugar, de conformidad con la normatividad vigente.

ARTÍCULO 14.- Comunicación y publicación. La presente resolución debe comunicarse a cada una de las dependencias del Instituto Distrital de Recreación y Deporte y cargarse para efectos de su publicación en el link de Transparencia y Acceso a la Información Pública de la página web del IDRD, en cumplimiento a lo dispuesto en la Ley 1712 de 2014 y el Decreto Nacional 103 de 2015.

ARTÍCULO 15. Vigencia. La presente Resolución rige a partir de su expedición.

Dada en Bogotá, D.C., a los 24 días del mes de Enero del 2022

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE,



BLANCA INÉS DURAN HERNÁNDEZ
Directora General

Proyectó: Jorge Alberto Farigua Gutiérrez
Laura M. Canizales – Abogada Contratista SAF
Mariluz Casas Acuña- Referente SIG – Contratista SAF
Revisó: Javier Ríos Molina – Profesional Especializado área de sistemas
Sandra Jaber Martínez – Secretaría General
Andrés Mejía Narváez– Jefe Oficina Asesora Jurídica
Héctor Elpidio Corredor Igua – Subdirector Administrativo y Financiero
Aprobó: Sandra Jaber Martínez – Secretaría General