

MANUAL DE USUARIO DEL GENERADOR DE INVENTARIOS DE SISTEMAS DE TRATAMIENTOS DE DATOS PERSONALES Y DEL GENERADOR DE PLANES DE TRABAJO



Versión 1.1

Agosto de 2024

CONTENIDO

CONTENIDO	1
ACERCA DE LA HERRAMIENTA	3
Para la elaboración del inventario de datos personales.....	4
Para la elaboración del análisis de riesgos	5
Para la elaboración del análisis de brecha.....	6
Para la elaboración del plan de trabajo	6
ACERCA DE ESTE MANUAL	8
¿A quién va dirigido este manual?	8
Introducción	8
Confidencialidad de las respuestas	9
GLOSARIO	11
ACCIONES GENERALES	15
Acceso a la herramienta	15
Registro de usuario	15
1. Lea el aviso de privacidad	15
2. Registre su información	16
3. Active su cuenta.....	17
Recuperación de contraseña	18
Acceder al módulo recuperar contraseña	18
Eliminación de usuario	19
Ingreso al sistema	19
Validar credenciales.....	20
Modificar cuenta	21
Recomendaciones de uso de la herramienta	21
Menú fijo	22
Opciones de usuario	22
Previsualizar	23
Editar.....	24
Eliminar	25
Elementos del cuestionario dinámico	26
Barra de navegación	26
Elemento de ayuda	26
Botones de navegación.....	27
Información importante sobre las cajas de texto en preguntas abiertas.....	27
Mensaje de error	28
GENERADOR DE INVENTARIOS DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES	29

Mis inventarios	29
Elaborar nuevo inventario.....	30
Estructura	31
Módulo 1	31
Módulo 2	32
Módulo 5	33
Módulo 6	34
Módulo 7	34
Módulo 8	35
Módulo 9	35
Módulo 10	37
Módulo 11	37
Módulo 12	38
Módulo 13	39
Módulo 14	41
Módulo 15	41
Módulo 16	42
GENERADOR DE PLANES DE TRABAJO	43
Mis planes de trabajo.....	43
Elaborar nuevo plan de trabajo	44
Definir el alcance, contexto y objetivos del análisis de riesgos	45
Identificar los activos	46
Determinar el valor del activo	47
Identificar las amenazas	48
Valorar el riesgo.....	48
Estimar el riesgo a partir de la ocurrencia de la amenaza	49
Identificar las vulnerabilidades del activo	50
Acciones importantes a considerar para la realización del análisis de riesgos	51
Análisis de brecha	52
Resultados	52

ACERCA DE LA HERRAMIENTA

La herramienta informática Generador de Inventarios de Sistemas de Tratamientos de Datos Personales y Generador de Planes de Trabajo surge como un instrumento de apoyo para los sujetos obligados del sector público que tratan datos personales y a quienes estén interesados en elaborar un inventario de datos personales o bien generar un plan de trabajo a partir del análisis de riesgos y análisis de brecha conforme a las normativa en la materia del sector público.

La elaboración del inventario de activos, del análisis de riesgos, del análisis de brecha y de la generación del plan de trabajo son obligaciones que mandata la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en adelante Ley General) y los Lineamientos Generales de Protección de Datos Personales para el sector público (en adelante Lineamientos Generales), por lo que, esta herramienta contempla los contenidos mínimos indispensables conforme a lo dispuesto en dicho marco normativo.

Para la elaboración del inventario de datos personales

En esta etapa se busca documentar un listado de todos los sistemas de tratamiento físicos y electrónicos donde se efectúe tratamiento de datos y se realice una clasificación de todos los datos personales. Los sujetos obligados deberán elaborar un inventario de datos personales y de los sistemas de tratamiento, conforme a lo dispuesto en la Ley General y los Lineamientos Generales. Por ello se recomienda atender lo siguiente:

Artículo 33 de la Ley General:

“Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

I. [...]

II. [...]

III. Elaborar un inventario de datos personales y de los sistemas de tratamiento.”

Artículo 58 de los Lineamientos Generales:

“Con relación a lo previsto en el artículo 33, fracción III de la Ley General, el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales, considerando, al menos, los siguientes elementos:

- I. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;*
- II. Las finalidades de cada tratamiento de datos personales;*
- III. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;*
- IV. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;*
- V. La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;*
- VI. En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable; y*
- VII. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.”*

Artículo 59 de los Lineamientos Generales:

“Aunado a lo dispuesto en el artículo anterior de los presentes Lineamientos generales, en la elaboración del inventario de datos personales el responsable deberá considerar el ciclo de vida de los datos personales conforme lo siguiente:

- I. La obtención de los datos personales;*

- II. El almacenamiento de los datos personales;
- III. El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;
- IV. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;
- V. El bloqueo de los datos personales, en su caso, y
- VI. La cancelación, supresión o destrucción de los datos personales.

El responsable deberá identificar el riesgo inherente de los datos personales, contemplando su ciclo de vida y los activos involucrados en su tratamiento, como podrían ser hardware, software, personal, o cualquier otro recurso humano o material que resulte pertinente considerar.”

Para la elaboración del análisis de riesgos

Debe contarse con un análisis de riesgos de datos personales para identificar peligros y estimar los riesgos, considerando las amenazas y vulnerabilidades para los datos personales y los recursos involucrados en su tratamiento. Pueden ser, de modo enunciativo mas no limitativo: hardware, software, personal del responsable, entre otros.

Conforme a la Ley General y los Lineamientos Generales, para el tema de análisis de riesgos, los sujetos obligados deberán atender lo siguiente:

Artículo 33 de la Ley General:

“Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

I. [...]

II. [...]

III. [...]

IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de modo enunciativo mas no limitativo, hardware, software, personal del responsable, entre otros;”

Artículo 60 de los Lineamientos Generales:

“Para dar cumplimiento al artículo 33, fracción IV de la Ley General, el responsable deberá realizar un análisis de riesgos de los datos personales tratados considerando lo siguiente:

- I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;*
- II. El valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida;*

- III. *El valor y exposición de los activos involucrados en el tratamiento de los datos personales;*
- IV. *Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y*
- V. *Los factores previstos en el artículo 32 de la Ley General.”*

Para la elaboración del análisis de brecha

Esta etapa consiste en identificar la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales, en ese sentido, el marco normativo prevé que se identifiquen los siguientes elementos:

Artículo 33 de la Ley General:

“Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

- I. [...]
- II. [...]
- III. [...]
- IV. [...]
- V. *Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;”*

Artículo 61 de los Lineamientos Generales:

Con relación al artículo 33, fracción V de la Ley General, para la realización del análisis de brecha el responsable deberá considerar lo siguiente:

- I. *Las medidas de seguridad existentes y efectivas;*
- II. *Las medidas de seguridad faltantes; y*
- III. *La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.”*

Para la elaboración del plan de trabajo

Una vez realizado el análisis de riesgos y el de brecha, debe priorizarse en la atención o tratamiento a los riesgos de mayor nivel, de los activos más críticos. De las medidas seleccionadas en el análisis de brecha, deberán establecerse los plazos, los pasos a seguir y las personas responsables de implementarlas, es decir, debe definirse un plan de trabajo. Por ello, en atención a la Ley General y Lineamientos Generales, los sujetos obligados deberán atender lo siguiente:

Artículo 33 de la Ley General:

“Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

- I. [...]

II. [...]

III. [...]

IV. [...]

V. [...]

VI. *Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;*

“Artículo 62 de los Lineamientos Generales:

De conformidad con lo dispuesto en el artículo 33, fracción VI de la Ley General, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar, de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.

Lo anterior, considerando los recursos designados, el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.”

En ese sentido, lo que se busca con esta herramienta es coadyuvar particularmente a sujetos obligados del sector público en la elaboración del documento de seguridad, específicamente en la integración de al menos cuatro de sus siete contenidos, así como a Responsables del sector privado como parte de la implementación de un sistema de gestión de seguridad de la información, específicamente en tres de los nueve pasos de implementación, lo anterior, a fin de documentar el cumplimiento del deber de seguridad conforme a lo descrito anteriormente.

ACERCA DE ESTE MANUAL

El manual de usuario de la herramienta informática *Generador de Inventarios de Sistemas de Tratamientos de Datos Personales y Generador de Planes de Trabajo* proporciona a los usuarios la información necesaria para operar la herramienta de manera correcta, orientando a los usuarios sobre la usabilidad de la herramienta, los elementos que la comprenden y brindar información que contextualice las preguntas que integran el cuestionario dinámico y ejemplifiquen que tipos de respuesta se esperan para cada pregunta.

¿A quién va dirigido este manual?

El presente manual está dirigido a los Responsables o Encargados de algún tratamiento de datos personales del sector público, así como personas propietarias o custodias de algún tratamiento de datos personales, incluso aquellas personas que estén interesadas en elaborar un inventario de algún tratamiento de datos personales o bien generar un plan de trabajo a partir del análisis de riesgos y análisis de brecha que se hayan registrado satisfactoriamente como usuarios en la herramienta Generador de Inventarios y Generador de Planes de Trabajo.

Se recomienda que los usuarios estén familiarizados con el uso de herramientas informáticas o aplicaciones web, tener conocimiento sobre los tratamientos y el ciclo de vida de los datos personales que va a trabajar, así como conocimientos básicos respecto a la seguridad de la información, debido a que deberá atender diversos cuestionamientos técnicos que requieren de conocimientos previos para abordar de mejor manera las preguntas de los cuestionarios dinámicos.

Introducción

Esta aplicación web es compatible con los navegadores de Internet más utilizados (Chrome, Firefox, Edge, Safari), permite a los Responsables de tratamientos de datos personales en el ejercicio de sus atribuciones generar los documentos concernientes a inventarios de sistemas de tratamiento y planes de trabajo a partir de un cuestionario automatizado que generará un archivo en formato PDF.

Es importante señalar que la utilidad del documento que se genere mediante el uso de esta aplicación depende directamente del usuario ya que, el cuestionario compila la información a través de las respuestas al cuestionario base, dependiendo completamente de la veracidad de las respuestas que este brindará.

Finalmente, dentro de la herramienta identificará elementos informativos que lo orientarán con información de interés que contextualizara a que se refiere cada pregunta y en algunos casos, brinda ejemplos de apoyo sobre lo que se espera de respuesta.

Esta herramienta se divide en dos apartados:

- **Generador de Inventarios**

Que incluye los elementos mínimos previstos en la Ley General y los Lineamientos Generales.

- **Generador de Planes de Trabajo**

Incluye preguntas que permiten realizar una valoración del riesgo al que se expone el tratamiento de datos personales para que, a partir de los escenarios de vulneración que sean definidos se puedan identificar controles o medidas de seguridad aplicables al contexto en el que sucede dicho tratamiento. Como se ha mencionado, la herramienta se separa en las siguientes partes:

- **Parte 1- Análisis de riesgos**, contempla elementos mínimos necesarios para la realización de un análisis de riesgos a partir de la valoración cuantitativa y cualitativa de los activos (datos personales), valorando su Confidencialidad, Integridad y Disponibilidad, permitiendo identificar amenazas y vulnerabilidades para cada tipo de activo que se vaya analizando, permitiendo tener elementos para identificar escenarios de vulneración a partir de las respuestas del usuario, conociendo el posible daño que pueden sufrir los activos en caso de la materialización de un incidente de seguridad.
- **Parte 2- Análisis de brecha**, aquí podrá encontrar un listado de controles para identificar si cuenta con medidas de seguridad físicas, técnicas o administrativas para el resguardo de los activos (datos personales), esta valoración permitirá identificar si existe una brecha de seguridad entre los controles de seguridad que debe implementar para proteger los activos (datos personales) que tiene a su resguardo.

