Metodología

Análisis de Brecha para la Seguridad Aplicada a los Datos Personales

V 5.0

Instituto Nacional Electoral

Figura 1. Modelo de Protección de Datos Personales del Instituto Nacional Electoral

CONTROL DE VERSIONES

VERSIÓN	COMENTARIO / DESCRIPCIÓN	RESPONSABLE DE ACTUALIZACIÓN / CREACIÓN / REVISIÓN	FECHA DE ACTUALIZACIÓN / CREACIÓN / REVISIÓN
1.0	Creación del documento.	José Antonio Galván Estrada	Enero 2019
1.1	Revisión del documento.	Blanca Estela Carrillo Sánchez	Febrero 2019
1.2	Actualización de archivos del Anexo 2	José Antonio Galván Estrada	Junio 2019
1.3	Actualización de archivo “Analizador de brechas de seguridad de Datos Personales” del Anexo 2.	José Antonio Galván Estrada	Agosto 2019
1.4	Actualización de archivo “Analizador de brechas de seguridad de Datos Personales” del Anexo 2.	José Antonio Galván Estrada	Octubre 2019
1.5	Actualización de archivo “Analizador de brechas de seguridad de Datos Personales” del Anexo 2.	José Antonio Galván Estrada	Noviembre 2019
1.6	Actualización de archivo “Analizador de brechas de seguridad de Datos Personales” del Anexo 2. Ajuste de los apartados no editables de la herramienta	José Antonio Galván Estrada	Enero 2020
2.0	Adecuación de fondo y forma de “Analizador de brechas de seguridad de Datos Personales” e “Informe ejecutivo” del Anexo 2. Se agrega hoja de medidas para presentación de resultados. Actualización y adecuación de fondo y forma para medidas físicas, técnicas y administrativas.	Diana Gabriela Noemí Benítez Mejía	Febrero 2020
2.0	Revisión del documento	Blanca Estela Carrillo Sánchez	Febrero 2020
2.0	Revisión de forma del documento. Revisión del “Analizador de brechas de seguridad de Datos Personales”.	Diana Gabriela Noemí Benítez Mejía	Marzo 2020
3.0	Actualización de archivo “Analizador de brechas de seguridad de Datos Personales” del Anexo 2. Se agregan	Guadalupe Castañeda Solis	Mayo 2020

VERSIÓN	COMENTARIO / DESCRIPCIÓN	RESPONSABLE DE ACTUALIZACIÓN / CREACIÓN / REVISIÓN	FECHA DE ACTUALIZACIÓN / CREACIÓN / REVISIÓN
	objetivos a los dominios y controles y se actualiza la redacción de preguntas en la sección Controles, se integra una columna de control implementado en la sección Medidas. Actualización de documento.		
3.0	Revisión de documento.	Diana Gabriela Noemí Benítez Mejía	Mayo 2020
3.1	Actualización de documento.	Genesis Hernández Otero Zaira Jiménez Alquicira	Marzo 2021
4.0	Actualización del Anexo 1. Descripción de la herramienta. Integración de los Analizador de brechas de seguridad de Datos Personales intermedio y básico al Anexo 2. Documentos de apoyo. Ajustes en el formato del documento.	Genesis Hernández Otero Zaira Jiménez Alquicira Fabiola Paulina Vázquez Ramírez	Mayo 2021
5.0	Actualización de metodología, atendiendo al Ajustes por actualización de ISO 27002:2022. Incorporar las consideraciones del ISO/IEC 27701:2019	Genesis Hernández Otero Norma Edith Cruz Francisco Jazmín Torres Blanco	Marzo 2023

CONTENIDO

TÉRMINOS Y DEFINICIONES

Activos: Es un bien (tangible o intangible) que una organización posee, y que es requerido para su funcionamiento y el logro de sus objetivos, es decir, tiene valor para la organización.

Activo primario: Es la información en cualquier soporte documental y formato digital –que contiene datos personales- y que es considerada una parte fundamental para el logro de los objetivos organizacionales.

Activo secundario: Son todos los elementos físicos –como archivos e instalaciones – y/o tecnológicos –como servidores y sistemas- en los que se apoyan los activos primarios que se encuentren directamente relacionados con datos personales.

Área responsable: Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de datos personales.

Base 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.

Ciclo de vida de la información o ciclo de vida: Son los estados por los que pasa la información que contiene datos personales, desde su obtención hasta la cancelación, supresión o destrucción.

Efectividad[1]**:** Medida en que se realizan las actividades planificadas y se logran los resultados planificados.

ISO: Organismo Internacional de Estandarización que busca la homologación de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

Ley de Datos: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Medidas de Seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten proteger datos personales.

Responsable: Los sujetos obligados a los que hace referencia el artículo 1 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados que deciden sobre el tratamiento de datos personales. En este caso el responsable serán las áreas de este Instituto que traten datos personales y utilicen o pretendan utilizar el servicio de cómputo en la nube.

Rol custodio: Área que administra diariamente la seguridad de los sistemas de información; posee una total responsabilidad del control y protección de todos los datos mientras estén en custodia.

Rol propietario: Se refiere a las personas servidoras públicas de las áreas responsables que deciden sobre el tratamiento de los datos personales. Es el responsable final de la protección y uso de los datos.

[1] Fuente ISO 9000:2015, 3.7.11

Rol usuario: El área autorizada para acceder a los datos. Son quienes utilizan la información.

Soporte documental o material: es el medio en el cual está contenida la información y puede variar según los materiales y la tecnología empleada, por lo que puede ser impreso o digital. Ejemplo: fotografías, filminas, cintas, plástico, metal, discos duros, memorias flash, discos compactos, entre otros.[2]

Unidad de Transparencia: Unidad Técnica de Transparencia y Protección de Datos Personales.

Usuario: El área autorizada para acceder a los datos. Son quienes utilizan la información.

Vulneración: Incidente de seguridad que involucra datos personales.

OBJETIVO

Apoyar a los propietarios de bases de datos personales en la ejecución del análisis de brecha en la seguridad aplicada a datos personales para identificar el estado actual de las medidas de seguridad implementadas con respecto al estado deseado.

ALCANCE

Dirigido al personal de los órganos ejecutivos, técnicos y de vigilancia, en materia de transparencia, y de control, que por sus funciones traten datos personales en el INE.

REFERENCIAS NORMATIVAS

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Reglamento del Instituto Nacional Electoral en materia de Protección de Datos Personales.

ANTECEDENTES

En 2019, la Unidad de Transparencia diseñó una metodología basada en el Estándar internacional ISO/IEC 27002:2013, que es un código de buenas prácticas para el establecimiento de controles de seguridad de la información.

