AGRICULTURA

SECRETARÍA DE AGRICULTURA Y DESARROLLO RURAL

DOCUMENTO DE SEGURIDAD

SERVICIO NACIONAL DE SANIDAD, INOCUIDAD Y CALIDAD AGROALIMENTARIA

SENASICA

SERVICIO NACIONAL DE SANIDAD, INOCUIDAD Y CALIDAD AGROALIMENTARIA

1. Presentación.

Los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos, establecen que el derecho al acceso a la información será garantizado por el Estado y que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la Ley, así mismo la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) establece por su parte un conjunto de bases, principios y procedimientos para garantizar el derecho a la protección de datos con carácter personal y que se encuentren en posesión de los sujetos obligados, entre los que se encuentra el Servicio Nacional de Sanidad, Inocuidad y Calidad Agroalimentaria (SENASICA), Órgano Administrativo Desconcentrado de la Secretaría de Agricultura y Desarrollo Rural (SADER), el presente Documento de Seguridad tiene como propósito establecer el marco de referencia del tratamiento de los datos personales que se llevan a cabo al interior de las unidades administrativas que conforman su estructura orgánica del SENASICA, para mantener vigente y promover la mejora continua en la protección de los mismos, en términos de lo previsto en los artículos 35 y 36 de la LGPDPPSO, además de desarrollar buenas prácticas en la materia.

En ese sentido, el SENASICA ha identificado los procesos trámites y servicios que involucran el tratamiento de datos personales, a efecto de mantener la seguridad de los mismos durante el ciclo de vida de la información, indicando la forma en la que se trata, las medidas de seguridad adoptadas y las unidades administrativas responsables de su protección, así como las finalidades del tratamiento de acuerdo a sus respectivas atribuciones, dichos elementos interrelacionados constituyen un sistema interno para la gestión y tratamiento de los datos personales en posesión de este Servicio Nacional, de conformidad con lo dispuesto en el artículo 34 de la LGPDPPSO, para establecer, operar, monitorear, mantener y mejorar el tratamiento y seguridad de los datos personales.

El SENASICA está comprometido con la tutela de los datos personales que trata y ha impulsado a su interior las acciones conducentes para evitar la alteración, pérdida, transmisión y acceso no autorizados a los datos, mediante la implementación de medidas físicas, administrativas y técnicas, tendentes a garantizar la seguridad e integralidad de los mismos, así como su seguimiento y supervisión continuos, por ello dicho Sistema permite disponer de información relacionada con las medidas de seguridad, el análisis general de las amenazas y posibles vulnerabilidades, así como los mecanismos o acciones a implementar para mitigarlas.

El presente documento se integra a partir de la gestión de actividades coordinadas para controlar y verificar que el tratamiento de los datos personales sea acorde con los principios que rigen su protección, para el SENASICA la seguridad en esta materia constituye un compromiso con el cumplimiento de las disposiciones previstas tanto en la citada LGPDPPSO, como en los Lineamientos Generales de Protección de Datos Personales para el Sector Público por parte de todos los involucrados. En términos de lo previsto en el artículo 36, fracción II de la Ley General, el presente documento se deberá mantener actualizado como resultado del proceso de mejora continua, así como de los cambios en la estructura orgánica y el Reglamento Interior, lo cual propicia la actualización de diversos elementos, tales como los inventarios de datos personales; las medidas de seguridad adoptadas con motivo de su tratamiento y, el análisis de riesgo y brecha, para monitorear las medidas adoptadas, identificar posibles vulneraciones y mitigar los riesgos; además de avanzar en un proceso de sensibilización permanente respecto de la relevancia que tiene para la institución adoptar medidas correctivas y preventivas, en función de los resultados obtenidos de la revisión de los sistemas de datos.

2. Objetivo y alcance

Implementar medidas de seguridad administrativas, físicas y técnicas que ha adoptado el SENASICA para garantizar la confidencialidad, integridad y disponibilidad de los datos personales; así como determinar las posibles vulnerabilidades, amenazas y riesgos de los que pueden ser objeto en un plano general los sistemas de información y procesos en los se tratan datos personales conforme a lo establecido en la LGPDPPSO y a los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Se identifican a través del inventario de datos personales, procesos administrativos trámites, servicios que brindad las unidades administrativas del SENASICA en los que se solicitan y tratan datos personales, mismos que se encuentran bajo su estricta responsabilidad tanto en los medios electrónicos como en los espacios físicos en que se operan y resguardan dichos datos personales.

En este sentido, la Unidad de Transparencia integra el presente Documento de Seguridad con base en la información generada por las unidades administrativas en el desarrollo de las sus funciones y, de conformidad con las disposiciones aplicables.

3. Sistema de gestión de los datos personales en posesión del SENASICA.

Para el tratamiento de los datos personales que lleva a cabo el SENASICA a través de su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación aplicable a los mismo, se realiza el establecimiento de políticas y métodos orientados a salvaguardar su confidencialidad, integridad y disponibilidad, conforme a los preceptos previstos por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley General de Transparencia y Acceso a la Información Pública.