De esta manera, al compilar y valorar la información proporcionada por el usuario, identificando los elementos mínimos que debe incluir un análisis de riesgos y un análisis de brecha, el usuario obtendrá un documento que le permitirá tener un panorama general respecto al nivel de riesgo al que se están enfrentando sus activos, permitiendo asociar amenazas y vulnerabilidades en escenarios que contarán con valoraciones cuantitativas y cualitativas a partir de la probabilidad de ocurrencia y el impacto que se tendría en caso de materializarse el incidente, adicionalmente, el usuario podrá identificar algunos controles de seguridad, que le permitirán tener un panorama respecto a las medidas de seguridad específicas necesarias para atender el contexto general del control identificado y así salvaguardar los activos (datos personales) que trata a partir de los resultados sugeridos por la herramienta

Confidencialidad de las respuestas

La información que proporcione el usuario será resguardada en una base de datos, la cual se encuentra configurada de tal manera que no es accesible para los administradores de la herramienta, deshabilitando la generación de copias o accesos a los contenidos de los cuestionarios dinámicos, por lo que, la información que proporcione el usuario solo podrá ser consultada y descargada desde la sesión del usuario.

El uso de la herramienta informática NO representa de ninguna manera la validación o visto bueno de las actividades correspondientes al cumplimiento del deber de seguridad, asimismo, en ninguna circunstancia podrá ser utilizada como evidencia o elemento que propicie una investigación o revisión a los sujetos obligados.

La herramienta informática sirve como apoyo para elaborar inventarios de sistemas de tratamientos de datos personales considerando los elementos mínimos previstos en el marco normativo y planes de trabajo a partir del análisis de riesgos y análisis de brecha, los cuestionarios dinámicos que integran la herramienta son una propuesta universal que no adopta de manera total ninguna recomendación



o estándar internacional, por lo que, los resultados del uso de la herramienta pueden ser complementados con la implementación de algún estándar o norma internacional en la materia.

GLOSARIO

Aceptación del riesgo: decisión informada para coexistir con un nivel de riesgo conocido.

Activo: en términos generales, un activo es cualquier elemento que representa un valor para una organización o sujeto obligado, acorde con la Real Academia Española (RAE) “valor” se define como a) grado de utilidad o aptitud de las cosas para satisfacer las necesidades o proporcionar bienestar o deleite y b) cualidad de las cosas, en virtud de la cual se da por poseerlas cierta suma de dinero o equivalente.

Específicamente en seguridad de la información, podemos encontrar dos tipos de activos:

- Los **activos primarios o de información**, son aquellos que corresponden a procesos de negocio y actividades, así como a información crítica de una organización. Ejemplos de procesos de negocio y actividades consideradas activos críticos o primarios son aquellos cuya pérdida o degradación hacen imposible cumplir con la misión de la organización o impiden el cumplimiento con requerimientos contractuales, legales o regulatorios. La información considerada como activo primario es por ejemplo toda la información vital para la operación de la organización, la información personal especificada dentro del marco regulatorio de privacidad e información estratégica que representa una ventaja competitiva para la organización. En este caso en particular, los activos de información son los datos personales.
- Los **activos de soporte** son aquellos que apoyan a los activos primarios para su operación y consisten en: equipo de cómputo (hardware), aplicaciones (software), equipos de comunicaciones, personal, instalaciones y estructura organizacional.

Análisis de riesgos: actividad que permite identificar los peligros y evaluar el nivel de riesgo hacia los datos personales.

Las metodologías de análisis de riesgos establecen un proceso sistemático que consiste en generar escenarios de riesgos identificando y correlacionando todos los elementos que intervienen en el riesgo como lo son activo (que en el presente contexto se refiere a los datos personales y los sitios en donde estos son resguardados), amenazas, vulnerabilidades, controles existentes e impactos o consecuencias. Una vez creados los escenarios de riesgo, se procede a evaluar cualitativa o cuantitativamente el riesgo mediante el establecimiento de parámetros como la probabilidad de ocurrencia, el nivel de impacto o el beneficio para el atacante.

Amenaza: se define como la circunstancia o evento con la capacidad de causar daño a una organización.

Áreas: instancias de los sujetos obligados revistas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o pueden contar, dar tratamiento, y ser responsables, encargadas o custodias de los datos personales.

Bases de datos: conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Bloqueo: la identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de estas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido este, se procederá a su cancelación en la base de datos que corresponda.

Confidencialidad: propiedad de la información para no estar a disposición o ser revelada a personas, entidades o procesos no autorizados.

Compartir el riesgo: proceso donde se involucra a terceros para mitigar la pérdida generada por un riesgo en particular, sin que el dueño del activo afectado reduzca su responsabilidad.

Comunicar el riesgo: proceso en el que se comparte o intercambia información entre los involucrados en el tratamiento del riesgo.

Custodios: son aquellas personas servidoras públicas o no que tienen una responsabilidad funcional sobre los activos, por ejemplo, responsables del departamento de datos, administradores de sistemas o responsables de un proceso o proyecto específico.

Datos personales: cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Datos sensibles: aquellos que se refieran a la esfera más íntima de la persona titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Documento de seguridad: instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Disponibilidad: propiedad de un activo para ser accesible y utilizable cuando lo requieran personas, entidades o procesos autorizados.

Encargado: la persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

Evitar el riesgo: acción para retirarse de una situación de riesgo o decisión para no involucrarse en ella.

Identificar el riesgo: proceso para encontrar, enlistar y describir los elementos del riesgo.

Impacto: una medida del grado de daño a los activos o cambio adverso en el nivel de los objetivos de una organización.

Incidente: escenario donde una amenaza explota una vulnerabilidad o conjunto de vulnerabilidades.

Integridad: la propiedad de salvaguardar la exactitud y completitud de los activos.

Probabilidad: es un cálculo que permite conocer el nivel de certeza respecto a la ocurrencia de un evento, es decir, la medición de la frecuencia con la que es posible obtener un cierto resultado en el marco de un procedimiento de carácter aleatorio.

Reducir el riesgo: acciones tomadas para disminuir la probabilidad, las consecuencias negativas, o ambas, asociadas al riesgo.

Remisión: toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado dentro o fuera del territorio mexicano.

Responsable: los sujetos obligados a que se refiere el artículo 1º de la Ley General que deciden sobre el tratamiento de datos personales.

Retención del riesgo: proceso en el que se acepta formalmente la pérdida generada por un riesgo en particular, esta acción implica monitoreo constante del riesgo retenido.

Riesgo: combinación de la probabilidad de un evento y su consecuencia desfavorable.

Riesgo de seguridad: Es la combinación de la probabilidad de un evento y su consecuencia desfavorable. Para la mejor comprensión, se puede definir como la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas.

Riesgo inherente: es el riesgo intrínseco al activo, sin tener en cuenta las medidas de seguridad implementadas.

Riesgo residual: el riesgo remanente después de tratar el riesgo.

Seguridad de la información: es la preservación de la confidencialidad, integridad y disponibilidad de la información, así como otras propiedades delimitadas por la normatividad aplicable.

Sistema de Gestión de Seguridad de Datos Personales (SGSDP): Sistema de Gestión general para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios básicos de licitud, consentimiento información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad previstos en la Ley General, los Lineamientos Generales, normatividad secundaria y cualquier otro principio que la buena práctica internacional estipule en la materia.

Sujeto Obligado: son sujetos obligados por la Ley General, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, Órganos Autónomos, Partidos Políticos, Fideicomisos y Fondos Públicos.

Titular: la persona física a quien corresponden los datos personales.

Tratamiento: cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Transferencia: toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta al titular, del responsable o del encargado.

Tratar el riesgo: proceso que se realiza para modificar el nivel de riesgo.

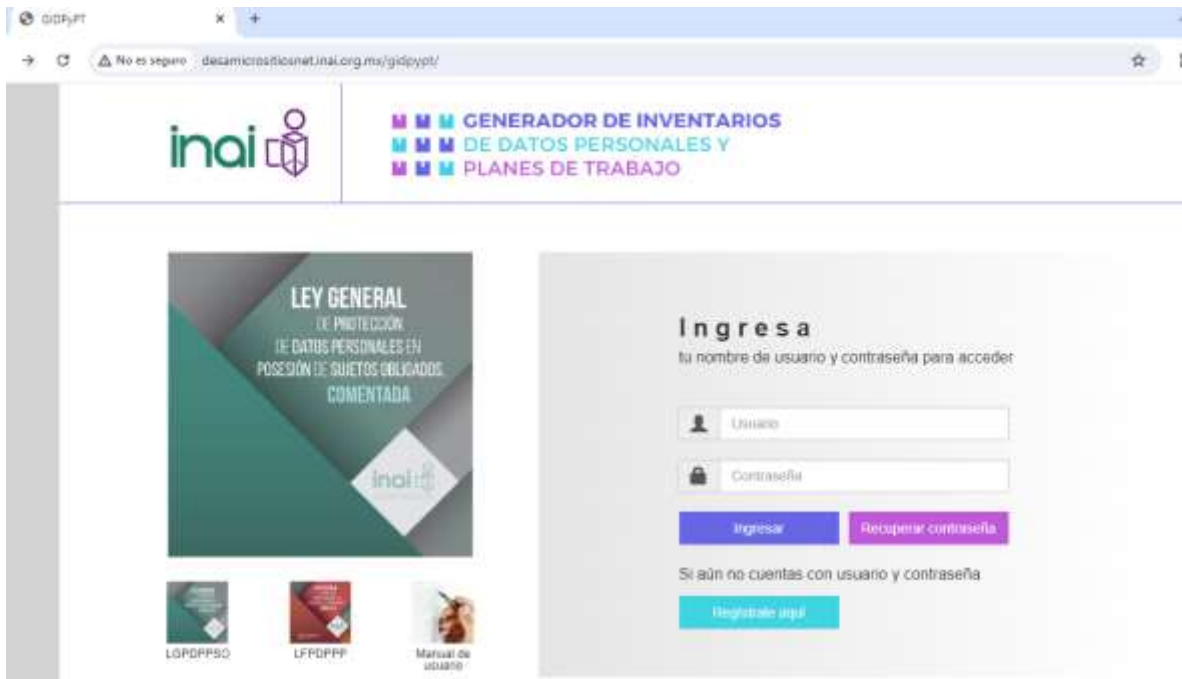
Valorar el riesgo: proceso para asignar valores a la probabilidad y consecuencias del riesgo.

Vulnerabilidad: falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o varias amenazas.

ACCIONES GENERALES

Acceso a la herramienta

Para ingresar a la Herramienta generadora de inventario de datos, se deberá ingresar en la siguiente liga: <http://desamicrositiosnet.inai.org.mx/gidpypt/>



Las acciones que deben realizar para generar una cuenta en esta herramienta son:

Registro de usuario

El registro de usuario se refiere al alta y validación de identidad de una persona a partir de su correo electrónico. Si es su primera vez en la herramienta y no cuenta con un usuario, deberá realizar los siguientes pasos:

1. Lea el aviso de privacidad

Aparecerá una ventana emergente la cual contendrá el aviso de privacidad correspondiente al registro en la herramienta, una vez leído y comprendido el contenido del aviso, si está de acuerdo, confirme que desea crear su cuenta dando clic en el ícono identificado con una "X".



Imagen 1. Aviso de privacidad


2. Registre su información

Una vez leído y comprendido el aviso de privacidad, deberá llenar un cuestionario con la siguiente información:



- **Nombre de usuario**, el nombre de usuario deberá contener entre 4 y 20 caracteres, es importante que recuerde su nombre de usuario ya que este es necesario para acceder a la herramienta, este le será de utilidad al querer recuperar su contraseña o al dar de baja su cuenta
- **Contraseña**, deberá definir una contraseña de entre 6 a 20 caracteres alfanuméricos, cuya composición incluya al menos una letra mayúscula, un número y un carácter especial.
- **Correo electrónico**, deberá ingresar un correo electrónico que utilice frecuentemente, ya que, le llegará un enlace de validación para finalizar con el registro de su usuario.
- **Tamaño de organización o dependencia**, para fines estadísticos deberá seleccionar alguna de las opciones que aparecen en esta pregunta.
- **Comunicación mediante correo electrónico**, si está de acuerdo con recibir información, al señalar la opción “Sí” en esta pregunta, podrá recibir información relacionada con el GIDPyPT (como novedades y encuestas de calidad) en su correo electrónico.



Imagen 2. Pantalla de registro

El ícono de ayuda , desplegará información de interés cuando pase el cursor sobre este, la información de apoyo busca orientarlo respecto a los datos que debe ingresar para responder esa pregunta.

