CONTROL DE CAMBIOS

No. DE ACTA DE APROBACIÓN	FECHA	VERSIÓN	DESCRIPCIÓN
		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 Francisco 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. INTRODUCCIÓN

Para comenzar, las diferentes empresas encausadas en la denominada revolución tecnológica y parte de la era digital, reconocen el protagonismo de la información en sus procesos productivos, por tanto la importancia de contar con una información adecuadamente identificada y protegida, como también la que es proporcionada a sus partes interesadas en el sector público distrital mencionamos al ciudadano, colectivos organizados, entre otros grupos de interés con los que el Instituto de Protección y Bienestar Animal enmarca las relaciones de cumplimiento, compromiso y contractuales como lo son los acuerdos de confidencialidad y demás compromisos, que obligan a dar tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia de los sistemas de información del Instituto.

La seguridad de la información en las entidades distritales tiene como objetivo la protección de los activos de información, en cualquiera de sus estados ante las diferentes amenazas, riesgos y brechas que se atentan contra los principios fundamentales de confidencialidad, integridad y la disponibilidad, buscando la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesto el Instituto y se logre alcanzar el máximo cumplimiento de las metas y objetivos de los proyectos que dan cuenta de las tareas del Plan de Desarrollo de Bogotá.

El Instituto de Protección y Bienestar Animal, decide vincular el modelo de administración de riesgos de seguridad de la información y las actividades de valoración de los riesgos expuestos en cumplimiento de una política de seguridad de la información aprobada por la Dirección, y como medio o herramienta para conseguir el logro de los objetivos de mantener una información con carácter confidencial, integra, disponible, a través de un ciclo de vida de los sistemas de información que inicia desde su captura, almacenamiento, explotación y eliminación.

Los principios de protección de la información se describen en:

- ✓ Confidencialidad, entendida como la propiedad que la información sea concedida únicamente a quien esté autorizado.
- ✓ Integridad, entendida como la propiedad que la información se mantenga exacta y completa.
- ✓ Disponibilidad, entendida como la propiedad que la información sea accesible y utilizable en el momento que se requiera.

2. OBJETIVO

Describir las actividades que detallan el plan de tratamiento de riesgos de seguridad y privacidad de la información que hace parte del Sistema de Gestión de Seguridad de la Información – SGSI del Instituto Distrital de Protección y Bienestar Animal; de tal forma que se definen y aplican los controles con los cuales se buscan mitigar la materialización de los riesgos de seguridad de la información. De

esta manera lograr mediante el tratamiento de los riesgos y el mejoramiento continuo de la Seguridad y Privacidad de la Información, las aportantes tengan mayor confianza en el tratamiento de la información que se gestiona y almacena en el Instituto.

Se debe mencionar que los objetivos específicos para el Instituto son:

- Brindar lineamientos y principios que busquen unificar los criterios para la administración de riesgos de seguridad de la información.
- Fortalecer el sistema de gestión de riesgos del Instituto incorporando controles y medidas de seguridad de la información acordes con el entorno de gestión del Instituto.
- Proteger el valor de los activos de información mediante el control de implementación de acciones de mitigación frente al riesgo y potencializar las oportunidades asociadas.
- Generar una cultura y apropiación del trabajo enfocada en la identificación de los riesgos de seguridad de la información y su mitigación.

3. TERMINOS Y DEFINICIONES

Seguidamente, se listan algunos términos y definiciones que se utilizaran durante el desarrollo de la gestión de riesgos de seguridad de la información en beneficio de unificar los criterios dentro del Instituto:

- ✓ *Administración del riesgo*, entendido como el conjunto de elementos de control que al relacionarse brindan al Instituto la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.
- ✓ *Activo de Información,* En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.
- ✓ *Análisis de riesgos,* Definido como un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.
- ✓ *Amenaza,* definida como la causa potencial de una situación de un incidente y no deseada por la organización.
- ✓ *Causa,* Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentas generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales, entre otros.
- ✓ *Confidencialidad,* Entendida como la propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- ✓ *Consecuencia,* Es el resultado de un evento que afecta los objetivos.
- ✓ *Criterios del riesgo,* Definidos como los términos de referencia frente a los cuales la importancia de un riesgo es evaluada.
- ✓ *Control,* Es la medida que modifica el riesgo.
- ✓ *Disponibilidad,* Es la propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- ✓ *Evaluación de riesgos,* Es el proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- ✓ *Evento,* Es un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
- ✓ *Estimación del riesgo,* Es el proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
- ✓ *Evitación del riesgo,* Es la decisión de no involucrarse en una situación de riesgo o tomar una acción para retirarse de dicha situación.
- ✓ *Factores de riesgo,* Son las situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o atienden a aumentar la exposición, pueden ser internos o externos al Instituto.
- ✓ *Gestión del Riesgo,* Son las actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se componen de la evaluación y el tratamiento de riesgos.
- ✓ *Identificación del Riesgo,* Entendido como el proceso para encontrar, enumerar y caracterizar los elementos del riesgo.
- ✓ *Incidente de seguridad de la Información,* Es el evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (confidencialidad, integridad y disponibilidad)
- ✓ *Integridad,* Es la propiedad de la información relativa a su exactitud y completitud.
- ✓ *Impacto,* Entendido como el cambio adverso en el nivel de los objetivos del negocio logrados.
- ✓ *Nivel de riesgo,* Es la magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.
- ✓ *Matriz de riesgos,* Es el instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.
- ✓ *Monitoreo,* Es la mesa de trabajo que se realiza trimestral, semestral o anual, la cual tiene como finalidad, revisar, actualizar, o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorias de los sistemas de gestión.
- ✓ *Propietario del riesgo,* Es la persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
- ✓ *Proceso,* Es el conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.
- ✓ *Riesgo inherente,* Es el denominado nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
- ✓ *Riesgo residual,* Es el riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar controles.
- ✓ *Riesgo,* Efecto de la incertidumbre sobre los objetivos.
- ✓ *Riesgo en la Seguridad de la Información,* Entendido como el riesgo potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño al Instituto.
- ✓ *Reducción del riesgo,* Son las acciones que se toman para disminuir la probabilidad de las consecuencias negativas, o ambas, asociadas con un riesgo.

- ✓ *Retención del riesgo,* Es la aceptación de la perdida o ganancia proveniente de un riesgo particular.
- ✓ *Seguimiento,* Son las mesas de trabajo, en las cuales se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación de los controles de seguridad de la información sobre cada uno de los procesos.
- ✓ *Tratamiento del riesgo,* Es el proceso para modificar el riesgo.
- ✓ *Valoración del riesgo,* Es el proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.
- ✓ *Vulnerabilidad,* Entendida como aquella debilidad de un activo o grupo de activos de información.
- ✓ *Seguridad de la Información,* Entendida como la preservación de la confidencialidad, integridad y disponibilidad de la información.

4. ALCANCE

El alcance del plan de plan de tratamiento de riesgos de seguridad y privacidad de la información se aplica a los procesos del Instituto Distrital de Protección y Bienestar Animal, a cualquier sistema de información o aspecto de control del Instituto a través de los principios básicos y metodológicos para la administración del riesgo de acuerdo al alcance del Sistema de Gestión de Seguridad de la Información, donde se toman como opciones de tratamiento o manejo de riesgos según la zonas de riesgo en la cual se incluyan las pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

5. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para el contexto de la gestión de riesgos de seguridad de la información se definen los criterios básicos en las normas NTC-ISO/IEC 27005 y la NTC-ISO 31000. Dentro de las que se identifican os riesgos por parte del Instituto de Protección y Bienestar Animal y obtener los resultado esperados, basándose en la identificación de las fuentes que puedan dar origen a los riesgos y oportunidades en los procesos del Instituto, en el análisis de las debilidades y amenazas asociadas, en la valoración de los riesgos en términos de sus consecuencias para el instituto y en la probabilidad de que estos ocurran, al igual que en la construcción de acciones de mitigación en beneficio de lograr y mantener los niveles de riesgos controlados y aceptables por parte del Instituto.

5.1 PLANES DESARROLLADOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En la vigencia 2018 como primera tarea se adelantó el autodiagnóstico del componente de seguridad de la información y se definieron varias actividades dentro de las que se incluye la formulación del Plan de seguridad de la información y posteriormente se delimita el plan de tratamiento de riesgos.

Adicionalmente, se realizó la revisión y documentación de la Matriz de riesgos de seguridad de la información versus los controles que se deben atender desde el instituto; de tal forma que se definen

nuevos riesgos de seguridad de la información y se asocian a los existentes, la relación de los controles aplicados versus los controles de la Norma ISO 27001:2013, se aplica a cada uno de ellos para evitar la materialización de estos. Una vez realizado se aplicó la metodología de administración de riesgos del Departamento Administrativo de Función Pública.

