Tabla de contenido

1 DERECHOS DE AUTOR

2 INTRODUCCIÓN

El Sistema de Gestión de Seguridad de la Información – SGSI, del Instituto Distrital de Protección y Bienestar Animal-IDPYBA, es el documento de políticas de seguridad de la información, el cual expresa el compromiso de la alta dirección con la seguridad de la información, así como, la identificación de las reglas y procedimientos que cada usuario que accede o usa los recursos tecnológicos de la Entidad y debe conocer para preservar la confidencialidad, la integridad y la disponibilidad de los sistemas y la información que usan.

Estas políticas serán revisadas con regularidad, 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.

3 OBJETIVO

Establecer y difundir los diferentes criterios y actividades que deben seguir todos los servidores públicos, contratistas, terceros, practicantes, usuarios, entre otros, que tengan una relación contractual con el Instituto Distrital de Protección y Bienestar Animal frente al acceso a los activos de información, con el propósito de que tengan acciones y comportamiento acordes con el plan de Seguridad y Privacidad de la Información. Buscando verificar y aplicar el mejoramiento continúo del Sistema de Gestión de Seguridad de la Información – SGSI del Instituto Distrital de Protección y Bienestar Animal.

3.1 OBJETIVOS ESPECIFICOS

Los siguientes son los objetivos de seguridad de la información a tener en cuenta en el IDPYBA:

- Proteger los recursos de información y tecnologías frente a amenazas internas y externas, deliberadas o accidentales, buscando asegurar el cumplimiento de confidencialidad, integridad y disponibilidad de la información, mediante el uso adecuado de los controles efectivos.
- Garantizar la integridad, confidencialidad y el acceso a la información de acuerdo a los niveles y criterios de seguridad que establecidos por la Entidad y a los exigidos por la normatividad vigente.
- Identificar mediante una adecuada evaluación del riesgo, el valor de la información, así como las vulnerabilidades y las amenazas a las que están expuestos los activos de información.
- 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, el entorno y la tecnología.
- Asegurar el mejoramiento continuo de la seguridad de la información para responder a Los cambios futuros.
- Crear un modelo organizacional de seguridad de la información, definiendo los roles y responsabilidades de los participantes en la implementación de la política.

- Promover y programar acciones continuas de mejoramiento de niveles de cultura en seguridad de la información, buscando lograr una concientización de los funcionarios mencionados anteriormente, minimizando la ocurrencia de incidentes de seguridad de información.
- Contar con la política de seguridad actualizada, con el fin de asegurar su vigencia y eficacia.
- Cumplir con los requisitos legales vigentes aplicables a la naturaleza de la Entidad en materia de Seguridad de la Información.

3.2 OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

a) Fortalecer la seguridad y disponibilidad de la información y plataforma tecnológica de acuerdo a procedimientos complementarios de apoyo.
b) Administrar los eventos de seguridad de la información.
c) Fortalecer el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información.
d) Cumplir con los requisitos legales aplicables a la Entidad en materia de Seguridad de la Información.
e) Fomentar una cultura de seguridad de la información en los servidores públicos (funcionarios y contratistas).

4 ALCANCE/APLICABILIDAD

El alcance de la Seguridad de la Información – SGSI, aplica a los activos de información de los procesos que conforman el mapa de procesos del IDPYBA. Por lo anterior, estas políticas aplican a toda la Entidad, sus funcionarios, contratistas, sujetos de control fiscal, usuarios internos y externos que acceden o hacen uso de cualquier activo de información, así como exfuncionarios y excontratistas que hayan tenido acceso a cualquier activo de información, independientemente de su ubicación, medio o formato del Instituto Distrital de Protección y Bienestar Animal-IDPYBA, así como a la ciudadanía en general.

5 CUMPLIMIENTO

Tanto la política General del SGSI como las políticas específicas que de esa se desprendan son de obligatorio cumplimiento para todas las personas mencionadas dentro del alcance y deberán dar acatamiento al 100% de las mismas.

El incumplimiento a la política de Seguridad y Privacidad de la Información del Instituto Distrital de Protección y Bienestar Animal-IDPYBA, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las Lineamientos que competen al gobierno nacional y territorial en cuanto a seguridad de la Información se refiere.

6 TERMINOLOGÍA

- **Activo:** en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tenga valor para la organización.
- **Activo 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.