Es importante que verifique que haya ingresado los datos solicitados y que éstos sean correctos, no obstante, los datos ingresados podrán ser modificados más adelante desde su panel de control de usuario.

Para finalizar su registro deberá dar clic en el botón , esto lo dirigirá a la pantalla de inicio de la herramienta. En caso de que decida no registrarse, puede dar clic en el botón , con lo que eliminará los datos que haya ingresado y la herramienta lo dirigirá a su página de inicio.

3. Active su cuenta

Una vez aceptado y completado el formulario de registro, el sistema le hará llegar al correo electrónico que registró un correo, el cual incluirá un enlace para que pueda validar su cuenta, una vez que haya realizado estos pasos, diríjase a la bandeja de entrada de su correo y busque el mensaje de activación de cuenta, de clic en el enlace para validar su registro.



Imagen 3. Ejemplo de correo de activación de cuenta

Es importante que tenga en cuenta que si no activa su cuenta no podrá usar la herramienta, por lo que, si han pasado 10 minutos y no ha recibido el correo de activación, deberá dirigirse a su bandeja de correos no deseados o spam y corroborar su existencia en alguna de estas bandejas, de no encontrarse, podrá enviar un correo informando su incidencia a: gidpypt@inai.org.mx.

Recuperación de contraseña

Cuando requiera recuperar su contraseña, deberá realizar lo siguiente:

Acceder al módulo recuperar contraseña

Desde la página de inicio deberá acceder al módulo de *Recuperar contraseña*, en donde tendrá que realizar lo siguiente:

1. Ingresar el correo electrónico registrado en la herramienta informática



Imagen 4. Pantalla del apartado de recuperación de contraseña

2. Ingresar los datos que le solicita la herramienta web, para recuperar su contraseña, es importante que recuerde el correo con el que haya registrado en su cuenta, si tiene algún inconveniente, podrá enviar un correo informando su incidencia a: gidpypt@inai.org.mx.
3. Ingrese al enlace de restablecimiento de contraseña, el sistema automatizado le hará llegar un correo que incluirá un enlace que lo dirigirá al módulo de recuperación de contraseña, esta opción le permitirá añadir una nueva contraseña, la cual deberá ser de entre 4 a 20 caracteres alfanuméricos, cuya composición debe incluir al menos una letra mayúscula, un carácter especial y un número.



Imagen 5. Vista del apartado de recuperación de contraseña

Recuerde que el proceso de activación es similar al de recuperación de contraseña respecto al envío de enlaces al correo electrónico registrado para realizar el proceso solicitado, por lo que, en caso de que no encuentre el correo con el enlace respectivo para realizar el procedimiento solicitado podrá enviar un correo informando su incidencia a: gidpypt@inai.org.mx.

Eliminación de usuario

Para eliminar su cuenta de usuario deberá enviar un correo electrónico a la dirección electrónica gidpypt@inai.org.mx.

Dicho correo electrónico deberá tener como asunto “**eliminación de cuenta**” y deberá ser enviado desde la cuenta de correo electrónico que desea dar de baja.

Ingreso al sistema

Al ingresar al enlace de la herramienta informática Generador de Inventarios de datos personales y Planes de Trabajo encontrará la página de acceso en dónde podrá observar las siguientes secciones:

- **Apartado de consulta de documentos**, en este apartado podrá consultar lo siguiente: (i) la Ley Federal de Protección de Datos Personales en Posesión de Particulares, a la (ii) Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y el (iii) Manual de usuario.
- **Ingreso a la herramienta**, en este apartado podrá ingresar su nombre de usuario y contraseña para acceder a su sesión de trabajo.
- **Recuperación de contraseña**, este apartado lo dirigirá al módulo que le permitirá recuperar su contraseña a partir del correo electrónico registrado.
- **Registro**, este apartado lo dirigirá al módulo de registro a la herramienta.



Imagen 6. Vista de página de acceso a la herramienta

Validar credenciales


Deberá ingresar su usuario y contraseña en sus respectivos campos de captura, posteriormente deberá dar clic al ícono *Ingresar*.

Cuando el sistema valide la combinación de los campos de usuario y contraseña con los registros de la herramienta aparecerá la pantalla de trabajo.



Imagen 7. Vista general de página de inicio de la herramienta

Modificar cuenta

Al ingresar en la pestaña  accederá a una sección de la herramienta que le permite realizar los siguientes cambios al usuario que dio de alta en la herramienta:

- Cambiar el nombre de usuario
- Cambiar la contraseña sin tener que acceder al módulo de recuperación de contraseña
- Modificar el correo asociado a la cuenta registrada



Imagen 8. Vista general de Modificar cuenta de usuario

Una vez realizados los cambios requeridos, deberá dar clic en el botón modificar para guardar los cambios que haya realizado, si da clic en los botones limpiar o cancelar, no se guardarán los cambios que haya realizado en la sección.

Recomendaciones de uso de la herramienta

Antes de comenzar la elaboración de un inventario de tratamiento de datos personales o de un plan de trabajo es importante que tome en cuenta los siguientes aspectos:

1. Para generar sus inventarios de sistemas de tratamiento y/o sus planes de trabajo será necesario que conteste las preguntas del cuestionario dinámico de la herramienta. Esto le puede tomar un tiempo estimado de más de una hora.
2. Es importante que tome en cuenta que en caso de que no sea posible concluir su inventario o plan de trabajo en una sola sesión, la información quedará guardada en la herramienta, por lo que podrá finalizarlo posteriormente desde la opción Editar.
3. En caso de que haya cerrado su sesión sin terminar su inventario o plan de trabajo, la herramienta le permitirá continuar con éste, a través de la opción Editar, la cual le permitirá continuar a partir de la última sección que tenía activa, permitiéndole añadir las secciones faltantes sección por sección. Para más detalle visite la sección Editar.
4. El sistema está configurado para que a los 25 minutos de inactividad se cierre la sesión por seguridad de su información. Para que pueda ver cuál es su tiempo restante antes de que el sistema cierre su sesión, podrá ver el temporizador ubicado debajo del banner superior de la herramienta



Imagen 9. Vista de menú fijo

- Las preguntas que ha contestado se guardarán cuando de clic en el botón o en el botón , los cuales se encuentran configurados para navegar entre las diferentes secciones del cuestionario dinámico. Es importante que considere que, si se encontraba en una sección y había contestado parcialmente las preguntas de ésta y por alguna razón se cerró su sesión, el sistema no registrará estos cambios ya que solo podrá ver las respuestas de las secciones anteriores a la sección en la que se quedó.
- En caso de presentar una falla durante el uso de la herramienta, podrá comunicarla mediante correo electrónico a la cuenta gidpypt@inai.org.mx, se le recomienda describir la situación que presenta la herramienta o el error observado y de ser posible incluir capturas de pantalla.

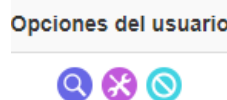
Menú fijo

Al iniciar sesión correctamente podrá identificar en la página de inicio y durante toda la navegación en la herramienta un menú en la parte superior de la pantalla con los siguientes íconos de acceso directo a contenidos:

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
 - Manual de usuario,
 - Regreso a la página de inicio
 - Salir de la herramienta
- Tu sesión por inactividad termina en: 0:24:22 minutos. Cronometro de 25 minutos que por seguridad cierra la sesión de usuario cuando identifica inactividad en el uso de la herramienta

Opciones de usuario

En la vista de la pantalla de la sección **Mis Inventarios** y **Mis Planes de Trabajo**, podrá ver que los cuestionarios que ha llenado para crear inventarios o planes de trabajo están acomodados en una tabla que describe actividades a los inventarios o planes de trabajo que ya se crearon.



Previsualizar

Esta opción le permite ver en formato HTML un inventario o plan de trabajo elaborado en la herramienta. Así mismo, permite exportar el inventario en formato Excel o el inventario en formato PDF.

Mis inventarios Elaborar nuevo inventario Mis planes de trabajo Elaborar nuevo plan de trabajo Modificar cuenta de usuario

Previsualización

Mis inventarios Elaborar nuevo inventario Mis planes de trabajo Elaborar nuevo plan de trabajo Modificar cuenta de usuario

Previsualización

Unidad administrativa: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
 Fecha de elaboración o última actualización: 29/04/2022 10:44:28 a. m.
 Nombre del tratamiento (proceso): REGISTROS
 Fundamento jurídico que habilita el tratamiento: XX FRACCIÓN SEGUNDA DEL ARTICULO 159 DE LA LOPDPPSO
 Atribuciones de la unidad administrativa para realizar el tratamiento: Atribuciones conferidas en el manual organizacional

Medio de elaboración de los datos personales (1)	Tipo de transferencia de los datos personales, en su caso (2)	Finalidades de la transferencia recibida, en su caso (3)	Límites de datos personales (4)	Servicio (5)	Formato de la base de datos (6)	Ubicación base de datos (7)	Sección de archivos (8)	
Señalar el o los medios a través de los cuales se contienen los datos personales en este tratamiento. Si se trata de un medio, se deberá indicar el medio por el que se realiza.	Describir el medio, por ejemplo la fuente de acceso: público, URL, correo, sistema, teléfono, entre otros.	Si en la columna 1 se indicó que los datos personales se reciben por transferencia, señalar el nombre del tercero o tercero que realizó la transferencia.	Si en la columna 1 se indicó que los datos personales se reciben por transferencia, señalar para qué finalidad se requiere dicha transferencia. De darse, utilizar la misma fila para indicar qué finalidad se requiere.	Indicar cada uno de los datos personales que se tratarán, sus categorías, uno por fila.	Señalar si el dato personal es sensible o no.	Señalar el o los formatos en los que se encuentra la base de datos del tratamiento.	Señalar la ubicación de la base de datos. Si se trata de más de una, se deberá indicar una por fila.	Indicar clave de identificación de la sección a la que corresponde el tratamiento.

Imagen 10. Vista de previsualización de un inventario

SECCIÓN I. DEFINICIÓN DE ALCANCE Y OBJETIVOS Y CONTEXTO

Alcance de su análisis de riesgos y análisis de brecha: Sistema de tratamiento del Concurso para ser Comisionada y Comisionado Infantil y formar parte del Pleno Niñas y Niños 2022

Objetivo de su análisis de riesgos y análisis de brecha: Tener identificados y ponderar los riesgos y brecha de seguridad a la que se enfrentan los activos que comprenden la base de datos del Concurso para ser Comisionada y Comisionado Infantil y formar parte del Pleno Niñas y Niños 2022

Contexto de la evaluación y tratamiento de riesgos: El tratamiento del Concurso para ser Comisionada y Comisionado Infantil y formar parte del Pleno Niñas y Niños 2022 abarca desde la recopilación de archivos y datos en la plataforma controlada por el INAI, el envío de videos a jurados, el proceso de evaluación y la publicación de videos ganadores

Criterios de aceptación de riesgos: Nivel de riesgo medio a bajo

Actividades a realizar a partir del nivel de riesgo: Reducción de riesgos hasta tratar de llegar a un nivel de riesgo bajo

Criterios de impacto: Vulneraciones de seguridad

Criterios para la evaluación de riesgos: Criticidad de activos involucrados en el tratamiento

SECCIÓN II. ACTIVOS DE INFORMACIÓN O DATOS PERSONALES

Nombre del tratamiento de datos personales: Sistema de tratamiento del Concurso para ser Comisionada y Comisionado Infantil y formar parte del Pleno Niñas y Niños 2022

Soporte en el que se encuentra tratamiento de datos personales: Físico y electrónico

Lugar donde se encuentra su tratamiento de datos personales: Dentro de las instalaciones de la institución u organización

Dimensión	Valor cuantitativo	Valor asignado	Tipo de datos personales identificado en su tratamiento
Integridad	2	Medio	
Disponibilidad	3	Alto	
Confidencialidad	3	Alto	datos de contacto, datos de identificación, datos personales de menores, copias de documentos oficiales (acta, identificación, boletas)

Imagen 11. Vista de previsualización de un plan de trabajo

Editar

Esta opción le permite modificar un inventario o un plan de trabajo por sección, únicamente actualiza los datos de la sección que va a modificar sin alterar el resto del contenido.