En febrero de 2022 dicho estándar sufrió una actualización (ISO/IEC 27002:2022) que incluye controles para:

- Seguridad de la información
- Ciberseguridad

[2] Definiciones tomadas del *"Aramburu, María José. Herramientas Informáticas para la Documentación"*, Universitat Jaume I. 2005

- Protección de la privacidad

Los principales cambios del estándar son:

- Modificación del título
- Eliminación del concepto objetivo de control para sustituirlo por los atributos de control, permitiendo así una clasificación más específica.
- Cambio de la estructura, presentando los controles con una taxonomía simple –cuatro temas- y atributos asociados.
- Actualización de 58 controles, fusión de 24 controles e integración de 11 controles nuevos

La edición 2022 anula y reemplaza la 2013.

Por lo anterior, la Unidad de Transparencia actualiza la metodología e incorpora como mejora la ISO/IEC 27701:2019, que es una extensión de las ISO/IEC 27001 y 27002 referente a privacidad.

INTRODUCCIÓN

El análisis de brecha, en general, es un método que permite comparar el estado de desempeño real o situación general de una organización en un momento determinado, con respecto a uno o más puntos de referencia seleccionados, de orden local, regional, nacional y/o internacional[3].

En otras palabras, se refiere a las diferencias presentadas en un momento determinado entre dos situaciones: el estado actual de un elemento y el estado deseado para ese mismo elemento, y puede ser utilizado en diversas áreas, como ventas, recursos humanos, control de costos, ingeniería, entre otros[4].

En materia de datos personales, la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, en sus artículos 33 y 35 –referentes a las medidas de seguridad que los responsables deben implementar para la protección de datos personales- señala que es necesario, entre otras actividades, llevar a cabo un análisis de brecha el cual debe ser incluido en el Documento de Seguridad, en conformidad con el artículo 34.

Además, los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en el artículo 61, establecen que, para la realización del análisis de brecha, los responsables deben considerar las medidas de seguridad existentes y efectivas, las faltantes y la existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

[3] Xiomara Ruiz Ballén. (2012). Guía Análisis de Brechas. 21/01/2019, de Universidad Nacional de Colombia Sitio web: http://www.odontologia.unal.edu.co/docs/claustros-colegiaturas_2013-2015/Guia_Analisis_Brechas.pdf

[4] Jeff Ball. (2018). GAP Analysis. 21/01/2019, de ProjectManagement.com Sitio web: https://www.projectmanagement.com/wikis/233055/Gap-Analysis

1 ANÁLISIS DE BRECHA APLICADO A LA PROTECCIÓN DE DATOS PERSONALES

A través de la ejecución de un análisis de brecha aplicado a las medidas de seguridad que poseen datos personales durante su ciclo de vida, es posible obtener un diagnóstico de las prácticas de seguridad de la información -con base en estándares internacionales- y contar con mecanismos efectivos para su protección.

La Ley, en su Artículo 31, señala que todos los sujetos obligados que usen datos personales deben de establecer y mantener, medidas de seguridad técnicas, administrativas y físicas para proteger los datos personales que estén en su posesión, garantizando su:

En este contexto, la Unidad de Transparencia elaboró la **Metodología de Análisis de Brecha en la Seguridad Aplicada a los Datos Personales** para generar el entregable que atiende a la "Etapa 2. Evaluación de las medidas de seguridad" de la Estrategia para el Cumplimiento de los Deberes de Seguridad y Confidencialidad para la Protección de Datos Personales 2018-2020 (en adelante, la Estrategia) la cual es parte del Programa para la Protección de Datos Personales del Instituto Nacional Electoral 2018-2023[5] (en adelante, el Programa).

2 ROLES Y RESPONSABILIDADES

- **Unidad de Transparencia**. Su actividad es **asesorar** a los propietarios en materia de seguridad aplicada a la protección de datos personales, de acuerdo con la normativa aplicable.
- **Rol propietario**. Su tarea es **ejecutar** el análisis de brecha, así como la generación del informe correspondiente.
- **Rol custodio.** Su responsabilidad es **proporcionar** a los propietarios, la información referente al tratamiento de datos personales respecto a: los Activos de Tecnologías de la Información y Comunicación, Capital Humano, Seguridad de la Información, Protección Civil, entre otros.
    - Ej: Medidas técnicas de seguridad aplicadas al centro de cómputo, lineamientos para la aplicación de medidas sancionadoras.

[5] https://sidj.ine.mx/restWSsidj-nc/app/doc/2035/INE-CT-ACG-PDP-004-2018_Anexo_DJ

3 DESCRIPCIÓN DE LA METODOLOGÍA

La Metodología de Análisis de Brecha se encuentra sustentada en los estándares internacionales:

- Estándar internacional ISO/IEC 27002:2022[6] *Information security, cybersecurity and privacy protection — Information security controls.*

- ISO/IEC 27701:2019[7] *Extension to ISO/IEC 27002:2022* 2022 *Information security, cybersecurity and privacy protection — Information security controls.*

Se ejecuta mediante preguntas basadas en las cuatro clausulas, 34 controles referidos en los estándares internacionales mencionados.

Se observó que tanto en las categorías de líneas base de la NSA INFOSEC Assessment Methodology (IAM) y en las categorías de medidas de seguridad del Evaluador de Vulneraciones del INAI, existe una importante convergencia entre sus sugerencias, mismas que el estándar internacional ISO/IEC 27002:2022 contempla e incluso sugiere medidas de seguridad adicionales.

Con base en lo anterior, la presente metodología se desarrolló tomando como referente el estándar internacional ISO/IEC 27002:2022 *Information security, cybersecurity and privacy protection — Information security controls*, que contiene los controles contemplados por los otros dos marcos de referencia además de una serie de medidas de seguridad técnicas, físicas y administrativas adicionales recomendadas para proteger la seguridad de la información -la cual puede estar contenida en cualquier tipo de soporte documental-.

Adicionalmente, la presente metodología se apoya de una herramienta denominada **“Analizador de Brechas de Seguridad para Datos Personales” -** incluida en el Anexo 2- desarrollada por la Unidad de Transparencia, donde se listan los controles mencionados anteriormente junto con una serie de preguntas que deberá responder el propietario de la base de datos para poder determinar la existencia o no de medidas de seguridad.

Es importante mencionar que la identificación de las brechas debe realizarse en todo el flujo de datos personales, es decir, durante su ciclo de vida, el cual está compuesto por las siguientes fases:

- Fase 1. Creación / colecta / captura
- Fase 2. Procesamiento
    a) Mantenimiento de datos / pre-procesamiento
    b) Almacenamiento
    c) Síntesis de datos / transformación
    d) Uso de la información
- Fase 3. Transferencia / publicación / revelación
- Fase 4. Archivado / retención
- Fase 5. Destino final
    a) Supresión / anonimización
    b) Conservación permanente

[6] https://www.iso.org/standard/54533.html

[7] Es posible consultar más información y comprar el estándar en https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en

La ejecución del análisis de brecha se lleva a cabo a través de cuatro pasos con el objetivo de identificar la base de datos personales, definir los objetivos de su ejecución, determinar el estado actual e identificar la brecha con respecto al estado deseado.

