PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2023

INSTITUTO DE PROTECCIÓN Y BIENESTAR ANIMAL DE CUNDINAMARCA – IPYBAC.

ELIANA MARGARITA RAMÌREZ ARENAS
GERENTE GENERAL

SUBGERENCIA DE ASUNTOS ADMINISTRATIVOS
2023

Contenido

1 INTRODUCCION.

El Instituto de Protección y Bienestar Animal de Cundinamarca – IPYBAC, Define la Seguridad de la Información como principio de la Política de Gobierno Digital, de igual manera define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

2 OBJETIVO.

Establecer las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad de la Operación Tecnológica, y el Modelo de Operación por Procesos del Instituto.

3 ALCANCE.

El Plan de Seguridad y Privacidad de la Información del Instituto de Protección y Bienestar Animal de Cundinamarca – IPYBAC, aplica donde éste, tenga presencia o desarrolle su acompañamiento a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, en el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos.

4 POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Instituto de Protección y Bienestar Animal de Cundinamarca – IPYBAC, protege, preserva y administra la integridad, confidencialidad, disponibilidad y autenticidad de la información, así como la seguridad y la gestión de la continuidad de la operación, previniendo incidentes mediante la gestión de riesgos integrales en seguridad y privacidad de la información, con la implementación de controles de seguridad físicos y digitales, orientados a la mejora continua en la gestión y el alto desempeño del Sistema de Gestión de Seguridad de la Información, con la finalidad de prestar servicios con calidad y transparencia.

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 directrices generales para mitigar el riesgo e 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.

4.1 OBJETIVOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

En una primera fase:

Controlar las acciones que afectan la seguridad de la información en el Instituto de Protección y Bienestar Animal de Cundinamarca – IPYBAC y que ponen en riesgo la disponibilidad, confidencialidad e integridad, como son:

- Dejar encendidos los computadores 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 Subgerencia de Asuntos Administrativos.
- Usar servicios de internet en los equipos del instituto, diferente al provisto por la Subgerencia de Asuntos Administrativos..
- 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 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 el escritorio o sala de juntas.
- 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 Subgerencia de Asuntos Administrativos 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/o bebidas, cerca de cuartos técnicos 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 IPYBAC, 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

En Tercera fase:

Se debe buscar la realización de acciones que permitan tener un mayor control en la Seguridad y Privacidad de la Información

- Brindar mecanismos de aseguramiento para el cumplimiento de la confidencialidad y confiabilidad de la información del Instituto de Protección y Bienestar Animal de Cundinamarca – IPYBAC.
- Mitigar los incidentes de Seguridad y Privacidad de la Información.
- Gestionar los riesgos de Seguridad y Privacidad de la Información.

- Establecer los lineamientos necesarios para el manejo de la información y los recursos tecnológicos del Instituto de Protección y Bienestar Animal de Cundinamarca – IPYBAC.

- Fortalecer las capacidades y cultura organizacional de Seguridad de la Información en los colaboradores y contratistas del Instituto de Protección y Bienestar Animal de Cundinamarca – IPYBAC.

5 PLAN DE SOSTENIBILIDAD DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Plan de sostenibilidad del Modelo de Seguridad y Privacidad de la Información comprende el siguiente cronograma y se le hace seguimiento mes a mes.

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha final
Gestión de Incidentes de Seguridad de la Información	Gestionar los incidentes de Seguridad de la Información reportados	Gestionar los incidentes de Seguridad de la Información.	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023
	Realizar informe de los incidentes de Seguridad de la información	Presentar los informes de los incidentes de seguridad de la información que se materializaron de manera mensual.	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023
	Informar las novedades de los Boletines del CSIRT al especialista de seguridad informática	Verificar las recomendaciones envidas por el CSIRT	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023
	Seguimiento a los Eventos o vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades.	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023
	Revisar el Procedimiento de gestión de Incidentes y actualizarse en caso de ser necesario.	Actualizar el Procedimiento de gestión de incidentes de seguridad de la Información en caso de ser necesario.	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023
Acciones Correctivas y Oportunidades de Mejora	Seguimiento a las Acciones Correctivas y Oportunidades de Mejora identificadas en el Eje de Seguridad de la Información	Informe cuatrimestral de Acciones Correctivas y Oportunidades de Mejora	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023

