GOBIERNO ABIERTO DE BOGOTÁ

# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2024

## INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL



ALCALDÍA MAYOR DE BOGOTÁ D.C. | BOGOTÁ

GOBIERNO ABIERTO DE BOGOTÁ

## CONTROL DE CAMBIOS

| NO. DE ACTA DE APROBACIÓN | FECHA | VERSIÓN | DESCRIPCIÓN |
|---|---|---|---|
| 12 | 27/12/2023 | 1.0 | Adopción Plan de Seguridad y Privacidad de la Información vigencia 2024 |

## AUTORIZACIONES

| ELABORÓ: | REVISÓ | APROBÓ |
|---|---|---|
| ÁREA TÉCNICA | OFICINA Y/O SUBDIRECCIÓN | LÍDER DEL PROCESO |
| Nombre:<br><br>Julio César Benavides Carranza<br>José Alfonso Pérez C | Nombre:<br><br>Loren Guisell Díaz Jiménez<br>Sara Sofia Lancheros Ramírez | Nombre:<br><br>Jesús Alberto Martínez Cespedes |
| Firma: | Firma: | Firma: |
| Cargo:<br><br>Profesional Contratista- SGC grupo de gestión Tecnológica | Cargo:<br><br>Contratista Profesional OAP<br>Profesional Especializado OAP | Cargo:<br><br>Subdirector de Gestión Corporativa |

TABLA DE CONTENIDO

GOBIERNO ABIERTO DE BOGOTÁ

# TABLA DE ILUSTRACIONES

GOBIERNO ABIERTO DE BOGOTÁ

# TABLA DE TABLAS

## 1. INTRODUCCIÓN.

El Instituto Distrital de Protección y Bienestar Animal, reconoce la importancia y el valor de la información con respecto a salvaguardar los niveles de seguridad de la información, entendiendo que la información no es sólo crítica para el éxito de la organización, sino estratégica para el cumplimiento de sus objetivos misionales y estratégicos a largo plazo, por esta razón, se establece el siguiente plan que regula el manejo de la información en el IDPYBA, orientado a definir las medidas que resguarden la confidencialidad, integridad y disponibilidad de la información propia del Instituto Distrital de Protección y Bienestar Animal, gestionando el acceso a la información, tomando como referencia la norma ISO 27001: 2013, la cual es adoptada por el Modelo de Seguridad y Privacidad de la Información impulsado por el MinTIC.

Es por ello que se hace necesario mantener y mejorar continuamente un Modelo de Seguridad y privacidad de la información o también llamado Sistema de Gestión de la Seguridad de la Información (SGSI), el cual permita lograr los niveles adecuados de seguridad para todos los activos de información de la entidad considerados relevantes, para garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados, como parte del proceso de revisión estratégica, o cuando se identifiquen cambios en la entidad, en su estructura, sus objetivos o en alguna condición que la afecte, para asegurar que dichas políticas sigan siendo adecuadas y ajustadas a los requerimientos de la Entidad.

## 2. OBJETIVO.

Orientar y dar lineamientos de seguridad de la información frente al acceso a los activos de información del Instituto Distrital de Protección y Bienestar Animal, entidad adscrita al Sector Ambiente de Bogotá D.C. con el fin de garantizar que los riesgos de seguridad de la información identificados, valorados y administrados de forma estructurada, eficiente y adaptada a los cambios que se produzcan en el entorno de las tecnologías de información, velando por principios de Integridad, confidencialidad y disponibilidad de los activos de información a través de mejora continua.