Figura 2. Pasos de metodología de brecha.

A continuación, se describe cada uno de los pasos mencionados:

3.1.1 Identificación del área

Selección de la problemática

Las personas responsables deben:

a) Seleccionar la base de datos,
b) Establecer el proceso del que forma parte,
c) Identificar el flujo de datos personales,
d) Identificar las áreas involucradas.

Esta información se obtiene al ejecutar la etapa preliminar “Identificación del Propietario de las Bases de Datos “y la etapa 1 “Identificación del Flujo de Datos Personales “de la Estrategia para el Cumplimiento de los Deberes de Seguridad y Confidencialidad para la Protección de Datos Personales.

3.1.2 Definición de los objetivos

¿Qué se quiere lograr?

Las personas responsables definen los objetivos de acuerdo con el alcance del análisis, por ejemplo:

El área responsable define los objetivos de acuerdo con el alcance del análisis, por ejemplo:

- **Supuesto 1:** El área responsable almacena la información en dos tipos de servidores:

  a) Físicos, propiedad del Instituto y
  b) En la nube.

  El área determina ejecutar el Análisis de Brecha **con alcance en los servidores físicos,** sin incluir en la nube**.**

- **Supuesto 2:** El área responsable trata datos personales contenidos en el expediente de personal, mediante un proceso manual y un sistema informático.

  El área decide solo ejecutar el Análisis de Brecha **con alcance en** el proceso manual sin incluir el sistema informático.

- **Supuesto 3:** El área responsable decide ejecutar el Análisis de Brecha **con alcance en** todos los activos secundarios, tanto físico como digital.

3.1.3 Determinar el estado actual

¿Dónde estamos?

Para determinar el estado actual, la Unidad Técnica de Transparencia utilizó la norma internacional *ISO/IEC 27002:2022*[8]*,* al ser auditable y que dispone de una extensión referente a Protección de Datos Personales denominada *ISO/IEC 27701:2019*[9]*.*

Con esta norma se generó un cuestionario -elaborado en hoja de cálculo- que permite a las áreas responsables unificar los criterios de identificación de las medidas de seguridad existentes, las medidas faltantes y la existencia de nuevas medidas de seguridad, que pudieran reemplazar a uno o más controles implementados actualmente, el cual se conoce como "***Analizador de Brechas de Seguridad para datos personales***" *-detallado en el Anexo 1 de este documento-*.

3.1.4 Determinar el estado deseado e Identificar la Brecha

¿Dónde y cuándo queremos llegar?

El área responsable debe identificar:

- qué controles aplican,
- qué tiempo tardará en implementarlos y,
- qué recursos requerirá para su implementación.

Lo anterior, considerando:

a) los avances tecnológicos,
b) los costos de implementación,
c) la naturaleza,
d) el ámbito,
e) el contexto y los fines del tratamiento de los datos personales,
f) los riesgos de diversa probabilidad y gravedad que entraña este para el derecho a la protección de datos personales de los titulares,
g) así como otros factores que el propietario considere relevantes.
a) De los controles identificados **sin brecha,** el área responsable debe analizar si es posible mejorar las medidas de seguridad actuales.

[8] https://www.iso.org/standard/75652.html
[9] Es posible consultar más información y comprar el estándar en https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en

b) De los controles identificados **con brecha**, el área responsable debe identificar qué medidas de seguridad faltan para cubrir la brecha.

3.1.5 Identificar la brecha

¿Qué tan lejos estamos del estado deseado?

Para ejecutar el Análisis de Brecha, el área responsable debe identificar:

a) Las medidas de seguridad existentes y efectivas;

b) Las medidas de seguridad faltantes, y

c) La existencia de nuevas medidas de seguridad que pudieran reemplazar a uno o más controles implementados actualmente.

Ejemplos

1. Medidas de seguridad existentes y efectivas

Control 5.9 Inventario de información y otros activos asociados					
Medida	**¿Implementada?**	**¿Es Efectiva?**	**¿Por qué es efectiva?**	**¿Existe Brecha?**	**¿Se debe mejorar?**
Inventario de equipos de cómputo	Sí	Sí	• Identifica la persona responsable del equipo de cómputo. • Permite la atención de requerimientos (por ejemplo: auditorías). • Se conoce los activos con los que cuenta el área, evitando la compra innecesaria de equipos de cómputo.	No	No es necesario hasta el momento.

2. Medidas de seguridad faltantes

Control 7.2 Entrada física					
Medida	**¿Implementada?**	**¿Es Efectiva?**	**¿Por qué es efectiva?**	**¿Existe Brecha?**	**¿Se debe implementar?**
Registro de accesos físicos en bitácora.	No	No aplica	No aplica	Sí, no se cuenta con una medida para controlar los accesos de personas visitantes o empleados dentro del inmueble.	Sí, se asignará personal de seguridad en las entradas del inmueble que verifiquen que las personas que ingresan se registren en la bitácora.

3. Existencia de nuevas medidas de seguridad que pudieran reemplazar a uno o más controles implementados actualmente

Control 8.13 Copias de seguridad de la información					
Medida	**¿Implementada?**	**¿Es Efectiva?**	**¿Por qué no es efectiva?**	**¿Existe Brecha?**	**¿Se debe implementar?**
Respaldos de datos personales en medios extraíbles (USB y discos duros).	Sí	No	Porque no se verifica la integridad de la información y no existe un procedimiento que describa las acciones a realizar y los responsables.	Sí, los respaldos se realizan sin periodicidad definida y solo cuando el área considera necesario.	Sí, se implementará un sistema automatizado para el respaldo de los datos personales con tiempo definido, responsables y verificación de la integridad de la información. Dicho respaldo estará alojado en un servidor propio con copia cifrada en la nube.

4 ANEXOS

ANEXO 1. DESCRIPCIÓN DE LA HERRAMIENTA

Como se ha mencionado con anterioridad, la presente metodología utiliza como referente el estándar internacional ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls , al ser auditable y que dispone de una extensión referente a Protección de Datos Personales denominada ISO/IEC 27701:2019 . Este estándar internacional está conformado por cuatro cláusulas y 34 controles.

La implementación de los controles se realiza a través de la selección de medidas de seguridad técnicas, físicas y/o administrativas, las cuales tienen como finalidad preservar la integridad, confidencialidad y disponibilidad de datos personales y que se clasifican en tres tipos como se describe a continuación.