5.2 RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se visualizan los riesgos de Seguridad de la Información, los cuales están asociados al Sistema de Gestión de Seguridad de la Información – SGSI del Instituto Distrital de Protección y Bienestar Animal, los cuales fueron evaluados sobre la vigencia de 2018.

No	Riesgo	Estado	Responsable	¿Materializado?
1	Inadecuada Gestión de la infraestructura tecnológica y de comunicaciones	Gestionado	Área de Tecnología	No
2	Manipulación no autorizada de la información registrada en los sistemas del Instituto	Gestionado	Área de Tecnología	No
3	Incumplimiento con el Modelo de Seguridad y Privacidad de la Información de las Políticas Gobierno Digital	Gestionado	Área de Tecnología	No

De acuerdo a la evaluación de los riesgos de seguridad presentados se explica que el Instituto para el año 2017 inicio sus actividades, en cuanto al tema tecnológico contrata sus servicios a través de un tercero el cual soporta la parte tecnológica de integración. Para el año 2018 se iniciaron las labores de consolidación de los sistemas tecnológicos y los sistemas de información, se levantaron activos de información de software y hardware y se realizaron los procedimientos de controles y mesa de servicios del Instituto.

Una vez definidos los riesgos se observa que se consideran los siguientes aspectos de impacto al formular los riesgos: Niveles de clasificación de los activos de información impactados, brechas en la seguridad de la información (perdida de la confidencialidad, integridad y disponibilidad), operaciones deterioradas (afectación a partes internas o terceras partes), incumplimiento de los requisitos legales, reglamentación o contractuales.

3.3 ACTIVIDADES PARA DESARROLLAR SOBRE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Para adelantar las actividades es necesario mencionar que hay tres fases claves en el tratamiento de riesgos y fueron definidos con cada una de sus fases:

Fase de Planificación: Dentro de esta fase se describe las actividades propias del relacionamiento de las actividades de implementación del Plan de seguridad de Información y los riesgos posiblemente se presenten.

Fase de Tratamiento de los riesgos de seguridad de la información: En esta fase el Instituto una vez identificados los riesgos en la implementación del plan de seguridad de la información aplicado a los procesos del Instituto, revisando primordialmente los procesos responsables como son el proceso de Gestión tecnológica, y los procesos que tengan relacionamiento con los sistemas de información misionales del instituto.

Fase de socialización: en la cual se presenta conjuntamente a los grupos de interés del Instituto y se define una propuesta de seguridad de la información para incluir en el manejo y tratamiento de los riesgos.

Seguidamente, presentamos el tratamiento de riesgos realizados durante la vigencia del año 2018.