## 2.1. OBJETIVOS ESPECÍFICOS.

- Establecer para todo el personal del IDPYBA la necesidad de conocer y gestionar la seguridad de la información y promover la comprensión de sus responsabilidades individuales, mediante el seguimiento de controles, actividades para gestión y monitoreo de seguridad de la información, fortalecimiento de la cultura en seguridad de la información, para la concientización de funcionarios, contratistas y terceras partes contribuyendo a minimizar la materialización de incidentes de seguridad de información.
- Fortalecer la cultura e higiene en seguridad de la información dentro del instituto.
- Determinar el acceso a los activos de información y adoptar las medidas esenciales de seguridad de la información necesarias para proteger al IDPYBA de amenazas que podrían afectar en alguna medida la confidencialidad, integridad y disponibilidad de la información, ocasionando pérdida o mal uso de los activos de información. Para ello se realizará la valoración y tratamiento de Riesgos de seguridad de la información, definido en el Plan de riesgos 2023.

- Cumplir con los requisitos legales vigentes aplicables a la naturaleza de la Entidad en materia de Seguridad de la Información, diligenciando y realizando seguimiento por medio de la herramienta de autodiagnóstico del MINTIC, el cual lidera la política de Gobierno Digital, apoyado por la Alta consejería para las TICs del Distrito y de conformidad con los requerimientos de las auditorías.

  Identificar y realizar la valoración de los activos de información, para determinar y evaluar los riesgos de seguridad de la información. Teniendo en cuenta las vulnerabilidades y amenazas que puede materializar el riesgo, como se establece en el plan de riesgos.

- Minimizar, gestionar y dar tratamiento a los riesgos de seguridad de la información, para que sean conocidos y según su impacto sean asumidos, transferidos, minimizados y/o eliminados de forma eficiente y adaptada a los cambios que se produzcan en la entidad, en el entorno y la tecnología.

- Continuar con el fortalecimiento e implementación de políticas y procedimientos específicos a la política de seguridad y privacidad de la información actualizada, con el fin de asegurar su vigencia y eficacia.

## 3. NORMATIVIDAD Y LINEAMIENTOS CONCEPTUALES Y METODOLÓGICOS.

Conforme con lo establecido en la normatividad vigente el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, hace referencia a las siguientes normas, que se deben tener en cuenta para el desarrollo de la apropiación del MSPI en la entidad:

| Marco Normativo | Descripción |
|---|---|
| Constitución Política de Colombia. Artículo 15 | Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar |
| Ley 1952 de 2019 | Por medio de la cual se expide el código general Disciplinario |
| Ley 1915 de 2018 | Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos. |
| Ley 1712 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 |
| Ley 1581 de 2012 | Por la cual se dictan disposiciones generales para la protección de datos personales. |
| Ley 1273 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 |
| Ley 1266 de 2008 | Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. |
| Ley 1221 de 2008 | Se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones |
| | |
| Decreto 680 de 2001 | |

| | |
|---|---|
| | Modifica la Comisión Distrital de Sistemas y es establece el carácter de obligatoriedad en la adopción de las políticas que la CDS determine. |
| Decreto 053 de 15 de febrero de 2002 | Por el cual se crea el Comité para la implementación del Número Único de Emergencias y Seguridad del Distrito Capital, del cual forma parte el secretario técnico de la CDS. |
| Decreto 397 de 17 de septiembre de 2002 | Delegar en el secretario general de la Alcaldía Mayor de Bogotá las atribuciones conferidas al alcalde Mayor en el Acuerdo 57 de 2002 como presidente de la Comisión Distrital de Sistemas, y las demás funciones que se requieran en el ejercicio de esta atribución |
| 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 619 del 28 de diciembre de 2007 | Que el Decreto Distrital 619 de 2007 establece la estrategia de Gobierno Electrónico en el Distrito y define la necesidad de reglamentar gradualmente por parte de la Secretaría General de la Alcaldía Mayor de Bogotá la utilización de medios Electrónicos en diversos trámites, procedimientos y actuaciones de las entidades distritales. |
| Decreto 2106 de 2019 | , establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones |
| Decreto 612 de 2018 | Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado. |
| Decreto 460 del 1995 | Registro Nacional del Derecho de Autor |
| Decreto 1421 de 1993 | Por medio del cual se dicta el régimen especial para el Distrito Capital de Santa Fe de Bogotá, ciudad con autonomía para la |