El SENASICA identifica todos y cada uno de los procesos, trámites y servicios a cargo de las unidades administrativas en los que, de acuerdo con el ámbito de sus atribuciones y funciones se involucra el tratamiento de datos personales, obteniendo el inventario de datos personales que se encuentran bajo su responsabilidad, considerando los elementos mínimos que establece el artículo 33, fracción II de la Ley General y el diverso 58 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

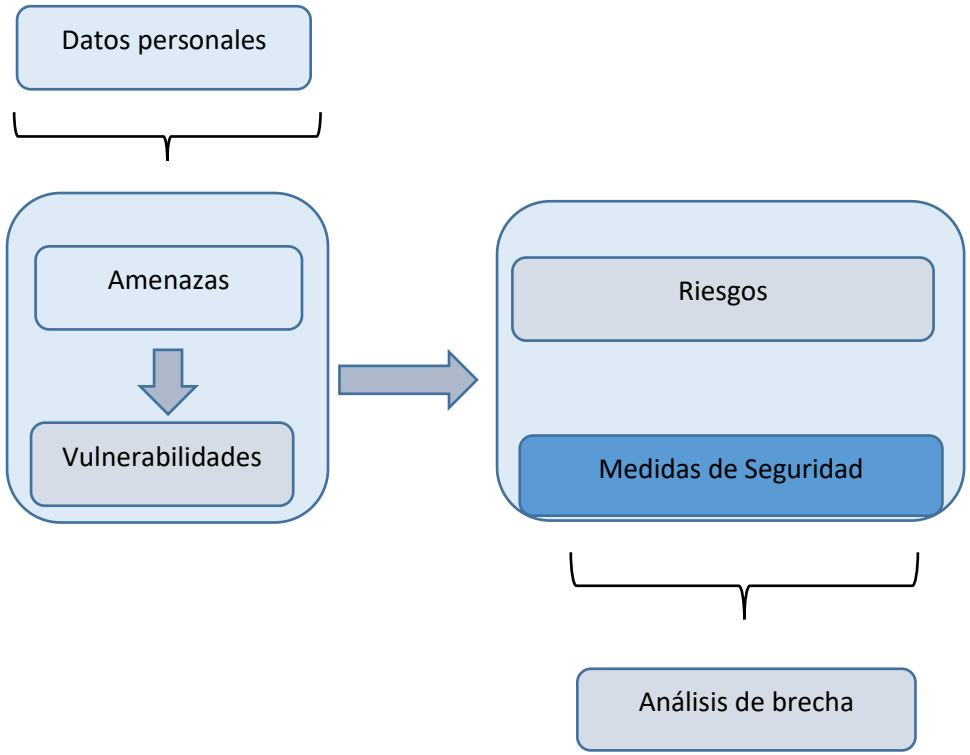
Para obtener el inventario de datos personales se utilizó un instrumento homogéneo y estandarizado, con el propósito de identificar, entre otros aspectos, la categoría y tipo datos que son sometidos a tratamiento, incluyendo los de carácter sensible; los medios a través de los cuales se obtienen dichos datos; el sistema físico y/o electrónico que se utiliza para su acceso, manejo, aprovechamiento, monitoreo y procesamiento; las características del lugar donde se ubican las bases físicas o electrónicas de datos; las finalidades del tratamiento, y el nombre, cargo y adscripción de los servidores públicos que tienen acceso al tratamiento, además de si son objeto de la transferencia y la identificación de los destinatarios o receptores de los mismos, así como las causas que la justifican.

En ese mismo sentido, el inventario ha contribuido desde el punto operativo a considerar el ciclo de vida de los datos personales, de forma tal que los servidores públicos que intervienen en el tratamiento conocen que, una vez concluida la finalidad los datos, éstos deben ser sometidos a un proceso de bloqueo y, en su caso, de cancelación, supresión o destrucción, lo que cobra especial relevancia en el marco del proceso de baja documental que las áreas realizan conforme a las disposiciones que regulan la gestión documental al interior de la Institución.

De igual forma, una vez integrados los inventarios de datos, se dispuso de la metodología para la elaboración del análisis de riesgos, en la cual, atendiendo a lo previsto en el artículo 33, fracción IV de la Ley General de la materia, las áreas responsables de su tratamiento identificaron el valor de los datos personales de acuerdo con su categoría

y el ciclo de vida; el valor de exposición de los activos involucrados en el tratamiento; las consecuencias que pueden generarse para los titulares de los mismos con motivo de su posible vulneración y, los factores de riesgo a los que eventualmente se encuentran expuestos.

Con base en dicho análisis de riesgo, además de promover el reconocimiento de las medidas de seguridad administrativas, entendidas como el conjunto de políticas y procedimientos de gestión, soporte y revisión de la seguridad de la información; físicas, que corresponden a las acciones o mecanismos para proteger el entorno físico de los datos, así como de los recursos involucrados en su tratamiento y, técnicas que se valen de la tecnología para proteger el entorno digital de la información, también se han registrado nuevas medidas de seguridad que deberán desarrollarse para fortalecer algunos de los controles que actualmente son implementados; es decir, el análisis de brecha a partir del cual será posible mitigar los riesgos a los que están expuestos los datos tratados, tal y como se ilustra a continuación el siguiente esquema:



Considerando que la identificación de vulnerabilidades tiene por objeto prevenir posibles dificultades en la seguridad de los datos bajo un enfoque proactivo; es decir, identificar áreas de oportunidad en materia de seguridad de datos personales sin que éstas constituyan un daño efectivo, es que se listan como posibles vulnerabilidades, las siguientes:

1. Controles de acceso físico y electrónicos inadecuados a sistemas de archivos.

2. Deficiente conocimiento de procedimientos en materia de seguridad de datos.

3. Inadecuada administración de autorizaciones de accesos a los datos personales (sistemas de privilegio)

4. Falta de definición de perfiles y roles para delimitar funciones manejo y uso de datos.

5. Falta de seguimiento y monitoreo a políticas de seguridad.

6. Ausencia de mecanismos de confidencialidad por parte del personal (interno) o por terceros (externos).

Aunado a las anteriores vulnerabilidades, de manera enunciativa más no limitativa, se examinan algunos tipos de amenazas, que pueden ser intencionales o no, a las que podría enfrentarse la Institución y sus activos de información.

Tipo de Amenazas:

- Robo, extravío o copia no autorizada.
- Uso, acceso o tratamiento no autorizado.
- Daño, alteración o modificación no autorizado.
- Pérdida o destrucción no autorizada.
- Otras.

El riesgo que de manera general puede presentarse en caso de que las amenazas señaladas potencialicen, es el de facilitar el acceso a los datos personales de manera no autorizada con el fin de comprometer su confidencialidad, disponibilidad e integridad, por lo que las medidas de seguridad por parte de las áreas responsables están orientadas a proteger los datos personales.

A partir de la identificación de vulnerabilidades y amenazas, se han establecido medidas generales de seguridad que de acuerdo a la experiencia y mejores prácticas son monitoreadas para lograr la mejora continua por parte de todos los involucrados en el tratamiento. Como parte del Sistema de Gestión y Política de Seguridad institucional, se enmarcan las reglas generales siguientes:

a) Tratar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley General;

b) Sujetar el tratamiento de los datos personales al principio de consentimiento, salvo las excepciones previstas por la Ley;

c) Informar a los titulares del tratamiento de los datos y sus finalidades. A través del Aviso de Privacidad;

d) Procurar que los datos personales tratados sean correctos y estén actualizados;

e) Suprimir los datos personales cuando hayan dejado de ser necesarios para las finalidades para las cuales se obtuvieron;

f) Tratar los datos personales estrictamente para propósitos legales o legítimos;

g) Limitar el tratamiento de los datos personales al cumplimiento de las finalidades;

h) No obtener datos personales a través de medios fraudulentos;

i) Respetar la expectativa razonable de privacidad del titular;

j) Tratar estrictamente los datos personales necesarios, adecuados y relevantes en relación con las finalidades;

k) Velar por el cumplimiento de los principios;

l) Establecer y mantener medidas de seguridad;

m) Guardar la confidencialidad de los datos personales;

n) Identificar el flujo y ciclo de vida de los datos personales;

o) Mantener actualizado el Inventario de datos personales o de las categorías que maneja el SENASICA;

p) Respetar los derechos de los titulares en relación con sus datos personales;

q) Aplicar las excepciones contempladas en la normativa en materia de protección de datos personales, y;

r) Identificar a los servidores públicos del SENASICA responsables del tratamiento de los datos personales.

Con base en lo anterior, el SENASICA determina las pautas de acción del personal encargado de tratamiento de datos personales con miras a generar su correcto resguardo, buscando en todo momento actuar en apego a las directrices de la LGPDPPSO y los Lineamientos de la materia, siempre en consideración de la salvaguarda del derecho a la privacidad y protección de datos de las personas.

4. Inventario de Datos Personales del SENASICA

Para cumplir con los objetivos y obligaciones que prevé la LGPDPPSO, particularmente en materia de seguridad y, como parte del Sistema de Gestión de Seguridad de Datos Personales del SENASICA, se realizó una actualización dentro las unidades administrativas que conforman su estructura orgánica, para identificar los trámites, servicios y procesos en los que actualmente se lleva a cabo tratamiento de datos personales; obteniendo con ello el denominado Inventario de Datos Personales del SENASICA.

Por inventario de tratamiento de datos, se entiende el control documentado del conjunto de operaciones que realizan las unidades administrativas del SENASICA con motivo de los datos que se recaban de las personas, a través de procedimientos automatizados o físicos, que van desde su obtención, registro, organización,

conservación, utilización, cesión, difusión, interconexión, hasta la rectificación, cancelación y oposición, con motivo de la atención del ejercicio de éstos derechos en el ámbito de sus atribuciones.

En tal virtud, en coordinación con las áreas y derivado del proceso de actualización de información, se advirte que en general las cuatro direcciones generales que realizan funciones sustantivas; Salud Animal, Sanidad Vegetal, de Inspección Fitozoosanitaria y de Inocuidad, Agroalimentaria, Acuícola y Pesquera, las direcciones generales de Administración e Informática, Jurídica, así como la Unidad de Coordinación y Enlace y la Dirección de Desarrollo y Vinculación, llevan a cabo el tratamiento de datos personales.

Como resultado de dicha actualización, se advirtió que en las unidades administrativas en la que se tratan datos, a través una o varias de las áreas que las conforman, dicho tratamiento se debe a la atención de los trámites, servicios, operaciones o procesos que realizan con motivo del ejercicio de sus facultades, así como actividades de carácter administrativo derivadas de la administración de recursos humanos, materiales y financieros, los procesos de capacitación, entre otros.