A) **Medidas de seguridad administrativas, son aquellas basadas en la cultura del personal.** Se encuentran enfocadas en roles y responsabilidades de personas o entidades involucradas en el tratamiento de los datos personales.

   La Ley de Datos define estas medidas como:

   - Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional.
   - La identificación, clasificación y borrado seguro de la información.
   - Sensibilización y capacitación del personal, en materia de protección de datos personales.

   Dentro de las medidas administrativas podríamos encontrar los siguientes ejemplos:

   - Concientización del personal en seguridad de la información y protección de datos personales,
   - Políticas de escritorio limpio,
   - Bloqueo de pantalla del equipo,
   - Sanciones.

B) **Medidas de seguridad físicas, son aquellas basadas en el entorno de trabajo físico.** La Ley de Datos considera la protección del entorno físico de los datos personales y de los recursos involucrados en su tratamiento y recomienda considerar lo siguiente:

   - Prevenir acceso no autorizado al perímetro, instalaciones físicas, áreas críticas, recursos e información.
   - Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas, recursos e información. La identificación, clasificación y borrado seguro de la información.

- Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
- Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;

En este caso, se sugiere el uso de medidas de seguridad como candados, Circuito Cerrado de Televisión (CCTV), guardias de seguridad en puntos de acceso clave, entre otras.

C) **Medidas de seguridad técnicas, son aquellas basadas en el entorno de trabajo digital,** la Ley de Datos considera todas las acciones y mecanismos tecnológicos relacionados con software y hardware para proteger el entorno digital de los datos personales y de los recursos involucrados en su tratamiento. Para ello, recomienda considerar al menos lo siguiente:
   - Que el acceso a las bases de datos, información y recursos sea para usuarios identificados y autorizados.
   - Generar un esquema de privilegios para que el usuario realice las actividades que requiere con motivo de sus funciones.
   - Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento de software y hardware.
   - Gestión de las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

En la siguiente tabla se observan los controles que corresponden a cada una de las cláusulas de la ISO/IEC 27002:2022.

Controles ISO/IEC 27002:2022			
Cláusula	**Tipo de control**	**Control**	**Título del control**
Organizacionales	Preventivo	5.1	Políticas de seguridad de la información
	Preventivo	5.2	Roles y responsabilidades de seguridad de la información
	Preventivo	5.3	Segregación de deberes
	Preventivo	5.4	Responsabilidades de gestión
	Preventivo / Correctivo	5.5	Contacto con autoridades
	Preventivo / Correctivo	5.6	Contacto con grupos de interés especial
	Preventivo / Correctivo / Dectectivo	5.7	Inteligencia de amenazas
	Preventivo	5.8	Seguridad de la información en la gestión de proyectos.
	Preventivo	5.9	Inventario de información y otros activos asociados
	Preventivo	5.10	Uso aceptable de la información y otros activos asociados
	Preventivo	5.11	Devolución de activos

Controles ISO/IEC 27002:2022			
Cláusula	**Tipo de control**	**Control**	**Título del control**
	Preventivo	5.12	Clasificación de la información
	Preventivo	5.13	Etiquetado de información
	Preventivo	5.14	Transmisión (Transferencia tecnológica) de información
	Preventivo	5.15	Control de acceso
	Preventivo	5.16	Gestión de identidad
	Preventivo	5.17	Información de autenticación
	Preventivo	5.18	Derechos de acceso
	Preventivo	5.19	Seguridad de la información en las relaciones con los proveedores
	Preventivo	5.20	Abordar la seguridad de la información en los acuerdos con los proveedores
	Preventivo	5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC
	Preventivo	5.22	Seguimiento, revisión y gestión de cambios de servicios de proveedores
	Preventivo	5.23	Seguridad de la información para el uso de servicios en la nube
	Correctivo	5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información
	Detectivo	5.25	Evaluación y decisión sobre eventos de seguridad de la información
	Correctivo	5.26	Respuesta a incidentes de seguridad de la información
	Preventivo	5.27	Aprender de los incidentes de seguridad de la información Recolección de evidencia
	Correctivo	5.28	Recolección de evidencia
	Preventivo / Correctivo	5.29	Seguridad de la información durante la interrupción
	Correctivo	5.30	Preparación de las TIC para la continuidad del negocio
	Preventivo	5.31	Requisitos legales, estatutarios, reglamentarios y contractuales
	Preventivo	5.32	Derechos de propiedad intelectual
	Preventivo	5.33	Protección de registros
	Preventivo	5.34	Privacidad y protección de información que contenga datos personales
	Preventivo / Correctivo	5.35	Revisión independiente de la seguridad de la información.
	Preventivo	5.36	Cumplimiento de políticas, normas y estándares de seguridad de la información

Controles ISO/IEC 27002:2022			
Cláusula	**Tipo de control**	**Control**	**Título del control**
De personas	Preventivo / Correctivo	5.37	Procedimientos operativos documentados
	Preventivo	6.1	Investigación/ Evaluación
	Preventivo	6.2	Términos y condiciones de empleo
	Preventivo	6.3	Concientización, educación y capacitación en seguridad de la información
		6.4	Proceso Disciplinario
	Preventivo	6.5	Responsabilidades después de la terminación o cambio de empleo
	Preventivo	6.6	Acuerdos de confidencialidad o no divulgación
	Preventivo	6.7	Trabajo a distancia
	Detectivo	6.8	Informes de eventos de seguridad de la información
Físicos	Preventivo	7.1	Perímetros de seguridad física
	Preventivo	7.2	Entrada física
	Preventivo	7.3	Seguridad de oficinas, salas e instalaciones
	Preventivo / Detectivo	7.4	Monitoreo de seguridad física
	Preventivo	7.5	Protección contra amenazas físicas y ambientales.
	Preventivo	7.6	Trabajar en áreas seguras
		7.7	Escritorio despejado y pantalla despejada
	Preventivo	7.8	Ubicación y protección de equipos
	Preventivo	7.9	Seguridad de los activos fuera de las instalaciones
	Preventivo	7.10	Medios de almacenamiento
	Preventivo / Detectivo	7.11	Utilidades de apoyo
	Preventivo	7.12	Seguridad del cableado
	Preventivo	7.13	Mantenimiento de equipo
Tecnológicos	Preventivo	7.14	Eliminación segura o reutilización de equipos
	Preventivo	8.1	Dispositivos de punto final de usuario
	Preventivo	8.2	Derechos de acceso privilegiado
		8.3	Restricción de acceso a la información
	Preventivo	8.4	Acceso al código fuente
	Preventivo	8.5	Autenticación segura
	Preventivo / Detectivo	8.6	Gestión de capacidad
	Preventivo / Correctivo / Dectectivo	8.7	Protección contra malware
	Preventivo	8.8	Gestión de vulnerabilidades técnicas
	Preventivo	8.9	Gestión de la configuración