| | |
|---|---|
| | gestión de sus intereses, dentro de los límites de la Constitución y la ley. |
| Decreto 1008 de 2018 | 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 728 de 2017 | Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico. |
| 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. |
| Decreto 1083 de 2015 | Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función<br>Pública.<br>Se establecen las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”. |
| Decreto 1081 de 2015 | Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia. |
| Decreto 1078 de 2015 | Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. |

| | |
|---|---|
| Decreto 1074 de 2015. | Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26. |
| Decreto 103 de 2015 | Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. |
| Decreto 886 de 2014 | Por el cual se reglamenta el Registro Nacional de Bases de Datos. |
| Decreto 1377 de 2013 | Por el cual se reglamenta parcialmente la Ley 1581 de 2012. |
| Decreto 2609 de 2012 | Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las entidades del Estado. |
| Decreto 1083 de 2015 | Decreto Único Reglamentario de Función Pública 1083 de 2015 |

| | |
|---|---|
| Decreto 1078 de 2015 | Manual para la Implementación de la Política de Gobierno Digital Decreto 1078 de 2015 libro 2, parte 2, título 9. Cap. 1. |
| Decreto 1080 de 2015 | Se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre. |
| Decreto 415 de 2016 | Se adiciona el Decreto Único reglamentario del sector de la Función Pública, Decreto 1083 de 2015, en lo relacionado con la definición de lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones". |
| Directiva 005 -junio de 2005 | Por medio de la cual se adoptan las Políticas Generales de Tecnología de Información y Comunicaciones aplicables al Distrito Capital. |
| Directiva 22 de 2011 | Política de estandarización de la información de identificación, caracterización, ubicación y contacto de los ciudadanos/as: que capturan las entidades del Distrito capital. |
| Directiva 005 del 12 de junio de 2005 | Por medio de la cual se adoptan las Políticas Generales de Tecnología de Información y Comunicaciones aplicables al Distrito Capital. |
| Resolución 305 de 2008 | Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre. |

| | |
|---|---|
| CONPES 3854 de 2016 | Política Nacional de Seguridad digital. |
| CONPES 3995 de 2011 | Política Nacional de confianza y seguridad digital. |

## 4. DIAGNÓSTICO.

Realizando el seguimiento y diagnostico por medio del documento "Instrumento_Evaluacion_MSPI 2023" se ha evidenciado un avance significativo durante la vigencia 2023, que requieren fortalecerse para la vigencia 2024 debido a que no se ha tenido un avance fuerte en algunas actividades, las cuales ya están establecidas en el Plan de Seguridad y Privacidad de la Información para la presente vigencia.

Como se observa en la ilustración No.1 de los catorce (14) dominios que comprende el MSPI se han gestionado trece (13) para una calificación de cuarenta y ocho (48) puntos de cien (100) puntos, en donde se han gestionado tres (3) dominios y un (1) optimizado, Seis (6) se encuentran en estado efectivo, cuatro (4) en estado repetible y uno (1) en estado inicial.