Se identificó que en el ejercicio sus atribuciones, las direcciones generales que realizan funciones sustantivas y administrativas el tratamiento de datos personales se categorizan en los siguientes rubros:

Unidad Administrativa	Trámite, Servicios o Proceso	Datos personales que trata
Dirección General de Inocuidad Agroalimentaria, Acuícola y Pesquera	Trámites, servicios, relacionados con dictámenes y resoluciones en materia de OGMs, autorizaciones y certificaciones en materia de TIF, así como cursos e informes.	Nombre, domicilio, firma RFC, CURP, número de teléfono, correo electrónico, Clave de elector
Dirección General de Inspección Fitozoosanitaria	Trámites y servicios relacionados con la expedición de certificados, autorizaciones, avisos de movilización, actas circunstanciadas, dictámenes, verificaciones , entre otros	Nombre, RFC, CURP, domicilio, correo electrónico, números de teléfono, tipo de actividad comercial, número de cédula profesional, número de credencial INE, clave de autorización.

Dirección General de Salud Animal	Trámites y servicios relacionados con Diagnóstico, Constatación y Ensayos de Aptitud; expedición de certificados de exportación e importación, autorizaciones, aprobaciones, entre otros.	Nombre, domicilio, firma RFC, número de teléfono, correo electrónico, CURP, secreto comercial, nacionalidad.
Dirección General de Sanidad Vegetal	Trámites y servicios relacionados con la expedición de certificados de exportación, importación y movilización, alertas fitosanitarias, aprobaciones de órganos de coadyuvancia, certificación de establecimientos, diagnóstico fitosanitario, entre otros	Nombre, domicilio, firma RFC, CURP, número de teléfono, correo electrónico.
Dirección General Jurídica	Recursos jurídicos, quejas y recomendaciones de la CNDH, procedimientos administrativos, juicios, convenios y contratos.	Nombre, firma, domicilio, correo electrónico, RFC, CURP, firma, clave de elector, cuenta bancaria, clabe interbancaria, número de teléfono, nacionalidad, datos familiares, fotografía, huella digital, sexo.
Dirección General de Administración e Informática	Administración de recursos humanos, financieros, recursos materiales, servicios y tecnologías de la información	Nombres, Domicilio, Correo electrónico, RFC, CURP, Datos Académicos y laborales, números de teléfono, clave de elector, clave interbancaria, cuenta bancaria, estado civil, sexo, nacionalidad, firma, estado de salud, evaluación psicométrica, origen racial o étnico, huella digital, cédula profesional, número de pasaporte, número de licencia de conducir, número de

		seguridad social, numero de licencia de conducir, número de placa de vehículo.
Unidad de coordinación y Enlace	Trámites del SENASICA, Control y Monitoreo de Residuos Tóxicos, suspensión o revocación de certificados, denuncia por la detección de Clenbuterol, Programa Proveedor Confiable, entre otros.	Nombre, domicilio, firma RFC, CURP, número de teléfono, correo electrónico.
Dirección de Desarrollo y Vinculación	Campañas de comunicación social, boletines informativos, reporteros articulistas, redes sociales, eventos y reuniones, entre otros	Nombre de persona física, RFC, domicilio correo electrónico y número telefónico.

A partir de lo anterior, el Inventario de Datos Personales del SENASICA posibilita la identificación de hallazgos en relación con el tratamiento de datos personales, aportando los elementos que permiten focalizar las áreas con mayor incidencia en el tratamiento de éstos, y con ello, enfocar los trabajos de atención para el cumplimiento de las disposiciones jurídicas en materia de protección de datos.

Sobre el particular, se identificó que por lo que hace al tratamiento de datos de identificación, se realizan en todas las unidades administrativas aludidas; por lo que hace a los patrimoniales en dos de ellas se realiza tratamiento de éstos, y por los que hace a los sensibles, únicamente en una se trata este tipo de datos.

Lo anterior, permite advertir que los datos personales de carácter identificativo y de contacto son los que se manejan todas las unidades administrativas, los patrimoniales en las áreas administrativas y, en casos muy específicos, los datos de naturaleza sensible. Sin embargo, es preciso indicar que se detectaron trámites, servicios y procesos en los que se realiza tratamiento de datos tanto identificativos y patrimoniales, otros con identificativos y sensibles, y también de identificativos, patrimoniales y sensibles en una misma unidad administrativa.

Ante este contexto, el Inventario de Datos Personales del SENASICA, a partir de los hallazgos identificados en su actualización, se constituye como un elemento del Sistema de Gestión de Datos Personales, que junto con las medidas de seguridad representa un instrumento de evidencia para la implementación de las directrices de la política en materia de protección de datos personales. Asimismo, delinea las rutas para una capacitación focalizada en materia protección de datos en aras de fortalecer la estructura de los operadores en cada uno de los