Controles ISO/IEC 27002:2022			
Cláusula	**Tipo de control**	**Control**	**Título del control**
	Preventivo	8.10	Eliminación de información
	Preventivo	8.11	Enmascaramiento de datos
	Preventivo / Detectivo	8.12	Prevención de fuga de datos
	Correctivo	8.13	Copia de seguridad de la información
	Preventivo	8.14	Redundancia de las instalaciones de procesamiento de información
	Detectivo	8.15	Inicio sesión
	Correctivo / Dectectivo	8.16	Actividades de seguimiento
	Detectivo	8.17	Sincronización de reloj
	Preventivo	8.18	Uso de programas de utilidad privilegiados
	Preventivo	8.19	Instalación de software en sistemas operativos
	Preventivo / Detectivo	8.20	Seguridad en redes
	Preventivo	8.21	Seguridad de los servicios de red.
	Preventivo	8.22	Segregación de redes
	Preventivo	8.23	Filtrado web
	Preventivo	8.24	Uso de criptografía
	Preventivo	8.25	Ciclo de vida de desarrollo seguro
	Preventivo	8.26	Requisitos de seguridad de la aplicación
	Preventivo	8.27	Principios de arquitectura e ingeniería de sistemas seguros
	Preventivo	8.28	Codificación segura
	Preventivo	8.29	Pruebas de seguridad en desarrollo y aceptación.
	Preventivo / Detectivo	8.30	Desarrollo subcontratado
	Preventivo	8.31	Separación de los entornos de desarrollo, prueba y producción
	Preventivo	8.32	Gestión del cambio
	Preventivo	8.33	Información de prueba
	Preventivo	8.34	Protección de los sistemas de información durante las pruebas de auditoría

Para ejecutar el Análisis de Brecha se utiliza un cuestionario -elaborado en hoja de cálculo basado en las normas *ISO/IEC 27002:2022 e ISO/IEC 27701:2019* - que permite a las áreas responsables unificar los criterios de identificación de las medidas de seguridad existentes, las medidas faltantes y la existencia de nuevas medidas de seguridad, que pudieran reemplazar a uno o más controles implementados actualmente, el cual se conoce como "*Analizador de Brecha de Seguridad para datos personales*", en adelante Analizador de Brecha.

Con base en lo anterior, la Unidad de Transparencia generó las herramientas de ***"Analizador de Brechas de Seguridad de Datos Personales***" *–incluidas en el Anexo 2-* que ayudarán al propietario a identificar las medidas de seguridad implementadas para proteger datos personales durante su ciclo de vida.

Existen tres categorías de analizadores de brecha, estos se eligen dependiendo del procedimiento a través del cual se tratan datos personales: manual o automatizado.

- **Completo:** Cuando en el tratamiento de datos personales se hace uso de un sistema informático desarrollado por el Instituto, por un tercero o adquirido por licencia y, en su caso, genera documentos físicos.

- **Intermedio**: Cuando en el tratamiento de datos se utilizan herramientas tecnológicas como Word, Excel, PDF, etc.; sin incluir un sistema informático automatizado.

- **Básico**: Cuando el tratamiento se lleva a cabo únicamente en papel sin el uso de herramientas informáticas.

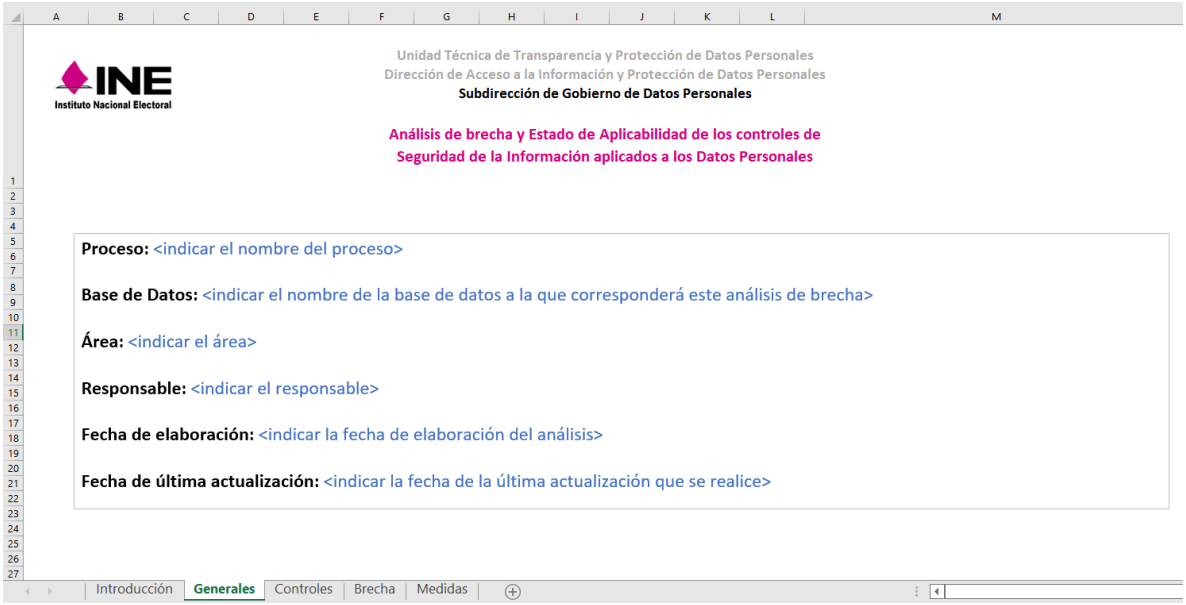
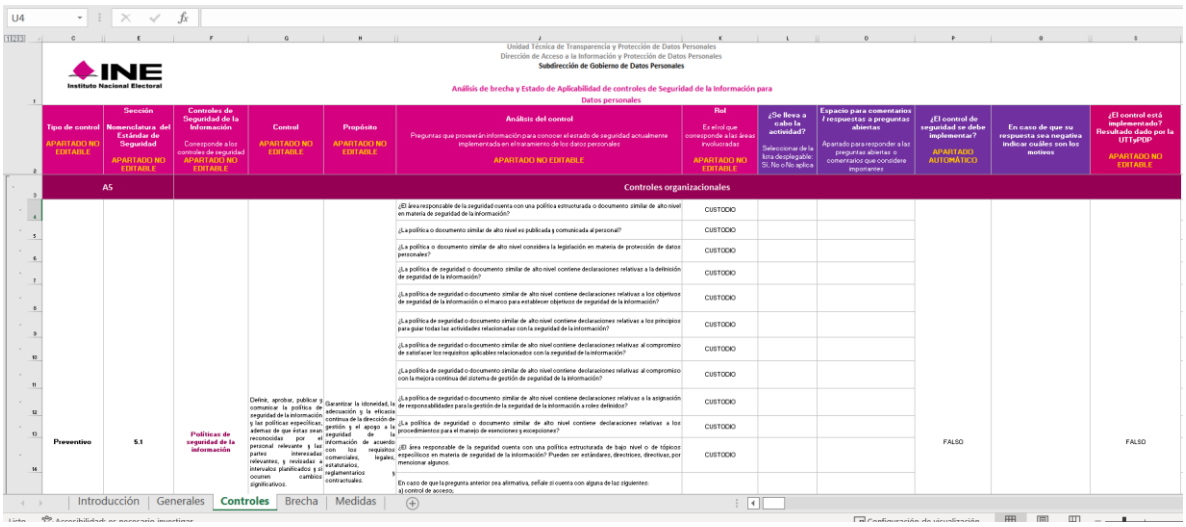