- **Activo de información:** Conocimiento o datos que tienen valor para el individuo u organización[1].
- **Acuerdo de Confidencialidad**: Documento donde se plasma el compromiso para mantener la confidencialidad de la información de la Entidad, a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud del desarrollo de las funciones desempeñadas en la Entidad.
- **Autenticación:** Asegurar que una característica declarada de una Entidad es correcta.
- **Autenticidad**: Propiedad de que una Entidad es lo que dice ser.
- **Confidencialidad**: Propiedad de la información que la hace no disponible o sea divulgada a individuos, Entidades o procesos no autorizados.
- **Dirección IP:** Número que identifica, de manera lógica y jerárquica en una red informática a un dispositivo (computadora, tableta, portátil, Smartphone).
- **Disponibilidad**: Propiedad de ser accesible y utilizable a demanda por una Entidad autorizada.
- **Incidente de seguridad:** Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información.
- **Información**[2]: Es un activo esencial para el negocio de una organización y por consiguiente necesita ser debidamente protegida. La información puede ser almacenada en muchas formas, incluyendo formato digital (por ejemplo, ficheros almacenados en medios electrónicos u ópticos), formato físico (por ejemplo, en papel), así como la información intangible que forma parte del conocimiento de los empleados. La información puede ser transmitida por diferentes medios incluyendo: mensajería, comunicación electrónica o verbal. Independientemente del formato o del medio por el cual se transmite la información, es necesaria siempre una protección adecuada.
- **Integridad**: Propiedad de exactitud y completitud de la información.
- **Medios removibles:** Dispositivos tecnológico de almacenamiento de información diseñados para ser extraídos del computador.
- **Mejora Continua:** El objetivo de la mejora continua de un SGSI es aumentar la probabilidad de lograr los objetivos relativos a la preservación de la confidencialidad, disponibilidad e integridad de la información. El foco de la mejora continua es buscar oportunidades para la mejora y no asumir que las actividades de gestión existentes son suficientemente buenas o tan buenas como podrían ser.
- **Política:** Declaración de alto nivel que describe la posición de la Entidad sobre un tema específico.
- **Seguridad de la información**: Asegura la confidencialidad, integridad y disponibilidad de la información. La seguridad de la Información implica la aplicación y gestión de controles apropiados que involucran la consideración de un amplio rango de amenazas, con el objetivo de asegurar el éxito empresarial sostenido, así como su continuidad, y minimizar las consecuencias de los incidentes de la seguridad de la información.
- **Vulnerabilidad:** Debilidad de un activo o control que pueda ser explotada por una a más amenazas.

7 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Instituto Distrital de Protección y Bienestar Animal-IDPYBA, administra los riesgos de seguridad de la información para generar, implementar y monitorear los controles que permitan mantener la

integridad y la disponibilidad de sus activos informáticos en cumplimiento de los requisitos aplicables. También promueve la cultura de la seguridad informática para evitar y administrar incidentes que ayudan al mejoramiento continuo de Gestión de Seguridad de la Información – SGSI.

Para el Instituto Distrital de Protección y Bienestar Animal-IDPYBA, 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 la misma, acorde con las necesidades de los diferentes grupos de interés identificados.
De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del 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 clientes, socios 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, terceros, aprendices, practicantes y clientes del IDPYBA.
- Garantizar la continuidad del negocio frente a incidentes.
- El IDPYBA 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.

8 ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN – SGSI - FASES DE IMPLEMENTACIÓN

EL SGSI es aplicable 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 la declaración de aplicabilidad avalada por el Comité de la Mesa de Tecnologías de la Información.

En una primera fase se debe buscar controlar las acciones que afectan la seguridad de la información y que ponen en riesgo la disponibilidad, confidencialidad e integridad en el Instituto 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 oficina de sistemas.
- 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.
- 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 Oficina 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, 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 a 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 4 de las 25 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 de administración de contraseñas.
- Política de control de acceso y áreas protegidas.
- Política de gestión de activos de información.
- Política de uso adecuado de los activos de información. (uso de internet, uso del correo electrónico, uso de redes, uso de computación en la nube, política de acceso y uso de componentes electrónicos de procesamiento.

En una tercera fase se deben fortalecer temas tales como mencionar el manejo y uso adecuado de los activos de información para los cuales ya se han realizado las tareas de levantamiento y se encuentran publicados los activos de acuerdo a su tipología como activos de software, hardware y los activos información. Antes de 31 diciembre de 2020, se debe entregar y publicar el nuevo inventario de activos de información del Instituto.

Hay que incorporar una tarea adicional que tiene que ver con el etiquetado de la información y la devolución de los activos esto relacionados con la gestión de los activos de medios removible y la disposición de los activos y los ubicados en dispositivos móviles.

