TABLA CONTENIDO

DERECHOS DE AUTOR 2
CONTEXTUALIZACIÓN 2
INTRODUCCIÓN 3
OBJETIVO 3
OBJETIVOS ESPECÍFICOS 3
ALCANCE 4
TERMINOLOGÍA ..... **¡Error! Marcador no definido.**
ESTRATEGIA 7
ACTIVIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 13
POLÍTICAS 8
SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 9
Seguridad de la Información: 9
Procedimientos: 9
Protección De Datos Personales: 9
Gestión De Riesgos: 9
ALCANCE DEL SISTEMA DE SEGURIDAD DE INFORMACIÓN 10
GRUPO DE SEGUIMIENTO A TECNOLOGÍAS DE LA INFORMACIÓN 17
LAS FUNCIONES DEL GRUPO DE SEGUIMIENTO A TECNOLOGÍAS DE LA INFORMACIÓN PARA EL TEMA DE SEGURIDAD DE LA INFORMACIÓN SON: ... **¡Error! Marcador no definido.**
RESPONSABLE DEL DOCUMENTO. ..... **¡Error! Marcador no definido.**

DERECHOS DE AUTOR

A menos que se indique de forma contraria, el copyright (traducido literalmente como derecho de copia y que, por lo general, comprende la parte patrimonial de los derechos de autor) del texto incluido en este documento es del Instituto Distrital de Protección Animal Bogotá. Se puede reproducir gratuitamente en cualquier formato o medio sin requerir un permiso expreso para ello, bajo las siguientes condiciones:

- *El texto particular no se ha indicado como excluido y por lo tanto no puede ser copiado o distribuido.*
- *La copia no se hace con el fin de ser distribuida comercialmente.*
- *Los materiales se deben reproducir exactamente y no se deben utilizar en un contexto engañoso.*
- *Las copias serán acompañadas por las palabras "copiado/distribuido con permiso de la República de Colombia. Todos los derechos reservados".*
- *El título del documento debe ser incluido al ser reproducido como parte de otra publicación o servicio.*

Si se desea copiar o distribuir el documento con otros propósitos, debe solicitar el permiso entrando en contacto con el del Instituto Distrital de Protección Animal Bogotá para obtener la autorización.

CONTEXTUALIZACIÓN

Con el ánimo de asegurar la integridad, disponibilidad, confidencialidad y privacidad de la información de sus procesos, el Instituto Distrital de Protección y Bienestar Animal, está en el proceso de transformación e implementación del Plan de Seguridad y Privacidad de la información (MSPI), así como el Sistema de Gestión y Seguridad de la Información (SGSI), 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 los sistemas y la información que usan.

INTRODUCCIÓN

El Instituto Distrital de Protección y Bienestar Animal, reconoce la importancia y el valor de la información con respecto al funcionamiento eficiente y efectivo de la institución, entendiendo que la información no es sólo crítica para el éxito de la organización, sino estratégica para su supervivencia a largo plazo, por esta razón, se establece el siguiente plan que regula el manejo de la información en el IDPYBA, orientada a definir las medidas que resguarden la confidencialidad, integridad y disponibilidad de la información propia del Instituto Distrital de Protección y Bienestar Animal el acceso a la información en conformidad con la norma ISO 27001: 2013.

Es por ello que se desea implantar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI) que permita lograr niveles adecuados de seguridad para todos los activos de información institucional considerados relevantes, de manera tal de 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.

1. 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 sean identificados, valorados y administrados de una 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. OBJETIVOS ESPECÍFICOS

- Establecer para todo el personal del IDPYBA la necesidad de la seguridad de la información y promover la comprensión de sus responsabilidades individuales, mediante campañas de sensibilización sobre el manejo de la misma.

- Determinar frente al 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.

- Crear un modelo organizacional de seguridad de la información, definiendo los roles y responsabilidades de los participantes.
- 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.
- Cumplir con los requisitos legales vigentes aplicables a la naturaleza de la Entidad en materia de Seguridad de la Información.
- 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, como lo siguiere 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, el entorno y la tecnología.
- Contar con la política de seguridad y privacidad de la información actualizada, con el fin de asegurar su vigencia y eficacia.
- Formular e implementar controles y acciones que signifiquen una adecuada prevención y administración del riesgo.

3. ALCANCE

El plan general de seguridad de la información aplica a todos los funcionarios, contratistas y terceros del Instituto Distrital de Protección y Bienestar Animal. De igual manera aplica a todos los procesos de la entidad bajo el marco de gestión establecido en el Modelo Integrado de Planeación y Gestión –MIPG.