*Ilustración 1*

Reporte de autodiagnóstico del MINTIC

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

| No. | Evaluación de Efectividad de controles DOMINIO | Calificación Actual | Calificación Objetivo | EVALUACIÓN DE EFECTIVIDAD DE CONTROL |
|---|---|---|---|---|
| A.5 | POLITICAS DE SEGURIDAD DE LA INFORMACIÓN | 60 | 100 | EFECTIVO |
| A.6 | ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | 36 | 100 | REPETIBLE |
| A.7 | SEGURIDAD DE LOS RECURSOS HUMANOS | 81 | 100 | OPTIMIZADO |
| A.8 | GESTIÓN DE ACTIVOS | 46 | 100 | EFECTIVO |
| A.9 | CONTROL DE ACCESO | 66 | 100 | GESTIONADO |
| A.10 | CRIPTOGRAFÍA | 20 | 100 | INICIAL |
| A.11 | SEGURIDAD FÍSICA Y DEL ENTORNO | 74 | 100 | GESTIONADO |
| A.12 | SEGURIDAD DE LAS OPERACIONES | 46 | 100 | EFECTIVO |
| A.13 | SEGURIDAD DE LAS COMUNICACIONES | 64 | 100 | GESTIONADO |
| A.14 | ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS | 41 | 100 | EFECTIVO |
| A.15 | RELACIONES CON LOS PROVEEDORES | 40 | 100 | REPETIBLE |
| A.16 | GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN | 29 | 100 | REPETIBLE |
| A.17 | ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO | 34 | 100 | REPETIBLE |
| A.18 | CUMPLIMIENTO | 56,5 | 100 | EFECTIVO |
| | *PROMEDIO EVALUACIÓN DE CONTROLES* | 50 | 100 | EFECTIVO |


Fuente: Herramienta de autodiagnóstico del MINTIC diligenciada para el IDPYBA

Por lo cual al verificar el estado de avance por el ciclo PHVA, se determina que el IDBYPA se encuentra la fase de planificación del 28%, Implementación 12%, Evaluación y desempeño 11% y mejora continua 12%, para un total de 63% de avance actual de la entidad. Evidenciando que se requiere fortalecer y dar continuidad con las acciones para el incremento de la fase de planeación, que contribuirán al aumento de las otras fases para alcanzar el avance esperado, según lo planteado en el autodiagnóstico del MSPI.

Teniendo en cuenta los anterior se hace necesario, efectuar actividades para dar continuidad con el seguimiento, implementación y mejora continua del plan de Seguridad y Privacidad de la Información dentro del IDPYBA.

1. Continuar con la consolidación de la actualización de inventario de activos de información y revisión con el apoyo de la oficina asesora jurídica para posterior aprobación en comité de Gestión y Desempeño, para la vigencia 2024.
2. realizar seguimiento de los riesgos para Seguridad Digital identificados con las áreas, para monitorear y efectuar las acciones que correspondan en pro de prevenir materialización de incidentes de seguridad de la información
3. Continuar con el monitoreo de controles de seguridad de la información, teniendo en cuenta las alertas del MinTIC y Alta Consejería que se emiten mensualmente, para adopción y fortalecimiento de cultura de seguridad de la información

## 5. DESARROLLO DEL PLAN.

Los activos de información del Instituto Distrital de Protección y Bienestar Animal han sido identificados y clasificados, para lo cual se considera dentro del presente plan, realizar la actualización y revisión al interior del Instituto para establecer su grado de criticidad. Así mismo, deben tener un propietario designado, quien tiene la responsabilidad de garantizar que se clasifican adecuadamente, revisar las restricciones de acceso y la seguridad del activo de información como insumo principal para desarrollar las actividades y controles relacionados con la seguridad de la información.

El IDPYBA realizará la clasificación de la información, teniendo en cuenta el criterio de confidencialidad de la siguiente manera:

**1)** Pública: Este nivel es bajo, donde todo el personal del área y del IDPYBA tiene acceso a la información, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad. Dentro de este nivel se encuentra:

a. Información pública de las entidades (Ley 1712 de 2014): ofertas de cargos en el sector público, actas de adjudicación de contratos. En este nivel se debe seleccionar la información pública que puede ser publicable (Información divulgada oficialmente por los canales de comunicación establecidos por el IDPYBA).

b. Información que contenga datos personales públicos (Ley 1581 de 2012): Documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y documentos que contengan información correspondiente al estado civil de las personas.

c. Información con datos abiertos (Ley 1712 de 2014): Archivos o documentos que contengan datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo custodia del

IDPYBA, los cuales pueden ser puestos a disposición de cualquier ciudadano, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de estos.