Mis inventarios
Elaborar nuevo inventario
Mis planes de trabajo
Elaborar nuevo plan de trabajo
Modificar cuenta de usuario

Modificar Inventario
Folio: 00000024

Elija el módulo a modificar:

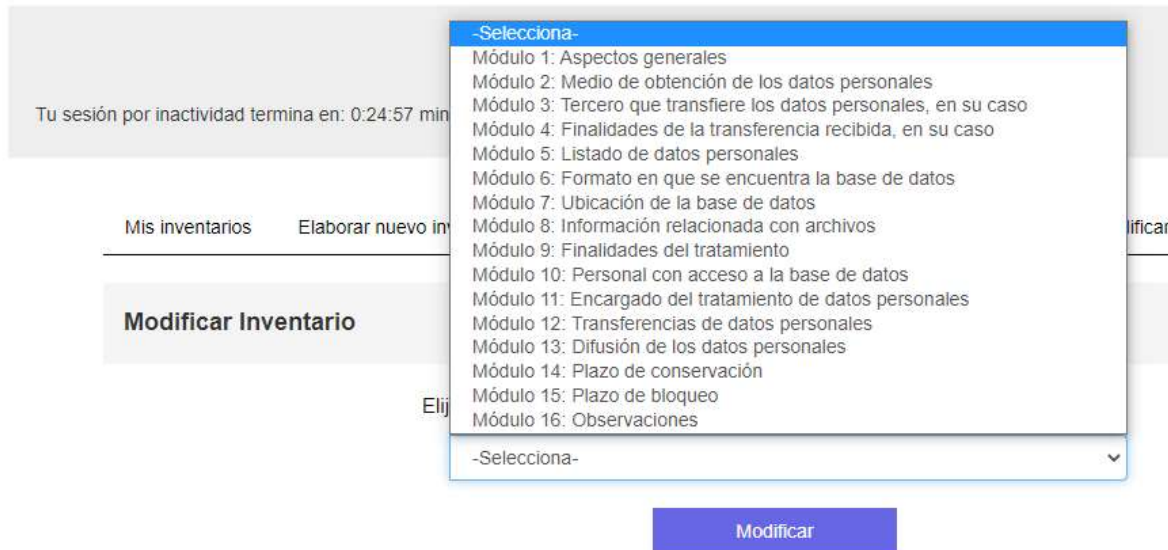


Imagen 12. Vista de modificar inventario

Eliminar

Esta opción le permite eliminar cualquier inventario o plan de trabajo, antes de eliminarlo de manera definitiva, el sistema le solicitará que confirme si quiere eliminarlo.

Es importante que considere que, una vez eliminado el inventario o plan de trabajo correspondiente, no existe la posibilidad de recuperar la información de éste, por lo que, queda eliminado de manera permanente del sistema.



Elementos del cuestionario dinámico

Los elementos que podrá identificar al elaborar un inventario o un plan de trabajo son:

Barra de navegación

La barra de navegación permite identificar en qué sección del cuestionario se encuentra y que secciones le faltan por atender.



Elemento de ayuda

Identifique los íconos , los cuales podrá encontrar antes de algunas preguntas, estos contienen información de apoyo que le orientarán en caso de requerir un contexto o información en particular para responder. La forma de visualizar esta información es pasar el cursor sobre el icono y la información aparecerá en una ventana emergente

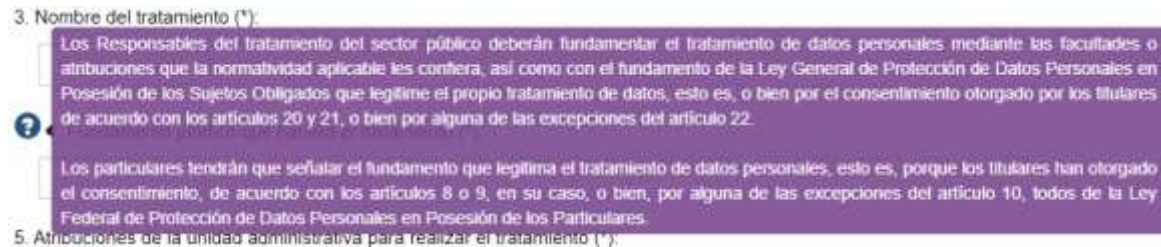


Imagen 13. Ejemplo de elemento informativo en el Generador de Inventarios

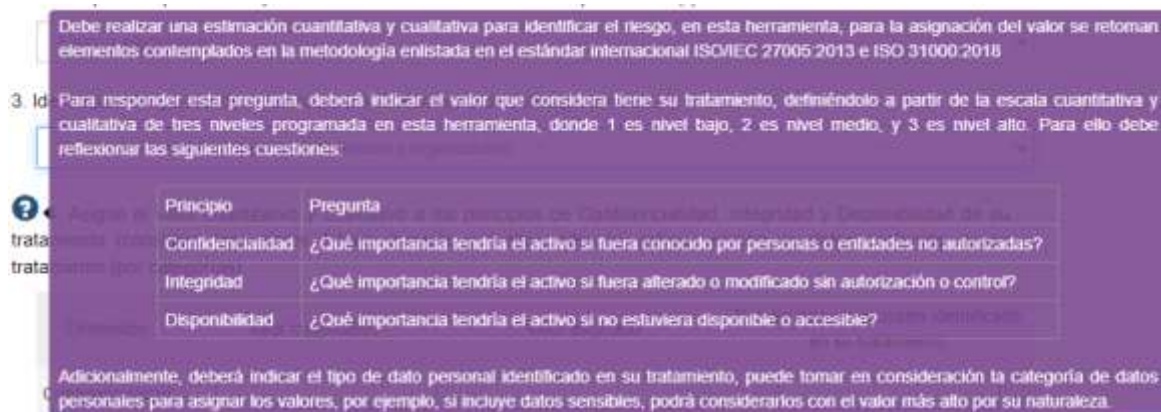






Imagen 14. Ejemplo de elemento informativo en el Generador de Planes de Trabajo

Botones de navegación

Cuando comience a elaborar un inventario o sistema de tratamiento de datos personales a partir de la sección 1, aparecerán los botones de navegación, mismos que se describen a continuación:

- Botón Siguiente , permite avanzar a la sección siguiente del cuestionario dinámico validando el formato de respuesta y verificando que se hayan contestado las preguntas que conforman la sección que se está respondiendo, además de guardar la información que haya contestado en la sección activa, por lo que, en caso de que el sistema encuentre una incongruencia o que falta información por contestar, aparecerá un mensaje en color rojo indicándole la incidencia que detectó el sistema.

• El sector es obligatorio.

- Botón Anterior , permite regresar a la sección anterior del cuestionario dinámico, guardará las respuestas que haya respondido sin validarlos.
- Botón Limpiar , permite eliminar las respuestas de una sección completa sin guardar cambios.
- Botón Guardar , este botón aparece cuando se encuentra en la última sección del cuestionario, sin importar si se trata de un inventario o un plan de trabajo, este botón guarda sus Inventarios y Planes de trabajo y se lo muestra en formato HTML, adicionalmente, le habilita la opción de descargar el archivo en formatos PDF para el plan de trabajo y Excel para el inventario de datos.

Información importante sobre las cajas de texto en preguntas abiertas

El cuestionario dinámico incluye preguntas en las que deberá contestar en cajas de texto (ver imagen), es importante que tome en cuenta que la herramienta informática actualmente se encuentra programada para guardar un máximo de 3,000 caracteres, por lo que se recomienda no exceder esta capacidad a fin de no generar un error en la herramienta que impida validar la información. En caso de que la información que desee agregar exceda estos caracteres, podrá incluir el texto directamente al archivo descargable que se genera cuando termina sus cuestionarios dinámicos.

1. Espacio libre para hacer aclaraciones y precisiones:



Imagen 15. Ejemplo de cuadro de texto

Mensaje de error

Cuando la herramienta detecte una cantidad mayor de caracteres en sus cajas de texto, aparecerá un mensaje de error.

Server Error in '/' Application.

Runtime Error

Description: An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It could, however, be viewed by browsers running on the local server machine.

Details: To enable the details of this specific error message to be viewed on remote machines, please create a <customErrors> tag within a "web.config" configuration file located in the root directory of the current web application. This <customErrors> tag should then have its "mode" attribute set to "Off".

```


<!-- Web.Config Configuration File -->
<configurations>
  <system.web>
    <customErrors mode="Off"/>
  </system.web>
</configurations>
  
```

Notes: The current error page you are seeing can be replaced by a custom error page by modifying the 'defaultRedirect' attribute of the application's <customErrors> configuration tag to point to a custom error page URL.

```

<!-- Web.Config Configuration File -->
<configuration>
  <system.web>
    <customErrors mode="RemoteOnly" defaultRedirect="mycustompage.htm"/>
  </system.web>
</configuration>
  
```

Imagen 16. Ejemplo de error

En este caso, deberá identificar en su navegador el botón “regresar” (ver imagen), el cual se encuentra ubicado al lado derecho de la barra de direcciones del navegador y es identificado con el icono , una vez que haya identificado este icono, deberá dar clic en él, esta acción lo regresará a la sección en donde estaba a fin de que pueda modificar la cantidad de caracteres que haya ingresado en las cajas de texto (hasta 3,000 caracteres) y, pueda guardar los cambios de la sección y continuar trabajando con su inventario o plan de trabajo.

En caso de que haya cerrado su navegador, la herramienta habrá guardado el avance que haya tenido hasta una sección anterior a donde apareció el error, por lo que le recomendamos realizar lo que se indica en el párrafo anterior.

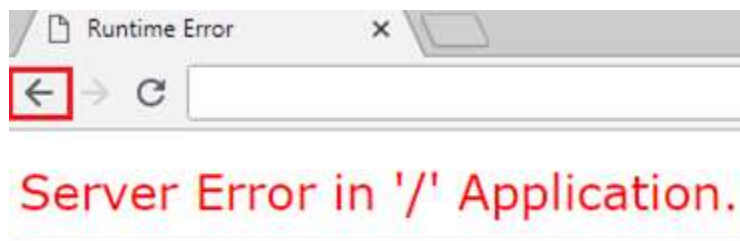


Imagen 17. Ejemplo de pantalla con error

GENERADOR DE INVENTARIOS DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

El escritorio de trabajo cuenta con dos pestañas dedicadas a generar inventarios

- Mis inventarios
- Elaborar nuevo inventario



Imagen 18. Vista general de Modificar cuenta de usuario

Mis inventarios

Esta sección Mis inventarios está programada para ser el home (inicio), es la primera pantalla que aparecerá al iniciar sesión y al dar clic en el icono home (inicio), en esta sección podrá visualizar los inventarios que vaya realizando identificados en una tabla con los siguientes rubros:

Mis inventarios			
Folio	Fecha de creación	Última fecha de modificación	Opciones del usuario
000000021	27/04/2022 11:42:45 a. m.	27/04/2022 11:44:30 a. m.	

Imagen 19. Tabla de opciones

- **Folio**, el sistema asigna de manera automática un número de folio a cada inventario.
- **Fecha de creación**, indica la fecha y hora de creación del inventario.
- **Fecha de modificación**, indica la fecha y hora de la última modificación, presentando los documentos más recientes al inicio.

- **Opciones del usuario**, en esta sección podrá previsualizar, editar o eliminar el inventario, para más detalle diríjase a la Sección *Opciones del Usuario* del presente manual.

