CONTROL DE CAMBIOS

No. DE ACTA DE APROBACIÓN	FECHA	VERSIÓN	DESCRIPCIÓN
063-	10 ABR. 2019	1.0	ADOPCIÓN DEL PLAN

AUTORIZACIONES

ELABORÓ:	REVISÓ	APROBÓ
ÁREA TÉCNICA	OFICINA ASESORA DE PLANEACIÓN	LÍDER DEL PROCESO
Nombre Juan Carlos Sanabria	**Nombre**: Diana María Mora Ramírez Yovanny Arias Guarín	**Nombre**: Jonathan Ramírez Nieves
Firma:	**Firma:**	**Firma:**
Cargo: Contratista Subdirección Gestión Corporativa	**Cargo**: Profesional Especializado Oficina Asesora de Planeación Contratista Profesional OAP	**Cargo**: Subdirector de Gestión Corporativa (E)

TABLA DE CONTENIDO

1. 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 continuo del Sistema de Gestión de Seguridad de la Información – SGSI del Instituto Distrital de Protección y Bienestar Animal. Promoviendo que el Instituto cuente con:

- Protección de 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.
- 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.

2. ALCANCE

El alcance del presente documento define los lineamientos, controles y directrices definidos en la política de seguridad de la información del Instituto. Buscando que la política establecida y las actualizaciones que se realicen apliquen al uso eficiente de los activos de información y a las partes interesadas del Instituto.

3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Instituto Distrital de Protección y Bienestar Animal, 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.

4. 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).

5. 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 debe desarrollar la implementación de políticas especificas de seguridad de la información dentro de las cuales se mencionan las siguientes:

- 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.
- Política de separación de ambientes.
- Política de gestión de registros (logs)
- Política de sensibilización, formación y toma de conciencia en seguridad de la información.
- Política de bloqueo de sesión, escritorio y pantalla limpia.
- Política de documentación de procedimientos operativos.
- Política de control de versiones.
- Política de seguridad de la información
- Política de uso de cuentas para acceso a recursos tecnológicos.
- Política de acceso a la red por terceros.
- Política de gestión de medios removibles.
- en la continuidad del negocio.
- Política de derechos de propiedad intelectual.
- Política de sanciones previstas por incumplimiento.

- Política de seguridad física y ambiental.
- Política de administración y control de usuarios al datacenter.
- Política de trabajo en áreas protegidas
- Política de seguridad y mantenimiento de los equipos.
- Política de seguridad de los equipos fuera de las instalaciones.
- Política de acuerdos de confidencialidad.
- Política de uso de dispositivos móviles y teletrabajo.
- Política de protección contra software malicioso.
- Política de administración de backups, recuperación y restauración de la información.
- Política de controles criptográficos.
- Política de gestión de vulnerabilidades técnicas.
- Política de administración de componentes electrónicos de procesamiento de información
- Política de adquisición de Hardware.
- Política de adquisición de software.
- Política de gestión de incidentes de seguridad de la información.
- Política de tratamiento de datos personales.

En una tercera fase se debe 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.

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.

6. 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 este 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.

7. 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 la gestión por valores del Modelo Integrado de Planeación y Gestión - 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

7. 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

8. ACTIVIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la vigencia 2019 se establecen las siguientes actividades en materia de Seguridad y Privacidad de Información, las cuales se encuentran enmarcadas en la Meta 4 del Plan de Acción del Área de Tecnología:

Actividad	Descripción	Responsable	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	Febrero 2019	Febrero 2019
Elaborar y socializar las políticas específicas de seguridad de la información	Elaborar cada una 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	Febrero 2019	Marzo de 2019
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	Marzo 2019	Marzo 2019
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	Marzo 2019	Marzo 2019
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.	Marzo 2019	Marzo 2019
Definir el marco de seguridad y privacidad de la información.	Se definirán las 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.	Área de Tecnología del Instituto Distrital de Protección y Bienestar Animal	01/02/2019	30/06/2019
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	01/02/2019	30/06/2019
Definir los lineamientos de	Contar con el documento de declaración de aplicabilidad.	Área de Tecnología del Instituto Distrital	01/02/2019	31/08/2019

declaración de aplicabilidad de seguridad de la información		de Protección y Bienestar Animal		
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	1/03/2019	30/04/2019
Monitoreo de tiempos de navegación y páginas visitadas por los funcionarios	Número de Backups realizados a todos los equipos utilizados de acuerdo al tipo de vinculación contractual del Instituto reporte mensual.	Área de Tecnología del Instituto Distrital de Protección y Bienestar Animal	1/01/2019	31/12/2019
Uso y Manejo de Backups a las personas que accesan a la información del Instituto.	Número de Backups realizados a todos los equipos utilizados de acuerdo al tipo de vinculación contractual del Instituto reporte mensual.	Área de Tecnología del Instituto Distrital de Protección y Bienestar Animal	1/01/2019	31/12/2019
Elaborar y socializar las 25 políticas especificas de seguridad de la información.	Elaborar cada una de las 25 políticas específicas, ajustarlas y socializarlas a cada uno de las dependencias del Instituto, en cada trimestre presentando 6 y el último trimestre 7.	Área de Tecnología del Instituto Distrital de Protección y Bienestar Animal	1/01/2019	31/12/2019
Actualizar los activos de información por cada dependencia del Instituto.	Número de dependencias con los activos de información actualizados.	Área de Tecnología del Instituto Distrital de Protección y Bienestar Animal	1/03/2019	30/04/2019

9. 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.

10. 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

11.RESPONSABLE DEL DOCUMENTO

Área de Tecnología/ Subdirección de Gestión Corporativa
Gestión de la Información / Subdirección de Gestión del Conocimiento y Participación Ciudadana.