		Gestionar el cargue del análisis de causas, plan de tratamiento o evidencia del cumplimiento de la actividad según sea requerido.	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023
Gestión de Riesgos	Sensibilización	Socializar la Guía y Herramienta-Gestión de Riesgos de Seguridad y privacidad de la Información.	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023
	Identificación de Riesgos de Seguridad y Privacidad de la Información.	Brindar apoyo en la Identificación, Análisis y Evaluación de los Riesgos - Seguridad y Privacidad de la Información.	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023
		Realizar la realimentación, revisión y verificación de los riesgos identificados con sus planes de tratamiento.	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023
Gobierno Digital	Modelo de Seguridad y Privacidad de la Información y Seguridad Digital	Sensibilizar y Apropiar a los Colaboradores del IPYBAC en los cambios de la herramienta de MINTIC.	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023
		Realizar la verificación del monitoreo a la infraestructura Tecnológica del IPYBAC por parte del CSIRT Gobierno, cuando se requiera	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023
		Participar en las reuniones de las infraestructuras criticas cibernéticas convocadas por CCOCI	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023
		Reportar las Infraestructuras críticas cibernéticas del IPYBAC al Comando Conjunto de Operaciones Cibernéticas de Min Defensa. CCOCI	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023

		Actualizar el Documento de autoevaluación de la Entidad en la Implementación de Seguridad y Privacidad de la Información	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023
		Actualizar el Documento FURAG de la Entidad en la Implementación de Seguridad y Privacidad de la Información	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023
Seguimiento Regionales y Procesos de la Sede de la Dirección General.	Reuniones de Seguimiento	Realizar reunión con los procesos y regionales donde se les explique las novedades del plan operativo.	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023
	Planificación Estratégica	Definir las actividades y tareas del plan de seguimiento SGSI	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023
Dominios de la Norma ISO 27001:2013	Revisión Manual Políticas de Seguridad de la Información, Resolución de Seguridad de la Información y documentación transversal al Eje	Implementar Manual Políticas de Seguridad de la Información y Resolución del Eje de Seguridad de la Información.	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023
		Apoyar en la actualización de la documentación transversal al Eje	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023
Auditorías Internas y Externas	Acompañamieto en las auditorías internas y externas que se presenten	Acompañar en las auditorías internas y externas que se presenten	Subgerencia de Asuntos Administrativos - Contratista Sistemas Tecnológicos	20/02/2023	31/12/2023

6 DOCUMENTOS DE REFERENCIA.

- Ley 44 de 1993 “por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944.” (Derechos de autor).
- Ley 527 de 1999 “por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.

- Ley 594 de 2000 “Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”.
- Ley 734 de 2002 “Por la cual se expide el Código Disciplinario Único”.
- Ley 1273 de 2009 “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”.
- Ley 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.
- Decisión Andina 351 de 2015 “Régimen común sobre derecho de autor y derechos conexos”.
- Ley 1955 de 2019 “Por la cual se expide el Plan Nacional de Desarrollo 2018-2023 “Pacto por Colombia, pacto por la Equidad”.
- CONPES 3854 de 2016 – Política de Seguridad Digital del Estado Colombiano
- CONPES 3995 Política Nacional de Confianza y Seguridad Digital
- Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC.
- Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.
- Decreto 1083 de 2015 sustituido por el artículo 1º del Decreto 1499 de 2017 - políticas de Gestión y Desempeño Institucional, (“11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital)

CUADRO CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**NATURALEZA DEL CAMBIO**
1	05/09/2022	Creación del documento.
2	25/01/2023	Actualización del documento para la vigencia 2023

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

Aprobó: Comité Institucional de Gestión y Desempeño
Revisó: Juan Pablo Piranquive Rodriguez – Subgerente de Asuntos Administrativos
Mónica Avellaneda - Contratista Control Interno
Oscar Marroquín – Contratista Planeación
Proyectó: Juan Pablo Piranquive Rodriguez – Subgerente de Asuntos Administrativos