PLAN DE TRATAMIENTOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020

INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL – IDPYBA
Subdirección de gestión corporativa

Bogotá Enero 2020

TABLA DE CONTENIDO

1. 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.

2. 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.

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

Para el marco del Modelo de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información –SGSI del Instituto Distrital de Protección y Bienestar Animal, se desea prevenir los efectos no deseados que se puedan llegar a presentar en el ámbito de la seguridad de la información, dado lo anterior de debe controlar y establecer los riesgos de la seguridad de información. De tal manera se pueda garantizar el tratamiento de los riesgos de seguridad de información y gestión de riesgo.

3.1 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.

3.2 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

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

3.3 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 2020, 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 2020

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 – revisión conjunta con el área de planeación las fechas de programación.	01/03/2020	01/06/2020
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	1/01/2020	31/12/2020
Definir los controles y las vulnerabilidades del sistema de información.	Controles y Analisis de vulnerabilidades definido	Área de Tecnología	01/03/2020	01/06/2020
Segunda Fase de tratamiento: definir los tratamientos y objetivos de seguimiento para los planes de manejo.	Planes de manejo del riesgo	Área de Tecnología	01/04/2020	01/06/2020
Definir la declaración de aplicabilidad.	Declaración de aplicabilidad a los procedimientos que manejan sistemas de información.	Área de Tecnología	01/05/2020	01/06/2020
Realizar Seguimiento al tratamiento de riesgos	Seguimiento al Cronograma de tratamiento y valoración de riesgos.	Área de Tecnología	01/08/2020	31/12/2020

	(trimestralmente)			
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	1/03/2020	01/06/2020

4. 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.

5. 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.

6. RESPONSABLE DEL DOCUMENTO

Área de Tecnología/ Subdirección de Gestión Corporativa.

NELSON JAVIER GOMEZ MALAVER
Director General
Instituto Distrital de Protección y Bienestar Animal

Elaboro: Christian Angulo – Contratista-SGC
Reviso: EDGAR ARTURO PINTOR PELÁEZ- Subdirector de Gestión Corporativa

Nota: este documento es susceptible a cambio de acuerdo con la aprobación del comité de gestión de desempeño.