Elaborar nuevo inventario

Para crear un nuevo inventario realice lo siguiente:

1. De clic en la opción Elaborar un nuevo inventario, se mostrará una ventana con información importante para el usuario en la cual deberá hacer clic en Aceptar para iniciar con el llenado del Cuestionario

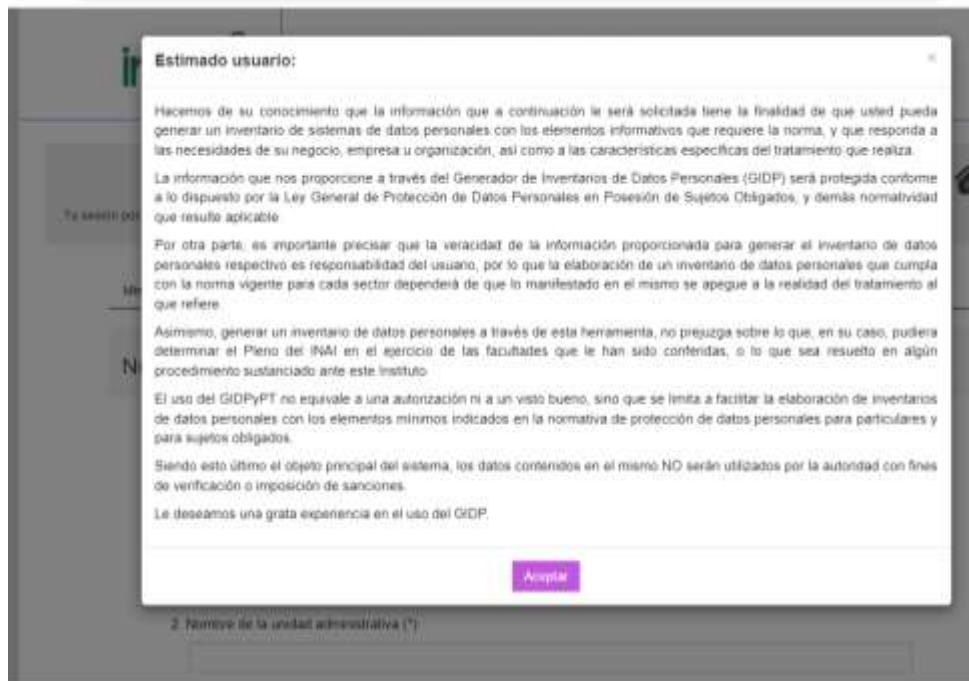


Imagen 20. Mensaje en ventana emergente

2. La herramienta mostrará preguntas por secciones, recuerde que las preguntas que inician con un (*) son preguntas obligatorias, si no cuentan con un (*) estas son opcionales.

1. Sector al que pertenecen (*):

Imagen 21. Ejemplo de pregunta obligatoria

El Generador de Inventarios de Sistemas de Tratamiento cuenta con 16 módulos que deberá llenar para conseguir un documento en formato Excel para su descarga:

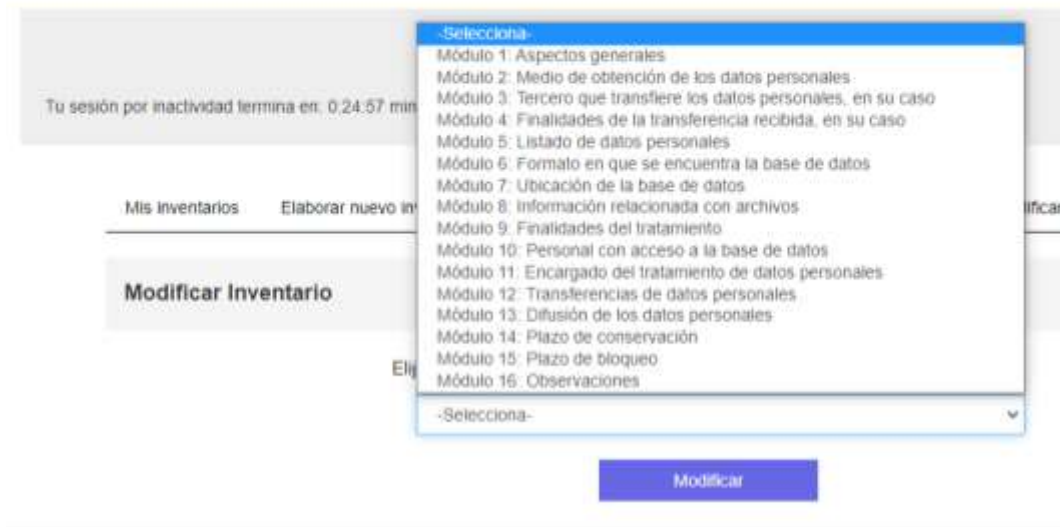


Imagen 22. Composición en secciones del cuestionario dinámico

Cuando haya llenado los 16 módulos del cuestionario, aparecerá la opción previsualizar que le permitirá descargar un documento en formato Excel y visualizar las respuestas que ingresó, en caso de no haber terminado el cuestionario, solo podrá editar las secciones.



Imagen 23. Ejemplo de vista de mis inventarios

Estructura

Módulo 1

En este apartado deberá llenar la siguiente información:

- Sector al que pertenecen
- Público
- Privado
- Nombre de la Unidad Administrativa a cargo o administradora del proceso o procedimiento que trata los datos personales.

- Nombre del tratamiento (proceso)
- Fundamento jurídico que habilita el tratamiento (Facultades)
- Atribuciones de la unidad administrativa para realizar el tratamiento

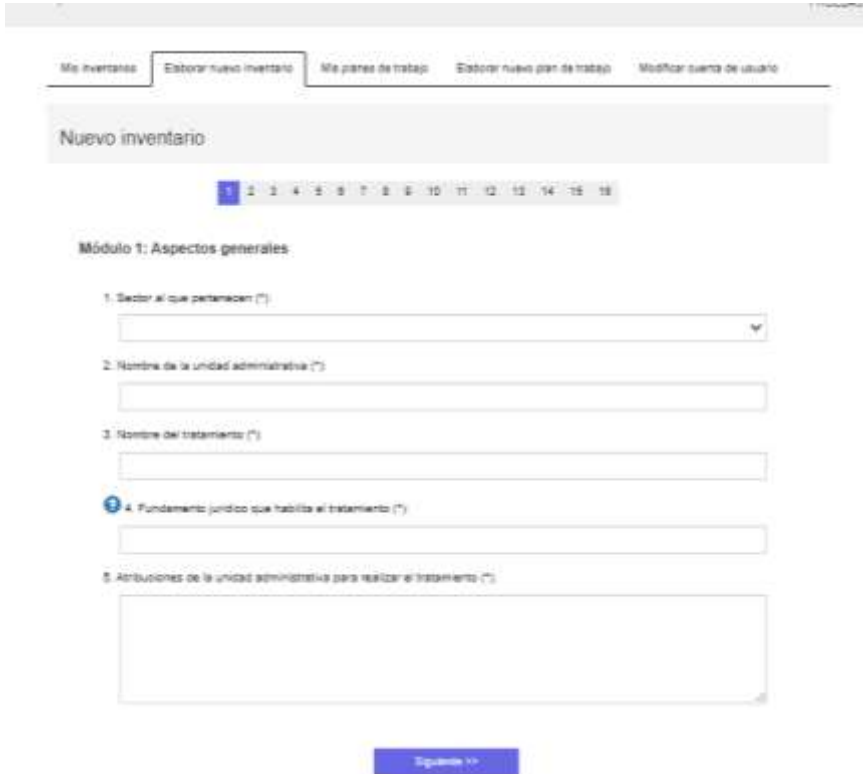


Imagen 24. Ejemplo de vista

Módulo 2

En este apartado se deberá indicar los medios de obtención de los datos personales y la descripción del medio

Nuevo inventario

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

Módulo 2: Medio de obtención de los datos personales.

1. Señalar el o los medios a través de los cuales se obtienen los datos personales en este tratamiento (*):
- De manera personal con la presencia física del titular de los datos personales o su representante, en su caso
 - Via telefónica
 - Correo electrónico
 - Internet o sistema informático
 - Escrito o formato presentado directamente en el Responsable del tratamiento de datos personales
 - Escrito o formato enviado al Responsable del tratamiento de datos personales por mensajería
 - Por transferencia
 - Fuente de acceso público
 - Otro

3. Descripción del medio, por ejemplo, la fuente de acceso público, URL, domicilio, número telefónico, entre otros, debe identificar si el medio de almacenamiento es físico o electrónico (*):

[<< Anterior](#) |
 [Siguiente >>](#)

Imagen 25. Ejemplo de vista

Módulo 5

Se refiere a Indicar cada uno de los datos personales que se tratan o sus categorías, así como si contienen datos sensibles o no.

Nuevo inventario

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

Módulo 5: Listado de datos personales

1. Indicar cada uno de los datos personales que se tratan o sus categorías (*):

Por tipo de dato |
 Por categoría

Datos de identificación y contacto

- Nombre
- Estado civil
- Registro Federal de Contribuyentes (RFC)
- Clave Única de Registro de Población (CURP)
- Lugar de nacimiento
- Fecha de nacimiento
- Nacionalidad
- Domicilio
- Teléfono particular
- Teléfono celular
- Correo electrónico
- Firma autógrafa
- Firma electrónica
- Edad
- Fotografía

Datos sobre características físicas

- Color de la piel
- Color del iris
- Color del cabello
- Señales particulares
- Estatura
- Peso
- Cicatrices
- Tipo de sangre

Datos biométricos

Imagen 26. Ejemplo de vista

Módulo 6

Se deberá señalar los formatos en los que se encuentre la base de datos

- Electrónica
- Física
- Fisca y electrónica

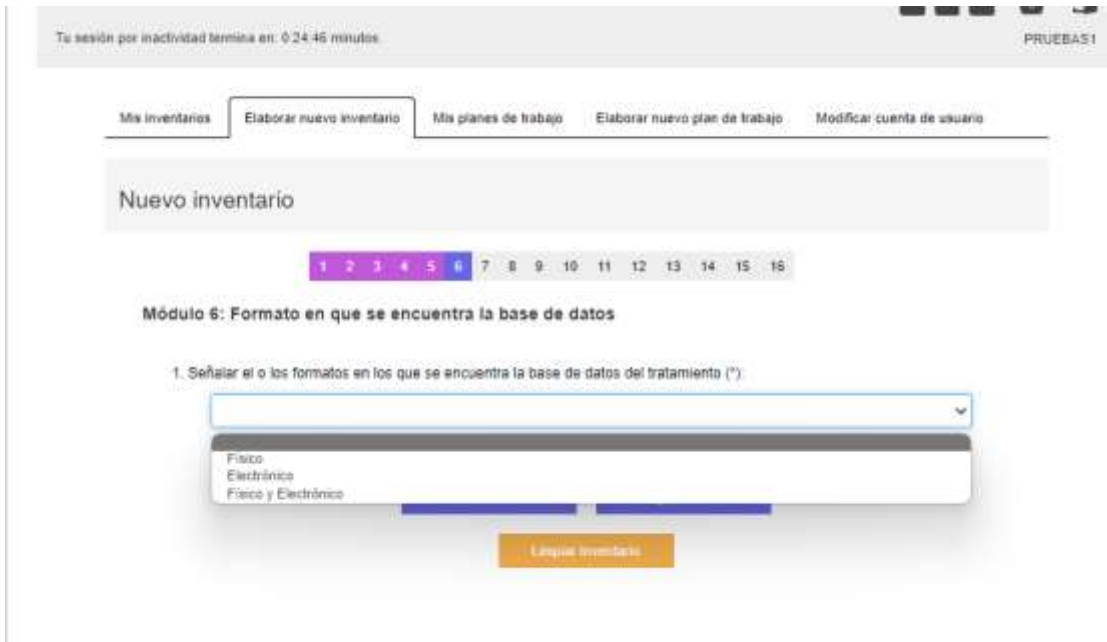


Imagen 27. Ejemplo de vista

Módulo 7

Se deberá identificar la ubicación de la base de datos.

- Archiveros de la unidad administrativa
- Equipo de cómputo
- Servidor de la Institución
- En la nube
- Archivo de concentración
- Otro



Imagen 28. Ejemplo de vista

Módulo 8

Se deberá identificar cual es la Sección, Serie y en su caso Subserie con base al Catálogo de Disposición Documental (CADIDO) de la organización.



Imagen 29. Ejemplo de vista

Módulo 9

En este apartado, se deberá describir la finalidad o las finalidades del tratamiento de manera explícita y concreta, así como si requieren o no consentimiento del titular.

En el caso de que requieran consentimiento, se deberá describir el tipo de consentimiento requerido.