9 MARCO DE REFERENCIA

Entendiendo que la información es un activo fundamental para el éxito y el cumplimiento de la misión del Instituto, este documento busca alinear los lineamientos contemplados en la ISO 27000 como principio normativo para la seguridad de la información.

La información, así como su plataforma tecnológica que la soporta, son considerados como activos estratégicos del Instituto, por lo tanto, se requiere para su implementación y puesta en marcha del establecimiento de políticas que definan el marco de control para brindar seguridad a los activos de información del Instituto.

Los activos de información deben ser clasificados como el soporte de la misión y visión, por lo requieren ser conceptualizados, utilizados y manejados dentro de un adecuado entorno de seguridad, cualquiera que sea el medio y el entorno tecnológico en el cual se presentan.

Todas las organizaciones de carácter público como privado toman como pilar fundamental los sistemas de información y los recursos informáticos como soporte de la gestión, por lo que se requiere de implementar el sistema de gestión de seguridad de la información como una estrategia que esté relacionada con las necesidades, objetivos institucionales y direccionamiento estratégico.

Al implementar el plan de seguridad de la información se orientan los aspectos necesarios para establecer, operar, mantener y dirigir de manera estandarizada, sistemática y organizada un sistema efectivo que permita un tratamiento seguro de la información.

10 COMITÉ MESA DE TECNOLOGIAS DE INFORMACIÓN

El Comité de Mesa de Tecnologías de Información, es creado en el Instituto Distrital de Protección y Bienestar Animal mediante lineamiento de MIPG y tiene dentro de sus funciones la de impulsar, hacer seguimiento y/o verificación de la implementación del Sistema de Gestión del PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Está conformado por:

a) El director del Instituto Distrital de Protección y Bienestar Animal o su delegado quien lo preside.
b) El Subdirector de Gestión Corporativa o su delegado.
c) El subdirector de Atención a la Fauna o su delegado.
d) El Subdirector de Cultura y Conocimiento o su delegado.
e) El Coordinador del Área de Tecnología o su delegado.
f) El jefe del Oficina Asesora de Planeación o su delegado.
g) El jefe de la Oficina de Control Interno o su delegado.
h) El jefe de la oficina asesora Jurídica o su delegado,
i) y los asesores de la dirección.

Las funciones del Comité de Mesa de Tecnologías de Información para el tema de Seguridad de la Información son:

a) Realizar el seguimiento y/o verificación de la implementación de los requisitos, controles e indicadores del Sistema de Gestión de Seguridad de la Información SGSI del Instituto Distrital de Protección y Bienestar Animal.
b) Establecer las medidas necesarias para evitar situaciones de riesgo o incidentes de seguridad física o virtual que puedan contribuir a la generación de pérdidas de Información en la entidad.
c) Dirigir las acciones y decisiones conforme a la normatividad vigente en materia de seguridad de la información.
d) Aprobar el uso de metodologías apropiadas para garantizar confiabilidad, disponibilidad e integridad de la seguridad de la información.
e) Establecer las medidas y acciones pertinentes, de acuerdo con los resultados arrojados en los diagnósticos de la seguridad de la información.
f) Revisar y aprobar los proyectos de seguridad de la información y ser un canal facilitador de su respectiva implementación.
g) Implementar y dar mejora continua al Sistema de Gestión de Seguridad de la Información SGSI.
h) Aprobar las medidas y Políticas de Seguridad de la Información y sus mejoras, en materia de activos de la información de la Entidad.
i) Analizar los respectivos planes de acción para mitigar y/o eliminar riesgos en materia de seguridad de la información.

j) Las demás funciones que el Comité de Mesa de Tecnologías de Información estime sean de su competencia en materia de seguridad de la información.

La mesa de tecnologías de información se entiende como un soporte técnico de apoyo a las decisiones que sean enmarcadas dentro de las políticas de seguridad de la información, incluyendo la ejecución del plan de seguridad de la información que se presenta, dentro de este comité se deben tener en cuenta la conformación de los roles y responsabilidades de cada área y dependencia del Instituto, en la cual se enmarcan los compromisos para dar cumplimiento a los lineamientos de seguridad de la información.