**2)** Pública clasificada: Este nivel de confidencialidad es restringido, en donde no todos los funcionarios, contratistas y terceras partes tiene acceso a la información. En este nivel se relaciona a los usuarios y cargos autorizados permitidos para realizar consultas. (autorizado por el responsable de la información, la cual está disponible para todos los procesos del IDPYBA, en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de esta). Dentro de los datos e información en este nivel se encuentra:

a) Información pública clasificada de las entidades (Ley 1712 de 2014): Toda información que pertenece al ámbito propio, particular y privado o semiprivado de una persona jurídica, información exceptuada por daño de derechos a personas jurídicas, información correspondiente a secretos comerciales, industriales y profesionales, así como los estipulados en el parágrafo del artículo 77 de la ley 1474 de 2011, información operativa del IDPYBA (detalles de configuración de la infraestructura, ubicación de áreas seguras), correspondencia, formas de comunicación de la entidad y planes operacionales.

b) Información con datos personales semiprivados (Ley 1581 de 2012): Toda información que pertenece al ámbito propio, particular y semiprivado de una persona natural y documentos que contengan información personal (número de cuenta de ahorros, dirección de residencia, teléfonos personales, datos de núcleo familiar, entre otros).

c) Información con datos personales privados (Ley 1581 de 2012): Toda información que pertenece al ámbito propio, particular y privado de una persona natural, información exceptuada por daño de derechos a personas naturales, información de la intimidad de las personas (bajo las limitaciones propias que impone la condición de servidor público), información que pueda afectar la vida, la salud o la seguridad del individuo y datos personales de las hojas de vida que no son públicos.

**3)** Pública Reservada: Este nivel de confidencialidad es alto, donde solo cierto personal del área (autorizado por el responsable de la información) tiene acceso a la información, en caso de ser conocida por terceros sin autorización del propietario de la información, puede conllevar un impacto negativo de índole legal, operativo, pérdida de imagen o económica. Dentro de este nivel se encuentra:

a) Información que por mandato legal tiene reserva (ej. reserva médica, reserva bancaria, reserva legal, identidad de menores involucrados en hechos delictivos o en situación de desplazamiento), información exceptuada de acceso a la ciudadanía por daño a los intereses públicos, información de defensa y seguridad nacional y de seguridad pública, información que afecte las relaciones internacionales, aquella que sirva para la prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso, derechos de la infancia y la adolescencia, estabilidad macroeconómica y financiera del país, salud pública o documentos que contengan las opiniones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos.

Igualmente se establecerán controles técnicos, para realizar seguimiento de la infraestructura tecnológica, velando por que estos cuenten con los principios de confidencialidad, integridad y disponibilidad de la información.

## 5.1. POLITICAS

El instituto Distrital de Protección y Bienestar Animal establece una política general, soportada por varias políticas específicas que dan apoyan el desarrollo de esta, en cumplimiento con el MSPI, todas diseñadas y lideradas desde la Subdirección de Gestión Corporativa (SGC), quien es la encargada de la seguridad de la información TIC, teniendo en cuenta los siguientes criterios:

- Creación de políticas

Las políticas deben ser creadas por el área encargada de la seguridad y privacidad de la información y respaldadas por la Alta Dirección de la entidad, con la asesoría de las áreas técnicas responsables de los temas asociados a las mismas. Estas políticas deben definir claramente roles y responsabilidades en la SGC y con los propietarios de la información y responsables de riesgos.

- Aprobación de políticas

Las políticas relacionadas con la seguridad y privacidad de la información deben ser aprobadas por el Comité Institucional de Gestión y Desempeño. Con base en las recomendaciones de la Subdirección de Gestión Corporativa, la Oficina Asesora de Planeación, la oficina asesora de Control Interno y demás interesados en la seguridad y privacidad de la información.