- Tácito
- Expreso o por escrito

Imagen 30. Ejemplo de vista

Y en caso de negativa se deberá señalar los supuestos por los que no se requiere el consentimiento

Imagen 31. Ejemplo de vista

Módulo 10

Se deberá señalar lo siguiente:

- Señalar los puestos de las personas que tienen acceso a la base de datos del tratamiento correspondiente
- Definir unidad administrativa a la que está adscrito quien tiene acceso a la base de datos.
- Señalar las facultades por las cuales las personas tienen acceso a la base de datos.

[Mis inventarios](#) | [Elaborar nuevo inventario](#) | [Mis planes de trabajo](#) | [Elaborar nuevo plan de trabajo](#) | [Modificar cuenta de usuario](#)

Nuevo inventario

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

Módulo 10: Personal con acceso a la base de datos

1. Señalar los puestos de las personas que tienen acceso a la base de datos del tratamiento correspondiente (estos puestos pueden ser genéricos en caso de no conocer el nombre del puesto) (*):

2. Definir unidad administrativa a la que está adscrito quien tiene acceso a la base de datos (estas unidades pueden ser genéricas en caso de no conocer el área de adscripción) (*):

3. Señalar las facultades por las cuales las personas tienen acceso a la base de datos (*):

<< Anterior
Siguiente >>

Limpiar Inventario

Imagen 32. Ejemplo de vista

Módulo 11

El usuario deberá señalar el nombre de la o las personas físicas o morales que actúan como encargados en el tratamiento, así como la clave, siglas o identificador del instrumento jurídico que regula la relación con el encargado

Imagen 33. Ejemplo de vista


Módulo 12

Se deberá establecer si se realizan transferencias o no. En caso afirmativo se deberá señalar lo siguiente:

- Nombre, razón o denominación social de los terceros a los que se transfieren los datos personales.
- Finalidades para las cuales se transfieren los datos personales por cada uno de los terceros.
- Si la transferencia requiere o no consentimiento
- Si la transferencia requiere de la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico

Imagen 34. Ejemplo de vista

En caso de que no se pasara al siguiente modulo.



Tu sesión por inactividad termina en: 0:23:53 minutos

PRUEBA01

[Mis inventarios](#)
[Elaborar nuevo inventario](#)
[Mis planes de trabajo](#)
[Elaborar nuevo plan de trabajo](#)
[Modificar cuenta de usuario](#)

Nuevo inventario

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

Módulo 12: Transferencias de datos personales

1. Señalar si se realizan o no transferencias en el marco del tratamiento (*)

Si No

[<< Anterior](#)
[Siguiente >>](#)

[Loguear \(Iniciar Sesión\)](#)


**GENERADOR DE INVENTARIOS
DE DATOS PERSONALES Y
PLANES DE TRABAJO**

Insurgente S.A. No. 3211 Cal. Insurgente,
 Ciudad. Alajuela, Costa Rica. C.R. 50106

Tel. 01 888 8334334

Imagen 35. Ejemplo de vista

Módulo 13

Para el caso de la difusión, se deberá si en el tratamiento se realiza la difusión de los datos personales.

En caso afirmativo, se deberá indicar el fundamento jurídico que ordena la difusión de los datos personales

Nuevo inventario

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

Módulo 13: Difusión de los datos personales:

1. Indicar si en el tratamiento se realiza la difusión de los datos personales (*):

Sí No

2. Indicar el fundamento jurídico que ordena la difusión de los datos personales:

<< Anterior

Siguiente >>

Guardar inventario

Imagen 35. Ejemplo de vista

En caso de negativo, se pasará al siguiente modulo.

Tu sesión por inactividad terminó en: 0:24:35 minutos

PRUEBA1

Nuevo inventario

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

Módulo 13: Difusión de los datos personales

1. Indicar si en el tratamiento se realiza la difusión de los datos personales (*):

Sí No

<< Anterior

Siguiente >>

Guardar inventario

Imagen 36. Ejemplo de vista

Módulo 14

El plazo de conservación lo podrá identificar en el Catálogo de Disposición Documental (CADIDO) de su Organización.



Imagen 37. Ejemplo de vista

Módulo 15

Este apartado dependerá del ciclo de vida de los datos personales

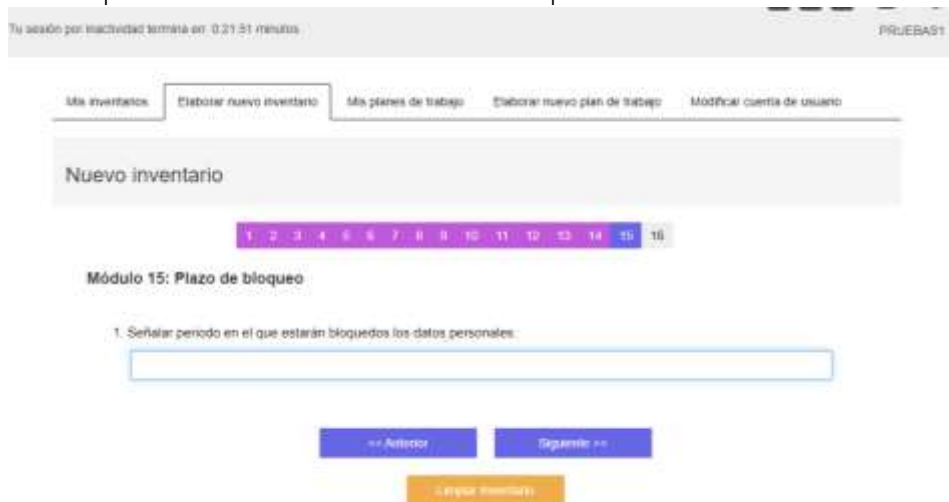


Imagen 38. Ejemplo de vista

Módulo 16

En este apartado el responsable podrá realizar sus observaciones.

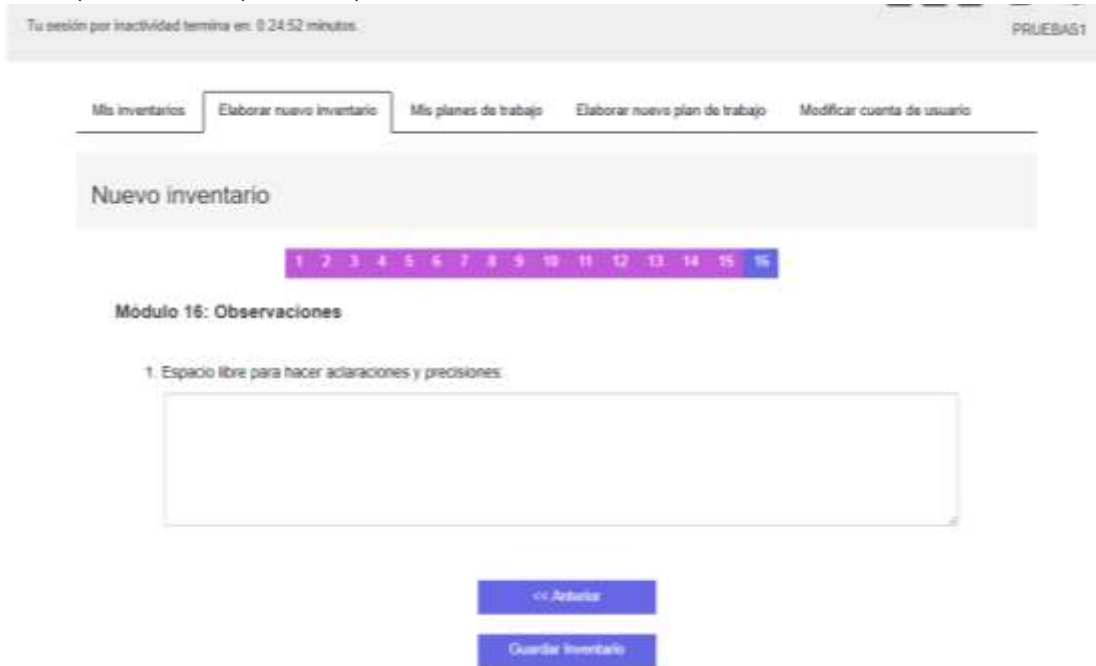


Imagen 39. Ejemplo de vista

Una vez, finalizado el módulo de observaciones, deberá dar clic en el apartado de “guardar inventario” y de esa forma de le generará un inventario con un número de folio, fecha de creación, fecha de modificación y opciones de previsualizar, editar o eliminar.



Imagen 40. Ejemplo de vista

GENERADOR DE PLANES DE TRABAJO

El escritorio de trabajo cuenta con dos pestañas dedicadas a generar planes de trabajo:

- Mis planes de trabajo
- Elaborar nuevo plan de trabajo



Imagen 41. Vista general de Modificar cuenta de usuario

Mis planes de trabajo

Esta sección **Mis planes de trabajo** podrá visualizar los planes de trabajo que vaya realizando identificados en una tabla con los siguientes rubros:

Mis inventarios

Folio	Fecha de creación	Última fecha de modificación	Opciones del usuario
00000021	27/04/2022 11:42:45 a. m.	27/04/2022 11:44:30 a. m.	

Imagen 42. Tabla de opciones

- **Folio**, el sistema asigna de manera automática un número de folio a cada plan de trabajo que vaya generando.
- **Fecha de creación**, indica la fecha y hora de creación del plan de trabajo.
- **Fecha de modificación**, indica la fecha y hora de la última modificación, presentando los documentos más recientes al inicio.
- **Opciones del usuario**, en esta sección podrá previsualizar, editar o eliminar el plan de trabajo, para más detalle diríjase a la Sección **Opciones del Usuario** del presente manual.

Elaborar nuevo plan de trabajo

Para crear un nuevo plan de trabajo realice lo siguiente:

- De clic en la opción Elaborar un nuevo plan de trabajo, al hacer esto, se mostrará una ventana con información importante para el usuario en la cual deberá hacer clic en Aceptar para iniciar con el llenado del Cuestionario

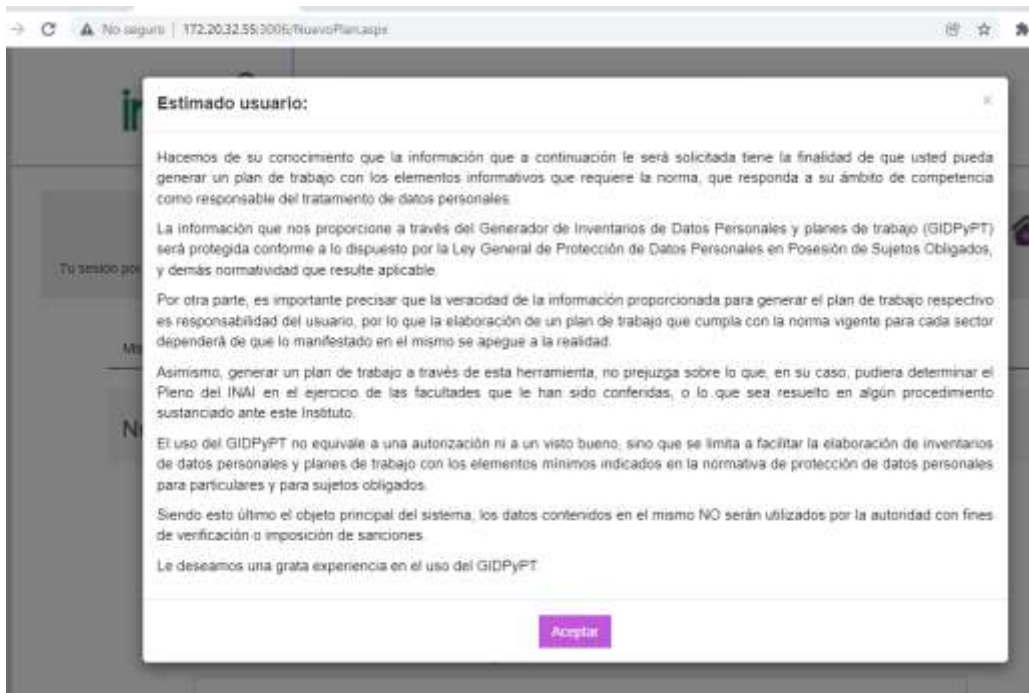


Imagen 43. Mensaje en ventana emergente

- La herramienta ira mostrando preguntas por secciones, recuerde que las preguntas que inician con un (*) son preguntas obligatorias, si no cuentan con un (*) estas son opcionales.