Figura 3. Describe el contenido de la hoja "Generales" del Analizador

a) **Controles.** Esta sección está conformada por diversos apartados que tienen la finalidad de determinar si el control se encuentra implementado.



Unidad Técnica de Transparencia y Protección de Datos Personales
Dirección de Acceso a la Información y Protección de Datos Personales
Subdirección de Gobierno de Datos Personales

Análisis de brecha y Estado de Aplicabilidad de controles de Seguridad de la Información para Datos personales

Tipo de control APARTADO NO EDITABLE	Sección Nomenclatura del Estándar de Seguridad APARTADO NO EDITABLE	Controles de Seguridad de la Información Corresponde a los controles de seguridad APARTADO NO EDITABLE	Control APARTADO NO EDITABLE	Propósito APARTADO NO EDITABLE	Análisis del control Preguntas que proveerán información para conocer el estado de seguridad actualmente implementada en el tratamiento de los datos personales APARTADO NO EDITABLE	Rol Es el rol que corresponde a las áreas involucradas APARTADO NO EDITABLE	¿Se lleva a cabo la actividad? Seleccionar de la lista desplegable Si, No o No aplica	Espacio para comentarios / respuestas a preguntas abiertas Apartado para responder a las preguntas abiertas o comentarios que considere importantes	¿El control de seguridad se debe implementar? APARTADO AUTOMÁTICO	En caso de que su respuesta sea negativa indicar cuáles son los motivos	¿El control está implementado? Resultado dado por la UTTyPDP APARTADO NO EDITABLE
A5		Controles organizacionales									
Preventivo	5.1	Políticas de seguridad de la información	Definir, aprobar, publicar y comunicar la política de seguridad de la información y las políticas específicas, además de que estas sean reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos.	Garantizar la idoneidad, la adecuación y la eficacia continua de la dirección de gestión y el apoyo a la seguridad de la información de acuerdo con los requisitos comerciales, legales, estatutarios, reglamentarios contractuales.	¿El área responsable de la seguridad cuenta con una política estructurada o documento similar de alto nivel en materia de seguridad de la información?	CUSTODIO			FALSO		FALSO
					¿La política o documento similar de alto nivel es publicada y comunicada al personal?	CUSTODIO					
					¿La política o documento similar de alto nivel considera la legislación en materia de protección de datos personales?	CUSTODIO					
					¿La política de seguridad o documento similar de alto nivel contiene declaraciones relativas a la definición de seguridad de la información?	CUSTODIO					
					¿La política de seguridad o documento similar de alto nivel contiene declaraciones relativas a los objetivos de seguridad de la información o el marco para establecer objetivos de seguridad de la información?	CUSTODIO					
					¿La política de seguridad o documento similar de alto nivel contiene declaraciones relativas a los principios para guiar todas las actividades relacionadas con la seguridad de la información?	CUSTODIO					
					¿La política de seguridad o documento similar de alto nivel contiene declaraciones relativas al compromiso de satisfacer los requisitos aplicables relacionados con la seguridad de la información?	CUSTODIO					
					¿La política de seguridad o documento similar de alto nivel contiene declaraciones relativas al compromiso con la mejora continua del sistema de gestión de seguridad de la información?	CUSTODIO					
					¿La política de seguridad o documento similar de alto nivel contiene declaraciones relativas a la asignación de responsabilidades para la gestión de la seguridad de la información a roles definidos?	CUSTODIO					
					¿La política de seguridad o documento similar de alto nivel contiene declaraciones relativas a los procedimientos para el manejo de esenciones y excepciones?	CUSTODIO					
					¿El área responsable de la seguridad cuenta con una política estructurada de bajo nivel o de tópicos específicos en materia de seguridad de la información? Pueden ser estándares, directrices, directivas, por mencionar algunos.	CUSTODIO					
					En caso de que la pregunta anterior sea afirmativa, señale si cuenta con alguna de las siguientes: a) control de acceso;						

Introducción | Generales | Controles | Brecha | Medidas

Figura 4. Describe el contenido de la hoja "Controles" del Analizador

Existen dos tipos de columnas: no editables y editables**.**

A continuación, se presentan los apartados ***no editables:***

Tipo de control	Sección	Controles de Seguridad de la Información	Control	Propósito	Análisis del control	Rol	¿El control está implementado? Resultado dado por la UTTyPDP
APARTADO NO EDITABLE	Nomenclatura del Estándar de Seguridad APARTADO NO EDITABLE	Corresponde a los controles de seguridad APARTADO NO EDITABLE	APARTADO NO EDITABLE	APARTADO NO EDITABLE	Preguntas que proveerán información para conocer el estado de seguridad actualmente implementada en el tratamiento de los datos personales APARTADO NO EDITABLE	Es el rol que corresponde a las áreas involucradas APARTADO NO EDITABLE	APARTADO NO EDITABLE

Figura 5. Apartados no editables de la herramienta "Analizador de brechas de seguridad de datos personales"

Donde:

- **Tipo de control:** Se clasifican en correctivo, preventivo o una combinación entre ellos.
- **Sección:** Corresponde a la nomenclatura del estándar internacional ISO/IEC 27002:2022.
- **Controles de seguridad de la información:** Corresponde a los controles de seguridad.
- **Control:** Define la declaración de control específica, para satisfacer el objetivo de control. (Son las actividades que quisiéramos hacer o a la que deseamos llegar)
- **Propósito:** Refleja a donde se quiere llegar al implementar medidas de seguridad
- **Análisis del control:** Contiene las preguntas que proveerán información para conocer el estado de seguridad actualmente implementada en el tratamiento de datos personales.
- **Rol:** Indica el rol que corresponde a las áreas involucradas en el apartado anterior.