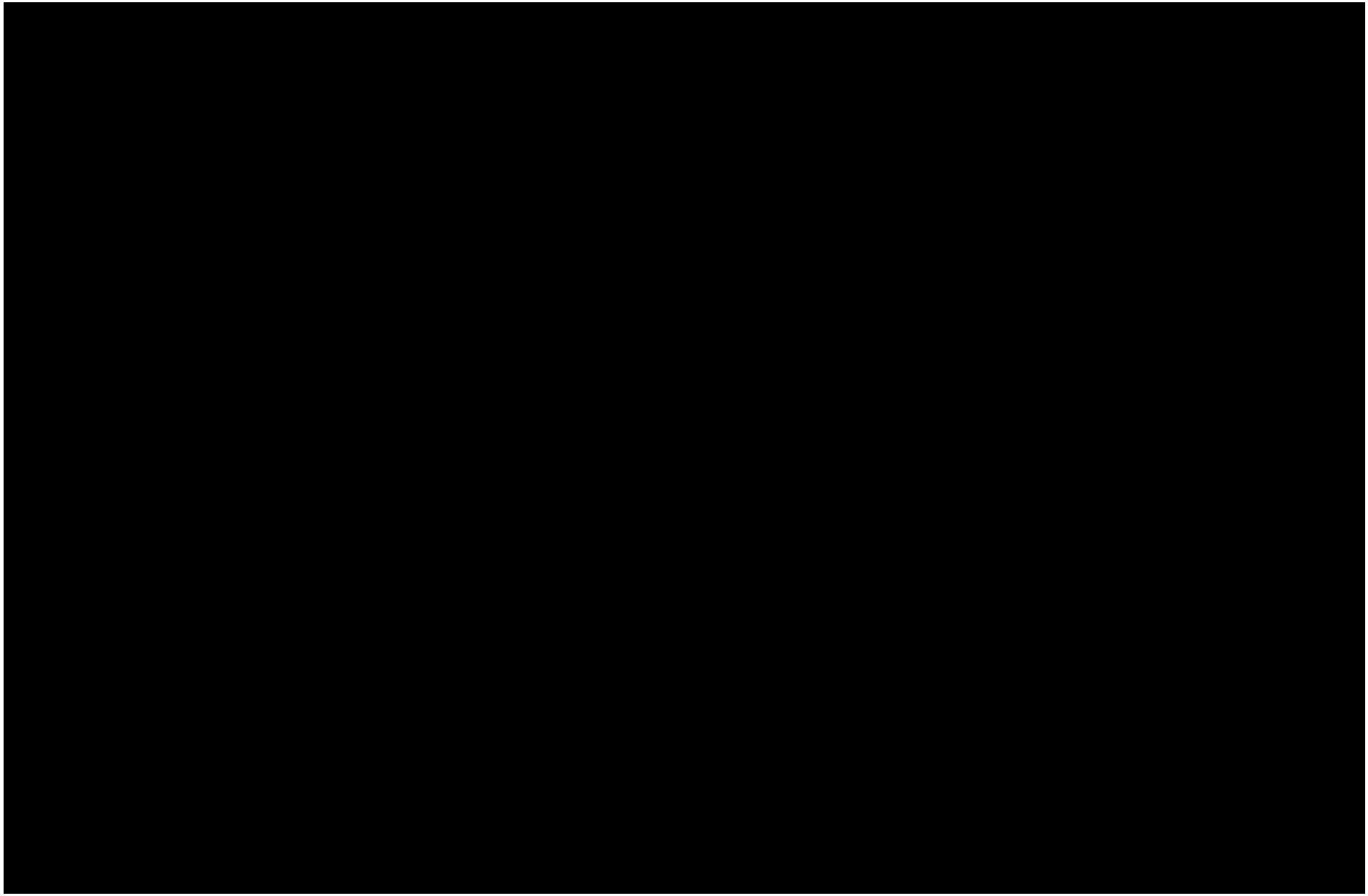
procesos en que se tratan datos, buscando con ello sensibilizar y preparar a los responsables y encargados de los mismos para que su tratamiento se lleve a cabo de conformidad con los estándares nacionales e internacionales en la materia. En tal virtud, el Inventario de Datos Personales se inscribe como un elemento más de la política para el cumplimiento de las directrices determinadas por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, aportando con ello certeza a la ciudadanía de cuáles son y cuál es el destino de los datos recabado por éste Servicio Nacional.

5. Análisis de riesgos.

[redacted]

6. Elementos para el análisis de riesgos.

[redacted]



Se clasifica la información contenida en el Documento de seguridad concerniente al Plan de Trabajo, el Análisis de Riesgo y Análisis de Brecha de conformidad con el Criterio 1 del Anexo 3. Herramienta de Evaluación de la Guía antes mencionada, asimismo, con fundamento en los artículos 113, fracción XIII de la Ley General de Transparencia y Acceso a la Información Pública y artículo 110, fracción XIII de la Ley Federal de Transparencia y Acceso a la Información Pública

7. Estado actual del riesgo de datos personales

[redacted]

8.- Análisis de brecha

[redacted]

9. Medidas generales de seguridad

Las medidas generales de seguridad administrativas, físicas y técnicas con las que actualmente cuenta el SENASICA para mantener la confidencialidad e integralidad de la información, así como para proteger los datos personales contra daño, pérdida, destrucción o alteración, así como evitar el uso, acceso o tratamiento no autorizado, e impedir la divulgación no autorizada, son las siguientes:

a) Medidas administrativas.

1. Adopción de un esquema de capacitación permanente en materia de la Ley General de Protección de Datos Personales en posesión de Sujetos Obligados (LGPDPPSO), impartido mediante el Campus Virtual de Capacitación del organismo garante.