Esta mesa de trabajo se conformó sobre finales del año 2018, definiéndose tareas específicas dentro de las cuales se encuentra la presentación del plan de seguridad de la información incluyendo las siguientes actividades:

- DEFINICIONES DE USUARIOS.
- SUMINISTRO DE CONTROL DE ACCESO
- GESTION DE CONTRASEÑAS
- PERIMETROS DE SEGURIDAD.
- AREAS DE CARGA

11 TAREAS DESARROLLADAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Se definieron y se ejecutaron las siguientes tareas asociadas a la Seguridad y Privacidad de Información:

Código	Nombre
1	La creación y documentación de Matriz de riesgos de seguridad de la información versus controles.
2	Creación de nuevos riesgos de seguridad de la información
3	Implementación del sistema de información de gestión de Documental y Correspondencia
4	Fortalecer y mejorar la seguridad de la información y la continuidad de la entidad, mediante la implementación de La seguridad centralizada que se administraba con el proveedor ETB, se ha cambiado por un FireWall INHOUSE que se implementó. Se realiza un levantamiento del protocolo de monitoreo. El monitoreo se realiza cada 4 horas independiente de las alarmas generadas.
5	Identificación de activos de información de software y hardware

12 ACTIVIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la vigencia 2020-2024 se deben establecer las siguientes las actividades en materia de Seguridad y Privacidad de Información teniendo en cuenta el nuevo Plan de Desarrollo Distrital y el plan de la Institucional.

Se establecen en las siguientes actividades específicas la fecha inicial y final, para desarrollar las primeras versiones de los productos que no están desarrollados y las actualizaciones para las que cuanta con una previa.

Actividad	Descripción	Responsable	Producto Entregable	Indicador	Fecha Inicial	Fecha Final
Aprobar la Política de seguridad de la información.	Aprobar el documento de política de seguridad de la información del Instituto.	Área de Tecnología del Instituto Distrital de Protección y Bienestar Animal	Política de seguridad de la información Aprobada.	Documento entregado y aprobado	Sep/2020	Dic/2020
Elaborar y socializar 4 políticas específicas de seguridad de la información	Elaborar 4 de las políticas específicas, ajustarlas y socializarlas a cada uno de las dependencias del instituto.	Área de Tecnología del Instituto Distrital de Protección y Bienestar Animal	Cantidad políticas elaboradas y socializadas	Cantidad de políticas elaboradas y socializadas / 4 políticas elaboradas y socializadas	Sep/2020	Dic/2020
Definir y socializar los roles y responsabilidades frente a la seguridad de la información.	Definir cada una de las acciones y responsabilidades en el cumplimiento de las políticas de seguridad de la información	Área de Tecnología del Instituto Distrital de Protección y Bienestar Animal	Documento de roles y acciones definidas	Total de acciones y roles definidos	Oct/2020	Dic/2020
Socialización de los procedimientos de acceso y uso de contraseñas	Realizar a través de la intranet la socialización del procedimiento de acceso y uso de contraseñas a todas las dependencias.	Área de Tecnología del Instituto Distrital de Protección y Bienestar Animal	procedimiento de acceso y uso de contraseñas a todas las dependencias. aprobado	Cantidad de socializaciones realizadas del procedimiento aprobado	Oct/2020	Dic/2020
Definir el protocolo de activos de información en el cual se actualicen y etiqueten los activos de información del Instituto	Protocolo de uso y actualización de activos de información.	Área de Tecnología del Instituto Distrital de Protección y Bienestar Animal y demás dependencias del Instituto.	Documento de protocolo de uso de activos de información aprobado Base con la cantidad de activos de información actualizada	Documento entregado y aprobado. Listado de activos de información	Oct/2020	Dic/2020
Definir el marco	Se definirán las	Área de	Documento	Documento	Oct/2020	Dic/2020