A continuación, se listan los campos ***editables:***

¿Se lleva a cabo la actividad?	Espacio para comentarios / respuestas a preguntas abiertas	¿El control de seguridad se debe implementar?	En caso de que su respuesta sea negativa indicar cuáles son los motivos
Seleccionar de la lista desplegable: Sí, No o No aplica	Apartado para responder a las preguntas abiertas o comentarios que considere importantes	APARTADO AUTOMÁTICO	

Figura 6. Apartados editables de la herramienta "Analizador de brechas de seguridad de datos personales"

- **¿Se lleva a cabo la actividad?:** esta pregunta contiene **tres** posibles respuestas en un menú desplegable que el **área responsable** debe seleccionar.

    - La respuesta será **Si** cuando el área responsable realice en su totalidad lo mencionado en la pregunta.
    - La respuesta será **No** cuando el área responsable realice la activad parcialmente o cuando no se lleve a cabo.
    - La respuesta será **No Aplica** cuando dentro del proceso no se contemple o no este definida la actividad expuesta en la pregunta y que no sea implícita.

- **Espacio para comentarios / respuestas a preguntas abiertas:** Apartado para que el área responsable responda a las preguntas abiertas o coloque comentarios que considere importante.
- **¿El control de seguridad se debe implementar?:** Apartado donde, con base en las respuestas dadas por el área, respecto al funcionamiento del proceso y derivado de un análisis por parte del equipo de la UTTyPDP, se determina si el control se debería o no aplicar a su proceso.

    Las posibles respuestas para este supuesto son:

    - "Si",
    - "No" y
    - "No Aplica"

- **En caso de que su respuesta sea negativa, indicar cuáles son los motivos:** Apartado donde se debe indicar porque se determinó que la medida de seguridad no se debe tener implementada.

- **¿El control esta implementado?:** Apartado donde se determina si el control está o no implementado considerando los siguientes criterios:

    - La respuesta será **Sí** cuando:

        a. La totalidad de las preguntas que corresponden al apartado en cuestión, están respondidas como "Sí".
        b. Existan respuestas "Sí" y "No aplica", siempre y cuando, en este último se tenga la evidencia y una justificación adecuada de que la actividad relacionada con la pregunta no se ejecuta para el proceso.

    - La respuesta será **No,** cuando al menos en alguna de las preguntas que corresponden al apartado en cuestión, están respondidas como "No".

    - La respuesta será **No Aplica** cuando la columna titulada *"¿Considera que la actividad se debe realizar?"* haya sido respondida como "No".

En la *figura 7* se visualiza el resultado del Análisis de brecha, esta se encuentra en la parte inferior de la hoja "*Controles":*

Total de controles aplicables	0		
Total de controles implementados	0		
Total de controles no implementados	0		
Porcentaje de implementación	#¡DIV/0!		

Figura 7. Describe la sumatoria de los controles aplicables, implementados y no implementados resultado de la hoja "Controles" del Analizador

b) Brecha

Esta sección contiene una gráfica donde es posible observar si existe o no una brecha. El valor máximo en la gráfica es 2, que corresponde a que existen controles implementados; mientras que todos los valores por debajo de este número son interpretados como brecha.

La gráfica cambiará dependiendo de las brechas encontradas en la sección ***CONTROLES como se muestra en la figura 8.***

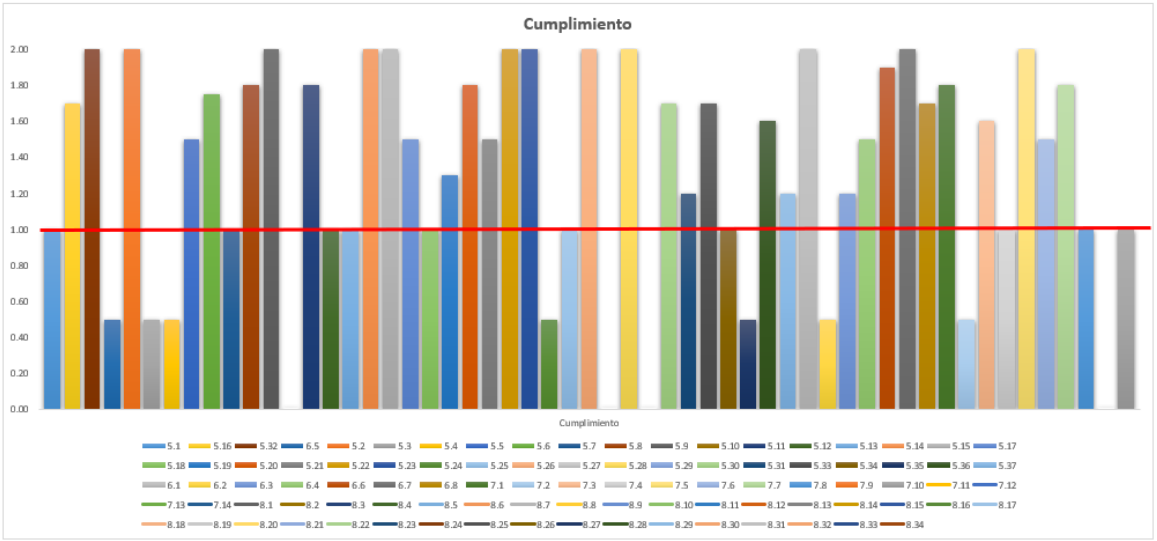


Figura 8. Describe la gráfica obtenida de la hoja "Brecha" del Analizador.