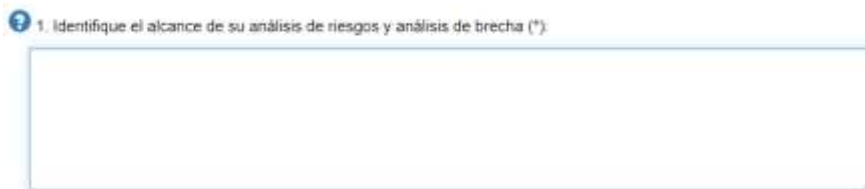


Imagen 44. Ejemplo de pregunta obligatoria

El Generador de Inventarios de Planes de Trabajo cuenta con 15 módulos divididos en dos secciones que comprenden el desarrollo de un análisis de riesgos y un análisis de brecha, estos apartados deberá llenarlos para conseguir un documento en formato PDF para su descarga:

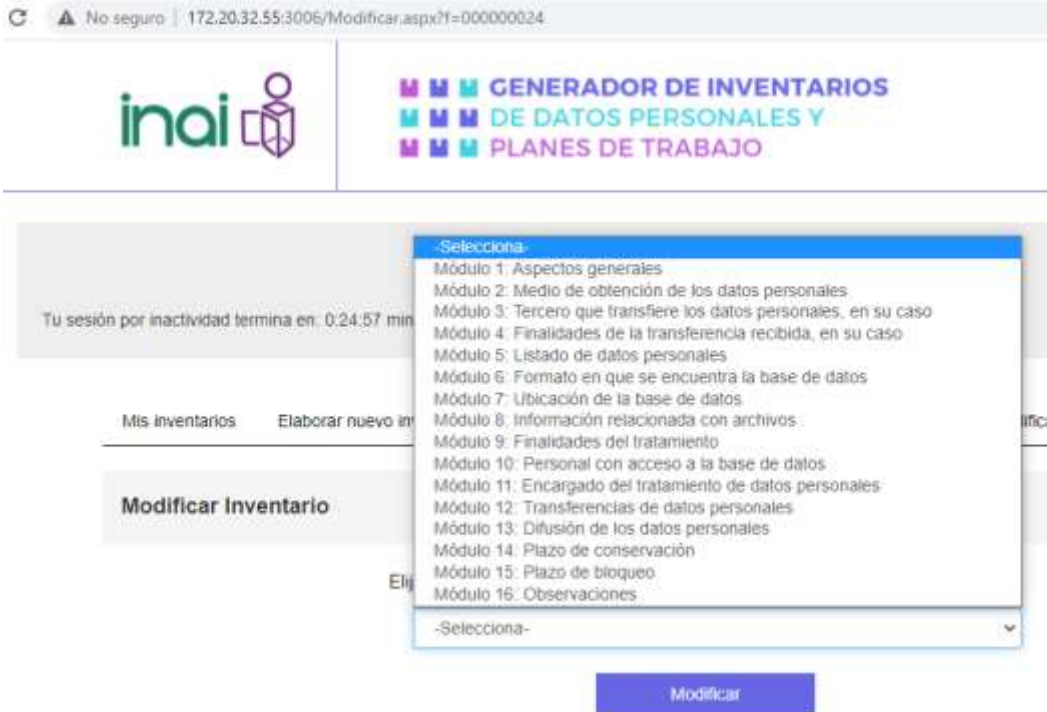


Imagen 45. Composición en secciones del cuestionario dinámico

Cuando haya llenado los 16 módulos del cuestionario, aparecerá la opción previsualizar, en caso de no haber terminado el cuestionario, solo podrá editar las secciones.

Mis planes de trabajo

Folio	Fecha de creación	Última fecha de modificación	Opciones del usuario
00000010	19/04/2022 01:16:25 p. m.	19/04/2022 01:16:25 p. m.	

Imagen 46. Ejemplo de vista de mis planes de trabajo

Definir el alcance, contexto y objetivos del análisis de riesgos

Previo a la identificación de los activos, se debe definir el alcance y objetivos del análisis de riesgos como parte de la gestión de riesgos, por lo que debe realizar lo siguiente:

1. El **alcance**, es la forma en que se describen los límites del proyecto, su cobertura, sus resultados y sus entregables. Al definirlo debe ser claro en su importancia, para ser comprendido por el equipo y la dependencia o entidad. De esta manera, con el alcance y los límites identificados, el equipo de análisis y la entidad serán capaces de determinar los bienes, personas, procesos y las instalaciones que estarán involucrados en la actividad de análisis y evaluación del riesgo.

Un ejemplo puede ser el alcance del análisis de riesgos de los sistemas de tratamiento de la Dirección General de Administración o su equivalente de la organización, mismo que

solamente involucra los sistemas físicos y digitales de tratamiento de datos personales generados a partir del ejercicio de atribuciones de dicha dirección general.

2. El **contexto**. Es esencial que la gestión de riesgos se integre con el resto de las Unidades Administrativas como con su entorno por lo que hay que definir el marco de trabajo, teniendo en cuenta a nivel interno la cultura, los recursos económicos y humanos, así como los procesos y los objetivos sustantivos y valores de la entidad.

En esta fase se deben establecer los criterios que se emplearán para la evaluación de los riesgos, en particular, los criterios para valorar la probabilidad y los criterios para el impacto asimismo tienen que establecerse y delimitarse los roles y responsabilidades, para esto último, es posible utilizar el documento que haya sido elaborado para atender la fracción II del artículo 35 de la LGPDPPSO.

3. Los criterios de impacto, en este caso relativo a los datos personales como activo de información o activo principal y en el sentido de que el derecho a la protección de datos personales se trata de un derecho fundamental, debe analizarse sobre los daños o afectaciones a las personas titulares de datos personales, considerando adicionalmente la afectación a la organización o al Sujeto Obligado, en sus recursos y su reputación, siendo lo primero el propósito de la realización proteger a las personas titulares de los riesgos y amenazas a los que se pueden enfrentar sus datos personales.

En ese sentido, si bien debe valorarse el impacto en el activo, debe hacerse un esfuerzo más de valorar también el impacto que causa el daño a los datos personales a las personas titulares, como, por ejemplo, sin ser este limitativo:

- I. Daños o riesgos físicos en su persona e integridad.
- II. Daños a su salud física o mental
- III. Discriminación o alguna vulneración de sus derechos fundamentales.
- IV. Daño moral
- V. Daño patrimonial

En este caso la valoración se realiza en una escala temporal traducida a una cuantitativa y cualitativa, la frecuencia de ocurrencia de las amenazas. Para estimar la frecuencia podemos basarnos en datos empíricos (datos objetivos) del histórico del Sujeto Obligado, o en opiniones de expertos (datos subjetivos).

4. Se deben establecer objetivos, es decir, establecer las metas que se quieren conseguir, por lo que, deben ser específicos, medibles o evaluables, alcanzables, relevantes y deben tener un tiempo definido, lo que permitirá la evaluación de resultados y la mejora continua.

Identificar los activos

Un activo se define, de acuerdo con la Guía de Gestión del riesgo y evaluación de impacto en tratamiento de datos personales, de la Agencia Española de Protección de Datos, como "todo bien o recurso que puede ser necesario para implantar y mantener una operación de tratamiento de datos personales en cualquier etapa de su ciclo de vida, desde su concepción y diseño hasta la retirada del tratamiento."

En ese sentido, los activos que tienen valor y requieren resguardarse son los datos personales, recordando que estos activos conviven con otros activos como lo son: servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

De esta manera, se pueden identificar dos tipos de activos:

- Activos de información, corresponden a la esencia de la entidad o Sujeto Obligado
 - Información relativa a los datos personales
 - Información de procesos del negocio, en los que interviene el flujo de datos personales, actividades involucradas en el tratamiento de éstos
- Activos de apoyo, en los cuales residen los activos de información en los cuales residen los activos de información:
 - Hardware;
 - Software;
 - Redes y telecomunicaciones o personal;
 - Estructura organizacional;
 - Infraestructura adicional.

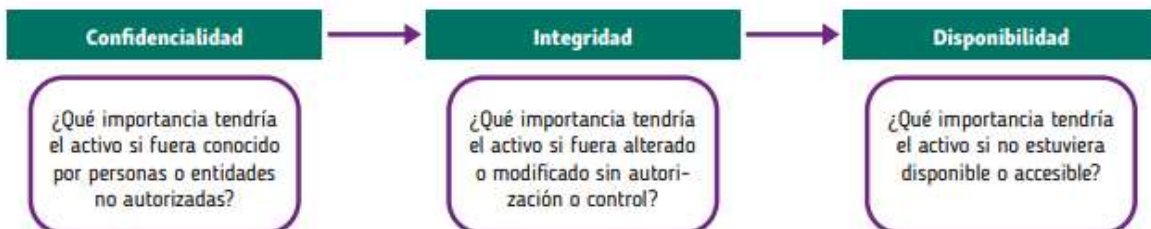
Para esta sección, se recomienda tener a la mano un inventario de sistemas de tratamiento de datos personales ya que éste contiene información detallada respecto a los activos que va a valorar.

Determinar el valor del activo

El valor del activo en función de los tres principios fundamentales de seguridad de la información: confidencialidad, integridad y disponibilidad, aplicándose una escala, en este punto deberá identificar el valor de su inventario, considere que, si su tratamiento incluye datos sensibles, estos deberán ser considerados con el valor más alto por su naturaleza.

Valor Cualitativo	Valor Cuantitativo
Bajo	1-3
Medio	4-6
Alto	7-9

Para determinar adecuadamente la valoración de los activos y su asociación con cada principio de seguridad de la información, se establecen las siguientes preguntas:



Identificar las amenazas

Una amenaza tiene el potencial de dañar un activo y causar una vulneración a la seguridad. Las amenazas pueden ser de origen natural o humano, y pueden ser accidentales o deliberadas; además provenir de adentro o afuera del sujeto obligado. Las amenazas deben ser identificadas considerando que algunas pueden afectar a más de un activo al mismo tiempo.

Las amenazas son "acciones que ocurren" y que pueden causarles daño a nuestros activos, son muy variadas y van cambiando con el tiempo. El desarrollo tecnológico, las comunicaciones y la información van asociadas, al tiempo van unidas al surgimiento de nuevas formas de vulneración de los datos personales, al honor, la intimidad personal y familiar e incluso a la propia imagen.

Por ello, es importante mencionar que, no toda~ las amenazas afectan a todos los activos, sino que hay cierta relación entre el tipo de activo y lo que le podría ocurrir.

En este paso se recomienda realizar las siguientes actividades:

- a) Identificar todas las amenazas relacionadas con cada activo. Las amenazas se identificarán utilizando los catálogos definidos para tal fin.
- b) Debe tomar en cuenta que cada activo puede estar relacionado con varias amenazas, y cada amenaza puede estar vinculada con varias vulnerabilidades.
- c) La identificación de amenazas será realizada por los propietarios de los activos.

SECCIÓN III. IDENTIFICACIÓN DE AMENAZAS

1. De entre las siguientes opciones indique las amenazas a las que se enfrenta su tratamiento (al menos deberá seleccionar una opción):

Tipo	Amenaza	Origen	Respuesta
Daño físico	Fuego accidental	Deliberada, Ambiental	<input checked="" type="checkbox"/>

Imagen 47. Pantalla de la sección de Identificación de amenazas

Valorar el riesgo

El propósito de la identificación del riesgo es determinar que podría suceder que cause una pérdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está pérdida, es por eso de ver realizar una estimación cuantitativa para identificar el riesgo, en esta herramienta podrá asignar un valor del 1 al 3 para identificar si es un riesgos bajo, medio o alto de ocurrencia.