Actividad	Descripción	Responsable	Producto Entregable	Indicador	Fecha Inicial	Fecha Final
de seguridad y privacidad de la información.	acciones a validar a nivel de seguridad y privacidad y de mitigación del riesgo de Seguridad de la Información, en el marco de SGSI del Instituto Distrital de Protección y Bienestar Animal.	Tecnología del Instituto Distrital de Protección y Bienestar Animal	del marco de seguridad y privacidad de la información.	entregado y aprobado		
Aplicar y mejorar la seguridad y privacidad de la información en el marco de SGSI del Instituto Distrital de Protección y Bienestar Animal.	Se realizarán las actividades para el seguimiento que permitan la evaluación de la seguridad y privacidad de la información, con el fin de realizar los ajustes adecuados.	Área de Tecnología del Instituto Distrital de Protección y Bienestar Animal	Documento de actividades de seguimiento para seguridad de la información	Documento entregado y aprobado	Oct/2020	Dic/2020
Definir los lineamientos de declaración de aplicabilidad de seguridad de la información	Contar con el documento de declaración de aplicabilidad.	Área de Tecnología del Instituto Distrital de Protección y Bienestar Animal	Documento de declaración de aplicabilidad.	Documento entregado y aprobado	Oct/2020	Dic/2020
Utilización de licencias de software para todos los equipos del Instituto	Licencias aprobadas por equipo	Área de Tecnología del Instituto Distrital de Protección y Bienestar Animal	Licencias adquiridas e instaladas aprobadas por equipo	Cantidad de Licencias adquiridas e instaladas aprobadas por equipo	Oct/2020	Dic/2020
Monitoreo de tiempos de navegación y páginas visitadas por los funcionarios	Número de visitas realizadas por jornada laboral	Área de Tecnología del Instituto Distrital de Protección y Bienestar Animal	Informe Número de visitas realizadas por jornada laboral	Número de visitas realizadas por jornada laboral	Oct/2020	Dic/2020
Uso y Manejo de Backups a las personas que accesan a la	Número de Backups realizados a todos los equipos	Área de Tecnología del Instituto Distrital de	Backups realizados a los equipos de la entidad	Numero de Backups realizados a los equipos de la	Oct/2020	Dic/2020

Actividad	Descripción	Responsable	Producto Entregable	Indicador	Fecha Inicial	Fecha Final
información del Instituto.	utilizados de acuerdo al tipo de vinculación contractual del Instituto reporte mensual.	Protección y Bienestar Animal		entidad		

13 MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Ley 1273 de 2009 “Protección de la Información y de los datos”
- Documento CONPES 3854 de abril de 2016 “Ciberseguridad y ciberdefensa. Política Nacional de Seguridad Digital”.
- Decreto 612 de 4 de abril 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 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

14 REQUISITOS TÉCNICOS

• Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
• Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías de Información y Comunicación- MINTIC

15 SITUACION ACTUAL

- El Instituto cuenta con Política de seguridad de la información adoptada mediante la Resolución 023 de 2019, la cual esta publicada en el portal institucional.
- Existe un inventario de activos de información con corte a diciembre de 2019, publicado en el portal institucional, se debe realizar la actualización de este inventario con sus respectivas tareas asociadas para su publicación el 31 de diciembre de 2020.
- Se debe continuar con el desarrollo de la implementación de políticas específicas de seguridad de la información, como inicio se entrega el documento de la política GESTIÓN DE ACTIVOS DE INFORMACIÓN para su respectiva verificación y posterior aprobación.

- Con la futura contratación para finales de septiembre de 2020, del seguridad de la información (Segurinfo), se inicia la gestión de configuración de los perfiles de roles del equipo responsable de la seguridad de la información, de esta manera contar con el equipo mínimo para desarrollar todas y cada una de las actividades asociadas a la seguridad de la información del instituto.

- Una vez se surta la contratación del Segurinfo se debe programar mesas de trabajo con el fin de adelantar todas y cada una de las actividades relacionadas con la seguridad y privacidad de la información contempladas en el punto 13 del presente plan.

- En esta fase inicial del desarrollo del Plan de Seguridad y Privacidad de la Información, se busca entender las características principales de la entidad con el fin de que los objetivos de este Plan estén alineados con los objetivos estratégicos de la entidad. Entre los aspectos que se deben considerar para lograr este entendimiento están: 1. La misión 2. La visión 3. Historia y antecedentes 4. Estructura organizacional 5. Procesos 6. Cultura y valores 7. Legislación pertinente.

- Para la realización del análisis dentro del Plan de Seguridad y Privacidad de la Información es necesario definir una serie de variables que ayuden a la priorización de los diferentes dominios de la NTC/ISO 27001:2013. Los dominios de la norma están conformados por controles. El Plan de Seguridad y Privacidad de la Información propone una estrategia para la implementación basada en una serie de variables que permiten inferir el orden de implementación de cada uno de los dominios teniendo en cuenta algunos aspectos asociados a cada uno de los controles. Por lo cual esta implementación de dominios y controles se debe establecer en las mesas técnicas asociadas a la Seguridad y Privacidad de la Información.

- El presente plan se presenta para lo que resta del año 2020 y 2021 con sus respectivas actualizaciones, cabe aclarar que se debe fortalecer y estructurar un plan más robusto que abarque el cuatrienio 2020-2023.

16 RESPONSABLE DEL DOCUMENTO

Área de Tecnología/ Subdirección de Gestión Corporativa