Así también tendrá como apoyo la política de seguridad y privacidad de la información, cada dominio especificado por el estándar ISO 27001: 2013 tendrá una política específica, que complementará la presente y normará las

particularidades de cada dominio. Cada Política deberá contar con procedimientos asociados, mecanismos de control de esta.

4. GLOSARIO DE TÉRMINOS Y DEFINICIONES

- **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 organización1.
- **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.
- **Aceptación de riesgo**: Decisión de asumir un riesgo.
- **Adaptabilidad**: Define los eventos y bajo qué criterios un sistema debe poder ser monitoreado y revisado para su control posterior.
- **Amenazas:** 1Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.
- **Análisis de Riesgo**: 2Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo aceptable.
- **Auditoria:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria.
- **Autenticidad:** Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidad.
- **Cifrado:** es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información. Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo aceptable al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

- **Confiabilidad de la Información:** Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Las políticas:** los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo aceptado.
- **Control:** Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. Declaración de aplicabilidad: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo particular
- **Custodio del activo de información**: Es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados. Derechos de Autor: es un conjunto.
- **Dato personal:** Es cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Dato público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **Datos sensibles**: Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.
- **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**: 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.

5. ESTRATEGIA

Los activos de información del Instituto Distrital de Protección y Bienestar Animal deben ser identificados y clasificados de acuerdo con 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.

Estos activos se pueden categorizar según la siguiente clasificación:

Confidencia: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado.

Privada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos

Pública: Información conocida y utilizada por cualquier persona., que un sujeto obligado genere, obtenga, adquiera, o controle.

Con el fin de propender por una cultura sólida en seguridad y privacidad de la información, el Instituto Distrital de Protección y Bienestar Animal definirá y ejecutará periódicamente programas de sensibilización y capacitación en seguridad de la información de acuerdo con las necesidades identificadas.

6. POLÍTICAS

EI instituto Distrital de Protección y Bienestar Animal establece una política general la cual se diseña desde la Subdirección de Gestión Corporativa, área encargada de la seguridad de la información TIC y varias políticas generales en cumplimiento con el MSPI, teniendo en cuenta los siguientes criterios:

- Creación de políticas

EI instituto Distrital de Protección y Bienestar Animal 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.

- Aprobación de políticas

EI instituto Distrital de Protección y Bienestar Animal, 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 del área encargada de 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 a la 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 del 100% de la política.

Participar en las auditorias internas y externas de la norma ISO 27001:2013

7. 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. (IDPYBA), 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.

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 la 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.

8. ALCANCE DE LA ESTRATEGIA DE SEGURIDAD DE INFORMACIÓN.

Los contenidos del presenta 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 la declaración de aplicabilidad avalada por el Comité Institucional de Gestión y Desempeño

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 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 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 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 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 bloqueo de sesión, escritorio y pantalla limpia
- Política de acceso de red a terceros.
- Política de gestión de medios removibles.
- Política de uso de cuentas para acceso de recursos tecnológicos

9. ACTIVIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la vigencia 2021 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	**Actividades**	**Tareas**	**Responsable de la Tarea**	**Fechas Programación Tareas**	
				Fecha	**Fecha**
Activos de información	Definir lineamientos para el levantamiento de activos de información	Elaboración metodología e instrumento de levantamiento de activos de información	Profesional del Área de tecnología	3-may-21	31-may-21
	Levantamiento Activos de Información	Validar activos de información en el instrumento levantado en la vigencia anterior	Responsable de cada proceso, Profesional del Área de tecnología.	7-jun-21	18-jun-21
		Identificar nuevos activos de información en cada dependencia	Responsable de cada proceso, Profesional del Área de tecnología	18-jun-21	25-jun-21
		Realizar informe de actualización a los activos de información, cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados.	Profesional del Área de tecnología	26-jul-21	31-dic-31
		Consolidar el instrumento de activos de Información.	Profesional del Área de tecnología	1-sept-21	10-sept-21