- Actualización de políticas

Las políticas de seguridad y privacidad de la información se deben revisar periódicamente o si ocurren cambios significativos. Cualquier requerimiento de modificación, cambio o actualización de las políticas de seguridad y privacidad de la información, debe ser dirigida al Comité Institucional de Gestión y Desempeño, con base en las recomendaciones del área de la seguridad y privacidad de la información.

- Nivel de cumplimiento de la política

Todas las personas cubiertas por el alcance y aplicabilidad deben dar cumplimiento de la política.

Participar en las auditorías internas y externas de acuerdo con lo establecido en el plan de auditorías para la vigencia 2023.

## 5.2. LINEAMIENTOS GENERALES PARA LAS POLÍTICAS ESPECIFICAS Y PROTOCOLOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Seguridad de la Información:

La seguridad de la información tiene por objetivo establecer los lineamientos generales con el propósito de preservar los niveles de confidencialidad, integridad y disponibilidad de los activos de información, que dependen o usan las tecnologías de la información y las comunicaciones del Instituto Distrital de Protección y Bienestar Animal, entidad adscrita al Sector Ambiente de Bogotá D.C., conforme a los controles de seguridad y privacidad determinados en la entidad.

Procedimientos:

Los procedimientos lineamientos e instructivos, constituyen una base importante para la preservación de la seguridad y privacidad de la información. Se han diseñado procedimientos, lineamientos e instructivos, que cubren las políticas de seguridad y privacidad de la información. A continuación, se indican:

- Política de Seguridad y privacidad de la información

- Políticas específicas de seguridad de la información
  - ✓ Política específica para clasificación de activos de
  - ✓ Política específica de seguridad física
  - ✓ Política de antivirus
  - ✓ Política de uso de correo electrónico corporativo
  - ✓ Política de uso de contraseñas
  - ✓ Política específica para dispositivos móviles
  - ✓ Política de uso de servicios de red
  - ✓ Política específica de teletrabajo
  - ✓ Política especifica de uso de medios tecnológicos de comunicación y acceso a Internet
  - ✓ Política específica de control de acceso a la información
  - ✓ Política específica de uso de controles criptográficos
  - ✓ Política específica de escritorio y pantalla limpios
  - ✓ Política específica de copias de respaldo de información
  - ✓ Política específica de transferencia o intercambio de información
  - ✓ Política específica de desarrollo software seguro
  - ✓ Política específica para relaciones con proveedores
  - ✓ Política específica de derechos de uso de propiedad intelectual
  - ✓ Política específica para clasificación de activos de información
  - ✓ Política de uso de red privada virtual (VPN)
  - ✓ Política de control de cambios
  - ✓ Acuerdo Confidencialidad Reserva Manejo Información
  - ✓ Acuerdo de confidencialidad y Transferencia de Información con terceros

Protección De Datos Personales:

Establecer criterios generales para la recolección, almacenamiento, uso, circulación y supresión de los datos personales y niveles de seguridad y privacidad adecuados en las bases de datos y activos de información que intervengan en el tratamiento de dichos datos, para evitar posibles adulteraciones, pérdidas, consultas, usos o accesos no autorizados.

Gestión De Riesgos:

El objetivo es brindar principios y directrices genéricos para gestionar el riesgo para identificar y establecer controles efectivos que garanticen salvaguardar los niveles de confidencialidad, integridad y disponibilidad de la información.

Así mismo, para la evaluación de riesgos en seguridad de la información se ha clasificado sus activos de información por proceso, a los cuales se les ha identificado los riesgos teniendo en cuenta que la entidad debe preservar la confidencialidad, integridad y disponibilidad de la información.

- Acceso no autorizado a la información.
- Divulgación de información sensible.
- Denegación del servicio.
- Daño de la información.
- Ataques externos o internos.
- Pérdida o robo de la información.
- Modificación no autorizada.