RIESGO	CAUSAS	EFECTO O CONSECUENCIA	CONTROL IDENTIFICADO	ACCIONES	RESPONSABLE
Inadecuada Gestión de la infraestructura tecnológica y de comunicaciones	Desconocimiento normativo vigente sobre plataforma tecnologica y comunicaciones.	incumplimiento de la misionalidad del instituto	Mesas de trabajo cada 3 meses para verificar el cumplimiento de la normatividad vigente	Capacitación en seguridad y privacidad de la información.	Area Tecnologia
	Fallas en la conectividad de los sistemas de información tanto interno como externo.	Perdida de la imagen institucional	socializacion de los lineamientos al interior del Instituto	Definir e implementar acciones de seguimiento al cumplimiento normativo.	Area Tecnologia
	Fallas en la conectvidad, página Web, PBX, correo electronico	Posibles investigaciones y sanciones.	Seguimiento al cumplimiento del PETIC.	Difundir los avances en el PETIC a las áreas competentes.	Area Tecnologia
Manipulación no autorizada de la información registrada en los sistemas del Instituto	Falta de controles para el acceso a los sistemas de que dispone la entidad.	Posible perdida de informacion	A cada funcionario o contratista de la Entidad se le asigna un usuario de red, así mismo el ingreso por parte de los usuarios a los aplicativos institucionales se encuentra supeditada al suministro de clave de acceso a los mismos con las restricciones pertinentes	Por solicitud mediante correo electrónico del jefe de área o la persona responsable, se solicita a la mesa de servicios informaticos, la creacionde usuarios de red para los nuevos funcionarios y/o contratistas	Area Tecnologia
	Falta de chequeo permanente a los permisos para el acceso a los sistemas de información.	Usuarios no tengan el perfil debidamente configurado a su funcion	Aplicación de firewall PF Sense, un servicio de IDS/IPS para brindar control de conexiones no autorizadas y así brindar protección perimetral y al interior de la red	Con el apoyo de la herramienta PF Sense se ha realizado monitoreo constante a la red del IDPYBA, existe identificacion de incidencias presentadas en el flujo de la red	Area Tecnologia
	Ineficacia de los mecanismos de seguridad informática implementados para impedir ataques y vulneraciones tanto de origen externo como interno.	Posibles ataque a la seguridad informatica del Instituto.	Generación de backups a la información primordial de la Entidad	Se han realizado backups a la información institucional relevante, se cuenta con servicio de backup en la nube.	Area Tecnologia
Incumplimiento con el Modelo de Seguridad y Privacidad de la Información de las Políticas Gobierno Digital	Falta de controles a los elementos informáticos de la infraestructura tecnológica del Instituto.	Fallas en la seguridad y privacidad de la información que es manejada por el Instituto.	Se tienen controles de seguridad perimetral y detección de intrusos asociados a la infraestructura tecnológica.	Se tiene controlada la actividad de la infraestrurara tecnologica	Area Tecnologia
	No se tienen los suficientes elementos tecnológicos en Hardware y Software para control de la seguridad informática del Instituto	Posible ataque externo e internos a la infraestructura informática del Instituto.	Incluir en los proyectos nuevos del PETI las necesidades de hardware y software requeridas para que sean tenidas en cuenta en la Planeación Estrategita Institucional.	Se realiza la implementación de un IDS/IPS para mantener un control de afectaciones tecnológicas.	Area Tecnologia
	Desconociemiento de la normatividad de seguridad y privacidad de la información	Posibles investigaciones y sanciones.	Mesas de trabajo mensual para verificar el cumplimiento del MSPI y los avances y oportunidades de mejoramiento.	Se realiza el levantamiento del estado actual del Instituto en temas de MSPI	Area Tecnologia

5.3 MONITOREO A CONTROLES DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Se programa el monitoreo de los controles definidos en cada uno de los riesgos de seguridad y privacidad de la Información para finales del 2018, el cual es realizado trimestralmente.

Hay que explicar que el Instituto de Protección y Bienestar Animal dentro del Plan Operativo Anual de gestión para el 2019, incluye la actividad de elaborar una actualización de los mapas de riesgos del Instituto acorde con la nueva metodología presentada por el Departamento Administrativo de Función Pública DAFP en el marco del Modelo Integrado de Planeación y Gestión MIPG, actividades que se encuentran contenidas en el siguiente cuadro de actividades:

CUADRO DE ACTIVIDADES PLAN TRATAMIENTO 2019

Actividad	Descripción	Responsable	Fecha Inicial Planificada	Fecha Final Planificada
Primera fase de planificación: valoración del riesgo seguridad de la información actualizada con la nueva metodología de administración de riesgos.	Valorar los riesgos del sistema de seguridad de la información	Área de Tecnología – revisar conjuntamente con el área de planeación las fechas de programación.	01/03/2019	01/04/2019
Definir el número de Backups realizados por cada dependencia evitando la perdida de información	Evitar el hurto, perdida o fuga de información pública, reservada o clasificada en la gestión de la plataforma.	Área de Tecnología	1/01/2019	31/12/2019
Definir los controles y las vulnerabilidades del sistema de información.	Controles y Analisis de vulnerabilidades definido	Área de Tecnología	01/03/2019	01/04/2019
Segunda Fase de tratamiento: definir los tratamientos y objetivos de seguimiento para los planes de manejo.	Planes de manejo del riesgo	Área de Tecnología	01/04/2019	30/04/2019
Definir la declaración de aplicabilidad.	Declaración de aplicabilidad a los procedimientos que manejan sistemas de información.	Área de Tecnología	01/05/2019	15/05/2019
Realizar Seguimiento al tratamiento de riesgos	Seguimiento al Cronograma de tratamiento y valoración de riesgos. (trimestralmente)	Área de Tecnología	01/08/2019	30/12/2019

Diseñar actividades por dependencia para definir el plan de continuidad de negocio del instituto.	Contar con el acceso continuo de la información permitiendo mantener, confidencialidad, integridad y disponibilidad de los activos de información por cada dependencia.	Área de Tecnología	1/03/2019	30/04/2019

6. 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.

7. 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, Mintic.

8. RESPONSABLE DEL DOCUMENTO

Área de Tecnología/ Subdirección de Gestión Corporativa.