		Publicar los instrumentos de activos de información consolidado en el sitio web de la entidad	Profesional del Área de tecnología	10-sept-21	30-sept-21
Política Seguridad y privacidad de la Información	crear procedimiento de incidentes de seguridad de la información	Publicar la política de seguridad de la información en el sitio web de la entidad.	Profesional del Área de tecnología	01-feb-21	20-feb-21
		Socializar los procedimientos asociados a la política de seguridad y privacidad de la información.	Profesional del Área de tecnología.	01-feb-21	30-abr-21
		Crear documento borrador de procedimiento de incidentes de seguridad de la información y enviarlo a revisión al área encargada.	Profesional del Área de tecnología. Área de planeación	10-abril-21	14-jun-21
		Aplicar correcciones al procedimiento según el área encargada, y enviar nuevamente para su	Profesional del Área de tecnología. Área de	17-jun-21	30-jun-21
		Socializar el procedimiento a los colabores de la entidad.	Profesional del Área de tecnología.	1-jul-21	30-dic-21
Auditorías Internas y Externas	Participación en las auditorías internas y externas de la norma ISO 27001:2013	Participar en las auditorías internas y externas de la norma ISO 27001:2013 programadas.	Todos los procesos del área de tecnología	1-oct-21	31-dic-21

Sensibilización sobre la protección de la información	Creación de plan de capacitaciones sobre tomar conciencia en la importancia de la seguridad de la información.	Programar jornada de capacitaciones en las diferentes áreas de la entidad.	Todas las áreas de la entidad	01-feb-21	30-nov-21
		Dar tips sobre la protección mediante correos electrónicos y/o Wallpaper en los equipos de la entidad.	Todas las áreas de la entidad	01-feb-21	31-dic-21
Creación de nuevas políticas complementarias y/o actualización	Revisar las políticas actuales del área TIC	Verificar si es necesario realizar ajustes y/o actualizaciones a las políticas ya creadas en la entidad.	Todos los procesos del área de tecnología	01-abr-21	20-nov-21
	Creación de política de gestión de incidentes de seguridad de la información.	Crear documento borrador de Política de incidentes de seguridad de la información y enviarlo a revisión al área encargada.	Profesional del Área de tecnología. Área de planeación	01-may-21	30-jun-21
		Aplicar correcciones a la según el área encargada, y enviar nuevamente para su aprobación por el área encargada.	Profesional del Área de tecnología. Área de planeación	15-jul-21	15-agos-21
		Exponer en comité de gestión la creación e implementación de la política, para su aprobación	Comité de gestión	01-oct-21	31-oct-21
		Socialización y publicación de la política de gestión de incidentes de seguridad de la información en el sitio web de la entidad.	Profesional del Área de tecnología.	15-Nov-21	30-Nov-21

	Creación de política de protección contra software malicioso	Crear documento borrador de política de protección contra software malicioso y enviarlo a revisión al área encargada.	Profesional del Área de tecnología. Área de planeación	01-may-21	30-jun-21
		Aplicar correcciones a la según el área encargada, y enviar nuevamente para su aprobación por el área encargada.	Profesional del Área de tecnología. Área de planeación	15-jul-21	15-agos-21
		Exponer en comité de gestión la creación e implementación de la política, para su aprobación	Comité de gestión	01-oct-21	31-oct-21
		Socialización y publicación de la política de protección contra software malicioso en el sitio web de la entidad.	Profesional del Área de tecnología.	15-Nov-21	30-Nov-21
	Creación de política de acceso a la red por terceros.	Crear documento borrador de política de acceso a la red por terceros y enviarlo a revisión al área encargada.	Profesional del Área de tecnología. Área de planeación	01-may-21	30-jun-21
		Aplicar correcciones a la según el área encargada, y enviar nuevamente para su aprobación por el área encargada.	Profesional del Área de tecnología. Área de planeación	15-jul-21	15-agos-21
		Exponer en comité de gestión la creación e implementación de la política, para su aprobación	Comité de gestión	01-oct-21	31-oct-21

		Socialización y publicación de política de acceso a la red por terceros en el sitio web de la entidad.	Profesional del Área de tecnología.	15-Nov-21	30-Nov-21

10. GRUPO DE SEGUIMIENTO A TECNOLOGÍAS DE LA INFORMACIÓN

El grupo de seguimiento a tecnologías de la información, se organizará dentro del área de tecnologías y se presentará para su creación formal en el Instituto Distrital de Protección y Bienestar Animal, y se plantea que tendrá dentro de sus funciones la de impulsar, hacer seguimiento y/o verificación de las actividades en materia de seguridad y privacidad de la información, que en conjunto con el Comité Institucional de Gestión y Desempeño harán seguimiento al cumplimiento de este plan, junto con los demás planes que sean implementados en pro de proteger la privacidad de la información.

En conjunto con el anterior, la mesa de tecnologías de información se entenderá 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.