PLAN DE TRATAMIENTO DE DATOS DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2022

INSTITUTO DE PROTECCIÓN Y BIENESTAR ANIMAL DE CUNDINAMARCA – IPYBAC.

ELIANA MARGARITA RAMÌREZ ARENAS

GERENTE GENERAL

SUBGERENCIA DE ASUNTOS ADMINISTRATIVOS
2022

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 de Protección y Bienestar Animal de Cundinamarca - IPYBAC, mediante el cual se definen los controles que permiten mitigar la materialización de los riesgos de seguridad de la información en el IPYBAC.

2 ALCANCE

El Plan de tratamiento de riesgos tiene alcance para el proceso de gestión de sistemas de información y el subproceso de infraestructura tecnológica del Instituto de Protección y Bienestar Animal de Cundinamarca - IPYBAC, en concordancia con el 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 de Protección y Bienestar Animal de Cundinamarca - IPYBAC, se desea prevenir los riesgos asociados que se puedan llegar a presentar en el ámbito de la seguridad de la información, De tal manera que se pueda garantizar el tratamiento adecuado 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 2022 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.

3.2 Riesgos de Seguridad y Privacidad de la Información.

A continuación, se visualizan los riegos de seguridad de la información, los cuales están asociados al Sistema de Gestión de Seguridad de La Información – SGSI del Instituto de Protección y Bienestar Animal de Cundinamarca - IPYBAC, los cuales fueron detectados sobre la vigencia 2022.

No	Riesgo	Estado	Responsable	¿Materializado?
1	Inadecuada gestión de infraestructura tecnológica y de comunicaciones	En proceso	Área de tecnología	No
2	Manipulación no autorizada de la información registrada en los sistemas del instituto.	En proceso	Área de tecnología	No
3	Incumplimiento con el modelo de Seguridad y privacidad de la información de las políticas del gobierno digital.	En proceso	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 2022.

RIESGO	CAUSAS	CONSECUENCIAS	CONTROLES (DESCRIPCIÓN)	ACCIONES A TOMAR	RESPONSABLE
Manipulación y adulteración de la información contenida en los sistemas de información para beneficio propio o de un tercero.	1. Delegación de ingreso a sistemas de información a funcionarios no autorizados. 2. Ataques cibernéticos. 3. Divulgación inapropiada de las claves de acceso. 4. Ingresos a URLS no autorizadas	1. Pérdida de la integridad de la información. 2. Investigaciones y/o sanciones administrativas, penales y fiscales. 3. Divulgación indebida de información.	* Administración del acceso a la información - permisos y roles	1. Definición de la política de control de accesos 2. Definición de la política de administración de contraseñas	Área tecnología
Fallas en los procesos de realización y restauración de los Backups (Aplicativos, Servidores, Servicios	- Almacenamiento inadecuado de las copias físicas de los backups - Mala calidad en el medio físico donde se almacena las copias - Fallas humanas - Falla lógica de la copia - Equipo de cómputo inadecuado para realizar el plan de copias	1. Manipulación o pérdida de información vital del Instituto. 2. Sanciones disciplinarias. 3. Parálisis en el normal funcionamiento de las dependencias 4. Limitaciones en la ejecución de alternativas de continuidad del negocio.	- Implementación y seguimiento del cronograma de copias de seguridad. - Asignación de personal para manejo de copias de seguridad. - Registro en la bitácora de la entrada de las copias de seguridad a la sede misional - Software de Backups	1. Mantener la adecuada ejecución de los Backups 2. Generar cronogramas de copias de seguridad	Área tecnología

3.4 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 2022, el cual es realizado trimestralmente.

Actividad	Descripción	Responsable	Fecha Inicial Planificada	Fecha Final Planificada
Primera fase de planificación: Valoración de riesgo seguridad de la información actualizada con la nueva metodología de administración del riesgo	Sistema de seguridad de la información	Tecnología revisión conjunta con el área de planeación las fechas de programación		
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	16/07/2022	19/08/2022
Definir los controles y las vulnerabilidades del sistema de información.	Controles y Análisis de vulnerabilidades definido	Área de Tecnología	16/07/2022	19/08/2022
Segunda Fase de tratamiento: definir los tratamientos y objetivos de seguimiento para los planes de manejo	Planes de manejo del riesgo	Área de Tecnología	19/08/2022	25/09/2022
Definir la declaración de aplicabilidad	Declaración de aplicabilidad a los procedimientos que manejan sistemas de información.	Área de Tecnología	19/08/2022	25/09/2022
Realizar Seguimiento al tratamiento de riesgos	Seguimiento al Cronograma de tratamiento y valoración de riesgos (trimestralmente)	Área de Tecnología	19/08/2022	25/09/2022
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	Área de Tecnología	19/08/2022	25/09/2022

	disponibilidad de los activos de información por cada dependencia.			

4 MARCO LEGAL.

Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
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 DOCUMENTO ASOCIADOS.

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 y Sistemas de Información.

CUADRO CONTROL DE CAMBIOS		
Versión	**Fecha**	**Descripción del Cambio**
1	05/09/2022	Emisión Inicial

ELIANA MARGARITA RAMÍREZ ARENAS
GERENTE GENERAL
Instituto de Protección y Bienestar Animal de Cundinamarca – IPYBAC

Aprobó: Juan Pablo Piranquive Rodriguez – Subgerente de Asuntos Administrativos
Revisó: Mónica Avellaneda - Contratista Control Interno
Oscar Marroquín – Contratista Planeación
Proyectó: Rafael Enrique Ayala Sánchez – Contratista de Tecnología e Informática.