2. Implementación de formatos de entrada y salida de préstamo de documentos por parte del área encargada del archivo.

3. Resguardo de los expedientes bajo los criterios, directrices y lineamientos para la atención de los expedientes técnicos.

4. Mecanismos de control desarrollados conforme a lo establecido en los lineamientos del Sistema de Gestión de Documentos institucional.

5. Difusión a través de los medios electrónicos internos a los usuarios o personal con acceso a sistemas de datos personales, acerca del deber de confidencialidad.

6. Reportar al superior jerárquico los incidentes detectados respecto de pérdida o alteración de cualquier documento que contengan datos personales.

7. Revisar que las versiones públicas de documentos que se publican o se entregan a personas a través de las solicitudes de acceso a la información, estén correctamente testadas.

b) Medidas físicas.

1. Resguardo de documentos e información en archivos físicos de trámite y concentración.

2. Disponer de la instalación de chapas con llave para mantener control de acceso de personas a espacios de resguardo de información.

3. Limitar el número de personas con acceso a archivos físicos.

4. Realizar el registro de personas con acceso a espacios físicos en los que se resguarda información con datos personales.

5. Procurar suscribir responsivas de confidencialidad con el personal que trata datos personales.

6. Designación de personal con acceso controlado a espacios de resguardo físico de expedientes y documentos con datos personales.

7. Resguardo de llaves en oficinas de acceso restringido.

c) Medidas técnicas.

1. Utilizar claves de usuario y contraseñas de manera personal, y evitar compartirlas, prestarlas o registradas a la vista de otras personas.

2. Establecer y utilizar contraseñas robustas, es decir, de al menos ocho caracteres alfanuméricos y especiales, evitando que sean iguales al nombre del usuario, o cualquier otro nombre de personas, considerando que éstas sean fáciles de recordar y difíciles de adivinar o descifrar por un tercero, a fin de salvaguardar la información y datos personales a los que se tenga acceso.

3. Notificar de manera inmediata a la Dirección de Tecnologías de la Información casos en los que los usuarios identifiquen o consideren que sus claves de usuario y/o contraseñas han sido utilizadas por un tercero.

4. Utilizar el correo electrónico para fines relacionados con las actividades laborales, evitando remitir datos personales.

5. Mantener los documentos electrónicos y físicos en lugares seguros, bajo llave, dentro de cajones cerrados, o bajo la protección de alguna contraseña, a fin de promover la restricción a los datos personales que pudieran contener.

6. No difundir, transmitir o compartir documentos electrónicos ni físicos que contengan datos personales, a fin de garantizar que estos no sean divulgados de manera no autorizada.

7. Evitar dejar u olvidar los documentos físicos que contengan datos personales en los equipos de impresión, así como evitar su impresión, escaneo y fotocopiado si no es realmente requerido para las actividades laborales.

8. Evitar el acceso a los sistemas de información de tratamiento de datos personales, bajo el precepto del mínimo privilegio; es decir, únicamente al personal que por sus funciones y facultades laborales los requiera,

a fin de mantener una adecuada segregación de funciones, restricción de acceso y tratamiento de esos datos.

9. Borrar o eliminar de la papelera de reciclaje del escritorio de los equipos de cómputo los documentos o archivos electrónicos que nos son necesarios para el desarrollo de funciones.

10. Notificar las bajas de accesos a los sistemas de información o de tratamiento de datos personales, con oportunidad, para restringir el acceso a dichos datos por personal no autorizado.

Adicionalmente, como parte de la política de seguridad técnica, la Dirección de Tecnologías de la Información implementa los siguientes controles:

1. Definición de políticas de contraseñas.

2. Asignación privilegios de acuerdo a roles y funciones.

3. Agente de seguridad instalado en administrativos de servidores de correo electrónico.

4. Tareas de respaldo por servidor y por agente.

5. Autenticación de correo electrónico.

6. Revisar información en alta disponibilidad con contraseña de directorio de datos y acceso restringido.

7. Tareas de respaldo por servidor y de las instancias de base de datos del servicio.

8. Acceso a los sistemas conforme a procedimiento de administración de usuarios y contraseñas con cuenta local con permiso de administrador.

9. Borrado seguro de la información que reside en los equipos de cómputo.

10. Deshabilitación de cuentas de personal que causa baja.

11. Acceso controlado de administración y accesos privilegiados.

12. Definición de procedimientos y controles de seguridad de la información.

13. Monitoreo de las medidas de seguridad.

La supervisión de las medidas de seguridad administrativas, técnicas y físicas son elementos importantes para la mejora continua, en virtud de que permiten definir nuevos controles de monitoreo y seguimiento de éstas. Entre las medidas de supervisión y monitoreo se encuentran las siguientes:

1. Revisar la actualización permanente del esquema de contraseñas de acceso a los sistemas, verificando que los valores se encuentren determinados conforme a la política implementada por la Dirección de Tecnologías de la Información.

2. Monitorear que todas las cuentas que se dan de alta para otorgar acceso a la red, sea validada en el campo correspondiente a la contraseña, a fin de asegurar el uso.