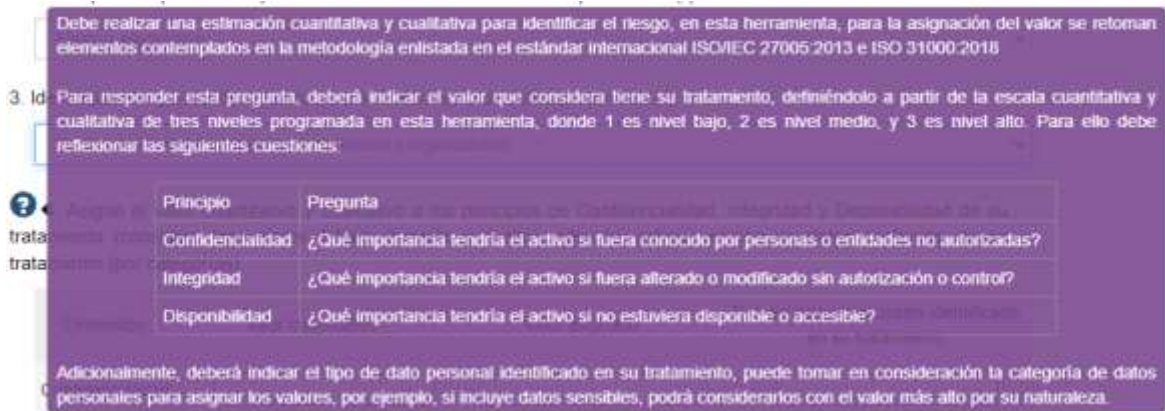


Imagen 48. Información de apoyo para la valoración del riesgo

En el proceso de identificación del riesgo se debe tener en cuenta cómo se podría vulnerar alguno de los pilares de la seguridad de la información:

- Confidencialidad
- Disponibilidad
- Integridad

En esta sección deberá asignar un valor entre 1 a 3 para valorar la confidencialidad, la integridad y la disponibilidad de sus tratamientos, la herramienta automáticamente asociará el valor cualitativo al valor que señale, identificará la pregunta de *tipo de datos personales identificados en su tratamiento* en esta pregunta podrá indicar si trata solo datos personales o si identifica algún dato sensible en su tratamiento, esta pregunta le puede ayudar a valorar si requiere asignar un valor más alto por el tipo de datos que trata.

4. Asigne el valor cuantitativo y cualitativo a los principios de Confidencialidad, Integridad y Disponibilidad de su tratamiento (considere los valores 1-bajo, 2-medio y 3-alto), además, indique el tipo de datos contenido en su tratamiento (por categorías):

Dimensión	Valor cuantitativo	Valor asignado	Tipo de datos personales identificado en su tratamiento
Confidencialidad	<input type="text" value="2"/>	<input type="text" value="Medio"/>	<input type="text" value="datos personales"/>
Integridad	<input type="text" value="1"/>	<input type="text" value="Bajo"/>	<input type="text" value="datos sensibles"/>
Disponibilidad	<input type="text" value="3"/>	<input type="text" value="Alto"/>	<input type="text"/>

Imagen 49. Pantalla de valoración de la confidencialidad, Integridad y Disponibilidad del activo

Estimar el riesgo a partir de la ocurrencia de la amenaza

Como se mencionó, debe recordar las amenazas que identificó a fin de valorar el impacto de que se explote la amenaza identificada y la probabilidad de ocurrencia, lo cual le ayudará a identificar el nivel de riesgo para su sistema de tratamiento, se debe realizar esta valoración por cada amenaza identificada en la sección de identificación de amenazas.

Para realizar la estimación o cálculo del riesgo se recomienda utilizar una escala cuantitativa y su equivalencia cualitativa con atributos calificativos para describir la magnitud de los impactos o consecuencias potenciales y la probabilidad o posibilidad de que ocurran. La estimación del impacto y probabilidad será realizada por los propietarios de los riesgos.

Ahora bien, el análisis de los riesgos de forma cuantitativa y cualitativa debe realizarse conforme a la fórmula universal del riesgo, donde:

$$\text{Riesgo} = \text{probabilidad} \times \text{impacto}$$

Recapitulando, tenemos la identificación de activos y su valoración. Posteriormente, por cada activo se habrán identificado sus vulnerabilidades y las amenazas. Por cada activo se asignarán varias amenazas (se recomienda limitar, máximo, a cinco; por ejemplo, priorizando las más importantes), y posteriormente por cada activo-amenaza-vulnerabilidad debe identificarse su impacto y probabilidad. Esto con los criterios que se proponen a continuación.

- A. IMPACTO
- B. PROBABILIDAD
- C. DETERMINACIÓN DEL RIESGO

Impacto		Probabilidad		Nivel de riesgo		
Cuantitativo	Cualitativo	Cuantitativo	Cualitativo	Cuantitativo	Cualitativo	
<input type="text" value="1"/>	Bajo	<input type="text" value="2"/>	Medio	<input type="text" value="2"/>	Bajo	Eliminar
<input type="text" value="1"/>	Bajo	<input type="text" value="3"/>	Alto	<input type="text" value="3"/>	Medio	Eliminar
<input type="button" value="Agregar"/>						

Imagen 50. Pantalla de cálculo de nivel de riesgo

Identificar las vulnerabilidades del activo

Las vulnerabilidades son debilidades en la seguridad de los activos. Pueden ser identificadas en los siguientes ámbitos:

- Organizacionales;
- De procesos y procedimientos;
- De personal;
- Del ambiente físico;
- De la configuración de sistemas de información;
- Del hardware, software o equipo de comunicación;
- De la relación con prestadores de servicios;
- De la relación con terceros.

La presencia de vulnerabilidades no causa daño por sí misma, se requiere de una amenaza que la explote. Una vulnerabilidad que no se encuentre expuesta a una amenaza identificada posiblemente no requiera la implementación de un control, pero debe ser reconocida y monitoreada constantemente, o bien cuando surja algún cambio. Por ejemplo, un equipo de cómputo o un archivero con información personal es vulnerable a inundaciones si se encuentra instalado en un sótano por el que pasan las tuberías del servicio de suministro de agua. De modo inverso, la amenaza de inundación se descarta si el equipo de cómputo o el archivero con datos personales se localiza en la parte más alta del edificio, lejos de tuberías de agua y de amenazas ambientales relacionadas.

Acciones importantes a considerar para la realización del análisis de riesgos

Respecto al análisis de riesgos, la herramienta tiene contemplado la asignación de valores estimados para ponderar los riesgos a partir de la identificación de amenazas y las vulnerabilidades, permitiendo contar con elementos que ayuden a realizar la descripción de escenarios de vulneración, lamentablemente al momento del lanzamiento de esta herramienta no se tiene implementada una función que herede valores de las secciones III. IDENTIFICACIÓN DE AMENAZAS Y V. IDENTIFICACIÓN DE VULNERABILIDADES, por lo que debe realizar lo siguiente:

1. Valorar el riesgo en la sección III. IDENTIFICACIÓN DE AMENAZAS para cada amenaza señalada, por lo que deberá hacer tantas valoraciones como amenazas haya identificado.
2. Avanzar a la sección V. IDENTIFICACIÓN DE VULNERABILIDADES, identifique las vulnerabilidades del tratamiento de datos
3. Regresar a la sección IV. ESTIMACIÓN DE RIESGOS para añadir la cantidad de elementos a valorar que señaló en la sección V. IDENTIFICACIÓN DE Vulnerabilidades.


Análisis de brecha

Esta etapa se debe tener en cuenta la evaluación de la existencia de controles o medidas de seguridad, se debe conocer sobre su existencia y en caso de que quiera ir más a fondo, deberá considerar su formalidad (si se encuentran o no documentados) y su efectividad (si se cuentan con parámetros de medición), de esta forma se busca escoger los controles que permitan disminuir los valores de exposición del riesgo.

Para ello, la herramienta le presenta una serie de controles agrupados en categorías donde podrá indicar si cuenta con controles de seguridad o no para cubrir el objetivo que se enlista.

PARTE II. ANÁLISIS DE BRECHA

SECCIÓN ÚNICA – IDENTIFICACIÓN DE CONTROLES DE SEGURIDAD

 A continuación, se presentan una serie de controles, indique si cuenta con ellos o no, o en su caso que no le aplican (NA)

Políticas de seguridad de la información

Objetivo: Proporcionar dirección de gestión y apoyo para la seguridad de la información de acuerdo con los requisitos comerciales y las leyes y regulaciones pertinentes.

ID	Objetivo	Descripción	Sí	No	NA
1	Políticas de gestión de datos personales	Deben existir políticas aprobadas por la Alta Dirección/Comité de Transparencia para la regulación específica, condiciones contractuales, así como para la creación, implementación y mantenimiento de los diferentes controles establecidos para salvaguardar los datos personales y sus activos relacionados durante el tratamiento, que sirvan como guía organizacional del propósito, objetivos, responsabilidades y compromisos establecidos por los involucrados para el cumplimiento de la normatividad aplicable a los datos personales.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Imagen 51. Pantalla de ejemplo de controles

Resultados

Después de conocer el nivel de riesgo de sus tratamientos y de elegir que controles son los más adecuados para tener un nivel de riesgo aceptable, se debe diseñar un plan de tratamiento de riesgos, este plan es el resultado del llenado del cuestionario, por lo que, ahora de los resultados obtenidos, deberá hacer una valoración para identificar las necesidades y programar las acciones encaminadas a salvaguardar la seguridad de los datos personales, identificando tiempos y personal asignado a la realización de diversas tareas que buscarán atender los controles de seguridad faltantes o que se deben reforzar.

RESULTADOS DE LA PARTE I – PLAN DE TRABAJO PARA LOS RESULTADOS DEL ANÁLISIS DE RIESGOS

SECCIÓN I. DEFINICIÓN DE ALCANCE Y OBJETIVOS Y CONTEXTO

Alcance de su análisis de riesgos y análisis de brecha: Sistema de tratamiento del Concurso para ser Comisionada y Comisionado Infantil y formar parte del Pleno Niñas y Niños 2022

Objetivo de su análisis de riesgos y análisis de brecha: Tener identificados y ponderar los riesgos y brecha de seguridad a la que se enfrentan los activos que comprenden la base de datos del Concurso para ser Comisionada y Comisionado Infantil y formar parte del Pleno Niñas y Niños 2022

Contexto de la evaluación y tratamiento de riesgos: El tratamiento del Concurso para ser Comisionada y Comisionado Infantil y formar parte del Pleno Niñas y Niños 2022 abarca desde la recopilación de archivos y datos en la plataforma controlada por el INAI, el envío de videos a jurados, el proceso de evaluación y la publicación de videos ganadores

Criterios de aceptación de riesgos: Nivel de riesgo medio a bajo

Actividades a realizar a partir del nivel de riesgo: Reducción de riesgos hasta tratar de llegar a un nivel de riesgo bajo

Criterios de impacto: Vulneraciones de seguridad

Criterios para la evaluación de riesgos: Criticidad de activos involucrados en el tratamiento

SECCIÓN II. ACTIVOS DE INFORMACIÓN O DATOS PERSONALES

Nombre del tratamiento de datos personales: Sistema de tratamiento del Concurso para ser Comisionada y Comisionado Infantil y formar parte del Pleno Niñas y Niños 2022

Soporte en el que se encuentra tratamiento de datos personales: Físico y electrónico

Lugar donde se encuentra su tratamiento de datos personales: Dentro de las instalaciones de la institución u organización

Dimensión	Valor cuantitativo	Valor asignado	Tipo de datos personales identificado en su tratamiento
Integridad	2	Medio	
Disponibilidad	3	Alto	
Confidencialidad	3	Alto	datos de contacto, datos de identificación, datos personales de menores, copias de documentos oficiales (acta, identificación, boletas)

ESCENARIOS DE VULNERACIÓN DEL ANÁLISIS DE RIESGOS

Derivado de los resultados obtenidos deberá añadir las actividades a realizar, el o los responsables que llevaran a cabo las actividades que usted añada y definir un tiempo para realizarlas.

Activo	Amenaza	Impacto	Probabilidad	Nivel del riesgo	Vulneraciones	Actividad a realizar	Responsable	Tiempo de ejecución
					Hardware ->			

Imagen 52. Pantalla de ejemplo de resultados en vista previa