## 6. ALCANCE DE LA ESTRATEGIA DE SEGURIDAD DE INFORMACIÓN

Los contenidos del presente plan son aplicables a los activos de información de todos los procesos del Instituto Distrital de Protección y Bienestar Animal, consta de las políticas, procedimientos y controles para la preservación de confidencialidad, integridad y disponibilidad de la información, en concordancia con el plan de riesgos y las actividades dentro del plan para el tratamiento de riesgos 2023.

Por lo anterior, se contempla como fase cero el atender los riesgos identificados en la valoración de riesgos e implementar el plan de tratamiento de riesgos 2024 como se muestra a continuación:

*Tabla 1*

Plan de tratamiento de riesgos

| | ACTIVIDAD | FECHA |
|---|---|---|
| 1. | Revisión de estado de tratamiento y controles de línea base de seguridad | TRIMESTRAL 2024 |
| 2. | Identificación y evaluación de riesgos de seguridad y privacidad de la información | 2 TRIMESTRE 2024 |
| 3. | Tratamiento y control de riesgos de seguridad y privacidad de la información | 3 TRIMESTRE 2024 |
| 4. | Monitoreo, planes de mejoramiento | TRIMESTRAL 2024 |

Fuente: Elaboración propia Gestión tecnológica

En paralelo la estrategia contempla el trabajo continuo en capacitación, concientización en seguridad y privacidad de la información. Lo anterior buscando controlar las acciones que afectan la seguridad de la información y que ponen en riesgo la disponibilidad, confidencialidad e integridad en el Instituto Distrital de Protección y Bienestar Animal, como son:

- Dejar los computadores encendidos en horas no laborables.
- Enviar información clasificada del instituto por correo físico, copia impresa, o electrónica sin la debida autorización y/o sin la utilización de los protocolos establecidos para la divulgación.
- Guardar información clasificada en cualquier dispositivo de almacenamiento que no pertenezca al Instituto.
- Conectar computadores portátiles u otros dispositivos electrónicos personales a la red de datos del Instituto sin la debida autorización.
- Ingresar a la red de datos por cualquier servicio de acceso remoto sin la autorización de la Subdirección de Gestión Corporativa – Grupo de sistemas, y sin la autorización de los propietarios de los activos de información, quienes determinan quienes acceden a la información y con que privilegios.
- Usar servicios de internet en los equipos del instituto, diferente al provisto por la oficina de sistemas.
- Promoción y mantenimiento de actividades personales, o utilización de los recursos tecnológicos del instituto para beneficio personal.
- Permitir que personas ajenas al Instituto ingresen sin previa autorización a las áreas restringidas o donde se procese información digital.
- No clasificar y/o etiquetar la información.

- No guardar bajo llave documentos impresos que contengan información clasificada al terminar la jornada laboral.
- No retirar de forma inmediata todos los documentos con información sensible que envíen las impresoras y dispositivos de copiado.
- Reutilizar papel que contenga información sensible, no borrar la información estricta de tableros o pizarras al finalizar las reuniones de trabajo y no garantizar que no queden documentos o notas escritas sobre las mesas.
- Hacer uso de la red de datos del Instituto, para obtener, mantener o difundir material publicitario o comercial (no institucional), así como distribución de cadenas de correos.
- Instalar software en la plataforma tecnológica del Instituto cuyo uso no esté autorizado por la Subdirección de Gestión Corporativa – Grupo de sistemas, y que pueda atentar contra las leyes de derechos de autor o propiedad intelectual.
- Uso de la identidad institucional digital (cuenta de usuario y contraseña) de otro usuario o facilitar, prestar o permitir el uso de su cuenta personal a otro funcionario o contratista.
- Dejar al alcance de personas no autorizadas los dispositivos portátiles, móviles y de almacenamiento removibles, entregados para actividades propias del cumplimiento de sus funciones.
- Retirar de las instalaciones del Instituto computadores de escritorio, portátiles e información física o digital clasificada previamente como confidencial o restringida, sin autorización o abandonarla en lugares públicos o de fácil acceso.
- Entregar, enseñar o divulgar información clasificada del Instituto a personas o entidades no autorizadas.
- Llevar a cabo actividades ilegales, o intentar acceso no autorizado a la plataforma tecnológica del instituto o de terceras partes.
- Ejecutar cualquier acción que difame, afecte la reputación o imagen del Instituto o alguno de sus funcionarios, utilizando para ello la plataforma tecnológica.
- Realizar cambios no autorizados en la plataforma tecnológica del Instituto.
- Otorgar privilegios de acceso a los activos de información a funcionarios o terceros no autorizados.
- Ejecutar acciones para eludir y/o modificar los controles establecidos en los lineamientos de la política de seguridad de la información.
- Consumir alimentos y bebida, cerca de cuartos o plataformas tecnológicas.
- Realizar cualquier otra acción que contravenga disposiciones constitucionales, legales o institucionales.