3. Revisar el cumplimiento de protocolos.

4. Validar que los accesos, baja o cambio a sistemas se realicen conforme al proceso de administración de usuarios.

5. Vigilar que el ingreso de personas sea a través de los accesos correspondientes, plenamente identificados.

6. Revisar la aplicación correcta de los formatos de entrada y salida de préstamo de documentos que se encuentran en archivos de concentración y de trámite por parte del área encargada del archivo.

7. Resguardo de los expedientes bajo los criterios, directrices y lineamientos para la atención de los expedientes técnicos y reservados.

10. Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad

El artículo 30, fracción V, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece que entre los mecanismos que se deberán adoptar para cumplir con el principio de responsabilidad, se encuentra el de establecer un sistema de supervisión y vigilancia, incluyendo auditorías, que permita comprobar el cumplimiento de las políticas de protección de datos personales.

En ese sentido, el artículo 35, fracción VI, de la Ley General establece que el documento de seguridad deberá contener, entre otros aspectos, los mecanismos de monitoreo y revisión de las medidas de seguridad.

Al respecto, el artículo 33, fracción VII, de la Ley General, dispone que se deberán de monitorear y revisar de manera periódica los aspectos siguientes:

1. Las medidas de seguridad implementadas en la protección de datos personales.

2. Las amenazas y vulneraciones a que están sujetos los tratamientos o sistemas de datos personales

En ese sentido, el artículo 63 de los Lineamientos Generales de protección de datos personales para el sector público establece que el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.

Para cumplir con lo anterior, el responsable deberá monitorear continuamente lo siguiente:

1. Los nuevos activos que se incluyan en la gestión de riesgos.

2. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras.

3. Las nuevas amenazas que podrían estar activas dentro y fuera del sujeto obligado y que no han sido valoradas.

4. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.

5. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.

6. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.

7. Los incidentes y vulneraciones de seguridad ocurridos.

Asimismo, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

En ese sentido, el SENASICA desarrollará el cumplimiento de dicha obligación a través de los siguientes mecanismos:
Mecanismo de monitoreo y supervisión
La Unidad de Transparencia será la encargada de ejecutar el mecanismo de monitoreo y supervisión de las medidas de seguridad implementadas en la protección de datos personales, conforme a las siguientes acciones:

1. Requerirá a cada una de las unidades administrativas que reportaron tratamientos de datos personales, la actualización de sus inventarios de datos personales y un reporte anual sobre el cumplimiento de las medidas de seguridad adoptadas en la protección de datos personales, que considere lo siguiente:

   - Las notificaciones a los servidores públicos que tratan datos personales mediante el cual se especifican las funciones, obligaciones y cadena de mando que contemplen acciones sobre la obtención, almacenamiento, uso, bloqueo, cancelación, supresión o destrucción de los datos personales.

- Lista de servidores públicos que tienen acceso a los sistemas, archivos físicos de tratamiento

- El análisis de riesgo y brecha identificando las amenazas, vulnerabilidades, medidas de seguridad existentes y efectivas, así como las medidas de seguridad faltantes y la existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados.

2. Analizará los reportes de las áreas y emitirá un dictamen o ficha técnica en el que se plasmarán las recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad, con la finalidad de que las áreas las atiendan y remitan las evidencias de su cumplimiento.

3. Además, la Unidad de Transparencia deberá monitorear las alertas de seguridad de los datos personales, como posibles incidentes de seguridad, mismo que se desarrollará a través de las siguientes actividades:

   - Verificar si el hecho o evento podía dar como consecuencia una vulneración a la seguridad (posible incidente de seguridad), es decir:

     - Que exista una amenaza que, de haberse concretado, hubiera producido sus efectos en el tratamiento de los datos personales.
     - Que dichos efectos, de haberse materializado, hubieran representado un daño en los activos.

   - El área que advirtió de la alerta de seguridad deberá enviar a la brevedad posible un reporte a la Unidad de Transparencia, en la deberá informar:

     - Circunstancias de modo, tiempo y lugar en que se detectó la amenaza.
     - Sistema de Tratamiento de Datos Personales, conforme al Inventario, en el que se detectó la amenaza.
     - Datos personales involucrados.
     - Datos de identificación y de contacto de la persona servidora pública responsable del tratamiento de los datos personales.

- Actuaciones que pueden evitar la explotación de la amenaza.
- Descripción de los controles físicos o electrónicos involucrados en la amenaza.

4. Con base en lo anterior Unidad de Transparencia registrará la alerta de seguridad y analizará el impacto de la amenaza y, de ser posible, determinará una estrategia de prevención, para lo cual, podrá apoyarse de las áreas técnicas y normativas del SENASICA, con la finalidad de evitar que la alerta de seguridad pueda desencadenarse.

5. Mantendrá actualizados los instrumentos de evaluación en el micrositio de protección de datos personales con el fin de que el Órgano Garante con base en su Programa de Verificación revise la eficacia y eficiencia del sistema de gestión, previo a la verificación realizar una auditoría interna y verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

6. Planteará e implementará, en su caso, en coordinación con las unidades administrativas, acciones de mejora encaminadas al fortalecimiento del Sistema de Gestión de Protección de Datos personales del SENASICA.