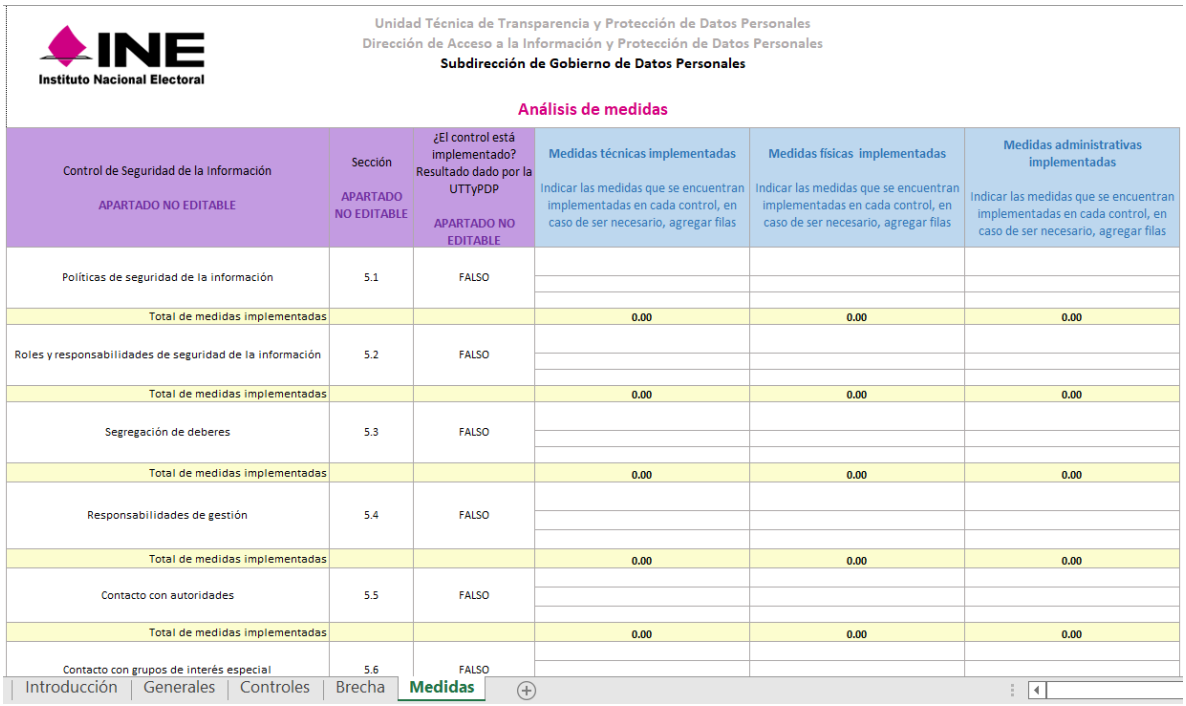
Donde:

- **Valores menores a 1**, indica que el control **no está implementado**.
- **Valores entre 1.1 y 1.9**, indican que el control se encuentra parcialmente implementado.
- **Valores iguales a 2**, indican que el control está **implementado completamente**.

Lugares vacíos. significa que el control “No Aplica” para el proceso evaluado y deberá quitarse dicho control a través del filtro de columna, con la finalidad de observar en la gráfica el estado de los controles que aplican.

a) Medidas

En la hoja de Medidas, el área responsable incorpora las medidas técnicas, físicas y administrativas que se encuentran implementadas por cada control de seguridad de la información, con la finalidad de identificar lo que se tiene actualmente.



Instituto Nacional Electoral

Unidad Técnica de Transparencia y Protección de Datos Personales
Dirección de Acceso a la Información y Protección de Datos Personales
Subdirección de Gobierno de Datos Personales

Análisis de medidas

Control de Seguridad de la Información APARTADO NO EDITABLE	Sección APARTADO NO EDITABLE	¿El control está implementado? Resultado dado por la UTTyPDP APARTADO NO EDITABLE	Medidas técnicas implementadas Indicar las medidas que se encuentran implementadas en cada control, en caso de ser necesario, agregar filas	Medidas físicas implementadas Indicar las medidas que se encuentran implementadas en cada control, en caso de ser necesario, agregar filas	Medidas administrativas implementadas Indicar las medidas que se encuentran implementadas en cada control, en caso de ser necesario, agregar filas
Políticas de seguridad de la información	5.1	FALSO			
Total de medidas implementadas			0.00	0.00	0.00
Roles y responsabilidades de seguridad de la información	5.2	FALSO			
Total de medidas implementadas			0.00	0.00	0.00
Segregación de deberes	5.3	FALSO			
Total de medidas implementadas			0.00	0.00	0.00
Responsabilidades de gestión	5.4	FALSO			
Total de medidas implementadas			0.00	0.00	0.00
Contacto con autoridades	5.5	FALSO			
Total de medidas implementadas			0.00	0.00	0.00
Contacto con grupos de interés especial	5.6	FALSO			

Introducción | Generales | Controles | Brecha | **Medidas**

Figura 9. Describe el contenido del apartado “Medidas” del Analizador.

En los apartados **no editables**, se muestran los controles de seguridad de la información y la sección a la que corresponden del ISO/IEC 27002:2022, el apartado “*¿El control está implementado?*” identifica con un “SÍ”, los controles que deberán ser documentados con las medidas de seguridad.

A continuación, se muestra la estructura de los apartados no editables:

Control de Seguridad de la Información APARTADO NO EDITABLE	Sección APARTADO NO EDITABLE	¿El control está implementado? Resultado dado por la UTTyPDP APARTADO NO EDITABLE

Figura 10. Apartados no editables de medidas del “Analizador de brechas de seguridad de datos personales”.

Dentro de los campos **editables,** que son los que se muestran a continuación, se agregan los nombres de todas las medidas técnicas, físicas y administrativas implementadas para cada control. Como resultado, se enlistan los nombres, la suma de cada una de ellas por control y al final, el total de cada tipo de medidas.

A continuación, se muestra la estructura de los apartados editables:

Medidas técnicas implementadas	Medidas físicas implementadas	Medidas administrativas implementadas
Indicar las medidas que se encuentran implementadas en cada control, en caso de ser necesario, agregar filas	Indicar las medidas que se encuentran implementadas en cada control, en caso de ser necesario, agregar filas	Indicar las medidas que se encuentran implementadas en cada control, en caso de ser necesario, agregar filas

Figura 11. Apartados editables de medidas del "Analizador de brechas de seguridad de datos personales".

Como resultado, se enlistan los nombres, la suma de cada una de ellas por control y al final, el total de cada tipo de medidas.

Total de medidas técnicas implementadas		0.00
Total de medidas físicas implementadas		0.00
Total de medidas administrativas implementadas		0.00

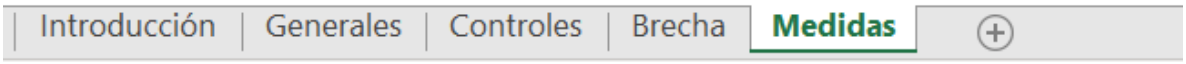


Figura 12. Describe el total de Medidas Implementadas en el apartado "Medidas"

Una medida de seguridad puede implementarse a más de un control, en caso de ser así, se considerará solo una vez en el total de medidas físicas, técnicas o administrativa.

Consideraciones finales

Por último, el propietario, tomando como base los datos obtenidos en la brecha, generará un Informe Ejecutivo de resultados y que formará parte del Documento de Seguridad, (disponible en el Anexo 2 del presente documento).

ANEXO 2. DOCUMENTOS DE APOYO

Anexo	Archivo
Analizador de Brechas de Seguridad de Datos Personales completo	 Analizador_Brecha_C_2023.xlsx
Analizador de Brechas de Seguridad de Datos Personales intermedio	 Analizador_Brecha_I_2023.xlsx
Analizador de Brechas de Seguridad de Datos Personales básico	 Analizador_Brecha_B_2023.xlsx
Informe Ejecutivo	 Plantilla_informeAB_v1.1.docx