Cada una de las prácticas anteriormente mencionadas u otras que afecten la seguridad de la información, acarrearán medidas administrativas, acciones disciplinarias y/o penales a que haya lugar, de acuerdo con los procedimientos establecidos para cada caso.

En una segunda fase se deben desarrollar y establecer la implementación de políticas específicas de seguridad de la información con cada una de las áreas del IDPYBA, se van a adoptar 5 políticas específicas de acuerdo con la guía impartida por MINTIC para la seguridad y privacidad de la información, a continuación, se mencionan las políticas específicas a adoptar:

- Política Controles Criptográficos
- Políticas de Firewall
- Políticas Base de Datos
- Políticas de Áreas Seguras
- Política de Desarrollo de Software

Se entiende Política de seguridad como una declaración de alto nivel que describe la posición de la entidad sobre un tema específico entorno a la Seguridad y privacidad de la información.

## 7. CRONOGRAMA

Para hacer realizables las estrategias, estas son materializadas en actividades de acuerdo con su complejidad; el IDPYBA tiene previsto realizar las siguientes actividades para el desarrollo y cumplimiento del Plan de Seguridad y Privacidad de la Información, el cual se encuentra en la matriz adjunta al presente documento.

## 8. EVALUACIÓN Y SEGUIMIENTO

*Tabla 2*

Indicadores de seguimiento del PSPI

| N° | ACTIVIDAD | META ESPERADA | PRODUCTO O ENTREGABLE | MES DE EJECUCIÓN | | RESPONSABLE |
|---|---|---|---|---|---|---|
| | | | | FECHA INICIO | FECHA FINAL | |
| 1 | Revisión y creación de Políticas de Seguridad de la información y procedimiento para su implementación | 4 | Documento de creación de Políticas y/o Procedimiento | Febrero | Octubre | Profesional Subdirección de gestión Corporativa Tecnología |
| 2 | Actualizar y hacer seguimiento al Autodiagnóstico de Seguridad y privacidad de la Información con la herramienta MINTIC de Gobierno Digital | 1 | Actualización de Autodiagnóstico con herramienta MINTIC de Gobierno Digital | Enero | Noviembre | |
| 3 | Actualización y Clasificación de los Activos de Información | 1 | Actualización de Activos de Información Actualizado | Junio | Diciembre | |
| 4 | Recibir auditorias solicitadas | 1 | Informe de Auditoria | Octubre | Diciembre | |
| 5 | Valoración de Riesgos, tratamiento y controles de Seguridad de la Información | 1 | Informe de Valoración y tratamiento de Riesgos | Julio | Diciembre | |

Fuente: Elaboración propia Gestión Tecnológica

**9.** REFERENCIAS Y BIBLIOGRAFÍA.

Listado maestro del Modelo de Seguridad y Privacidad de la información -MSPI
https://gobiernodigital.mintic.gov.co/692/articles-237872_maestro_mspi.pdf

Manual de implementación Gobierno Digital del MinTIC
https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/