11. Propuesta de capacitación en materia de datos personales.

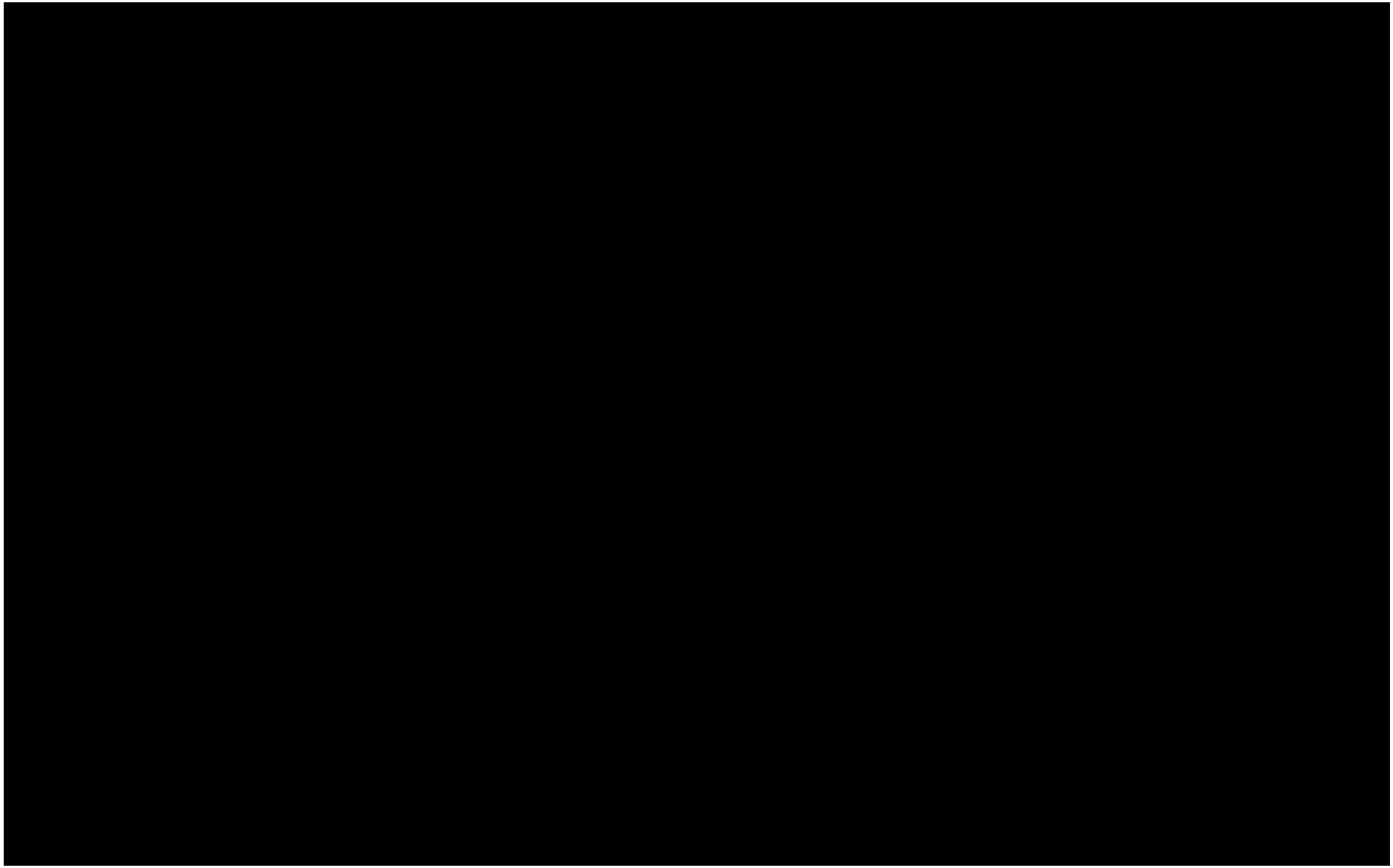
Uno de los factores esenciales para la implementación de los controles y demás medidas de seguridad, la actualización y mejora continua del inventario de datos personales, el apego a la normatividad y a Ley, así como la concientización en la materia por parte del personal involucrado en el tratamiento de datos personales, es el conocimiento y capacitación, por lo que el SENASICA aprovecha los recursos y herramientas que el propio Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), pone a disposición en esta materia. Entre los elementos de los que resulta necesario profundizar se encuentran los siguientes:

1. Introducción al derecho a la protección de datos personales.

2. Principios.

3. Deberes.
4. Sistemas de datos personales.
5. Medidas de seguridad.
6. Procedimientos y sanciones/ Derechos ARCO (acceso, rectificación, cancelación y oposición).
7. Medios de defensa.
8. La LGPDPPSO y sus Lineamientos.
9. Antecedentes, ¿A quién aplica? ¿Qué objeto tiene?
10. Inventario y Base de Datos
11. Análisis de brecha y de riesgo.
12. Funciones y obligaciones.
13. Avisos de Privacidad.

12. Plan De Trabajo



Se clasifica la información contenida en el Documento de seguridad concerniente al Plan de Trabajo, el Análisis de Riesgo y Análisis de Brecha de conformidad con el Criterio 1 del Anexo 3. Herramienta de Evaluación de la Guía antes mencionada, asimismo, con fundamento en los artículos 113, fracción XIII de la Ley General de Transparencia y Acceso a la Información Pública y artículo 110, fracción XIII de la Ley Federal de Transparencia y Acceso a la Información Pública