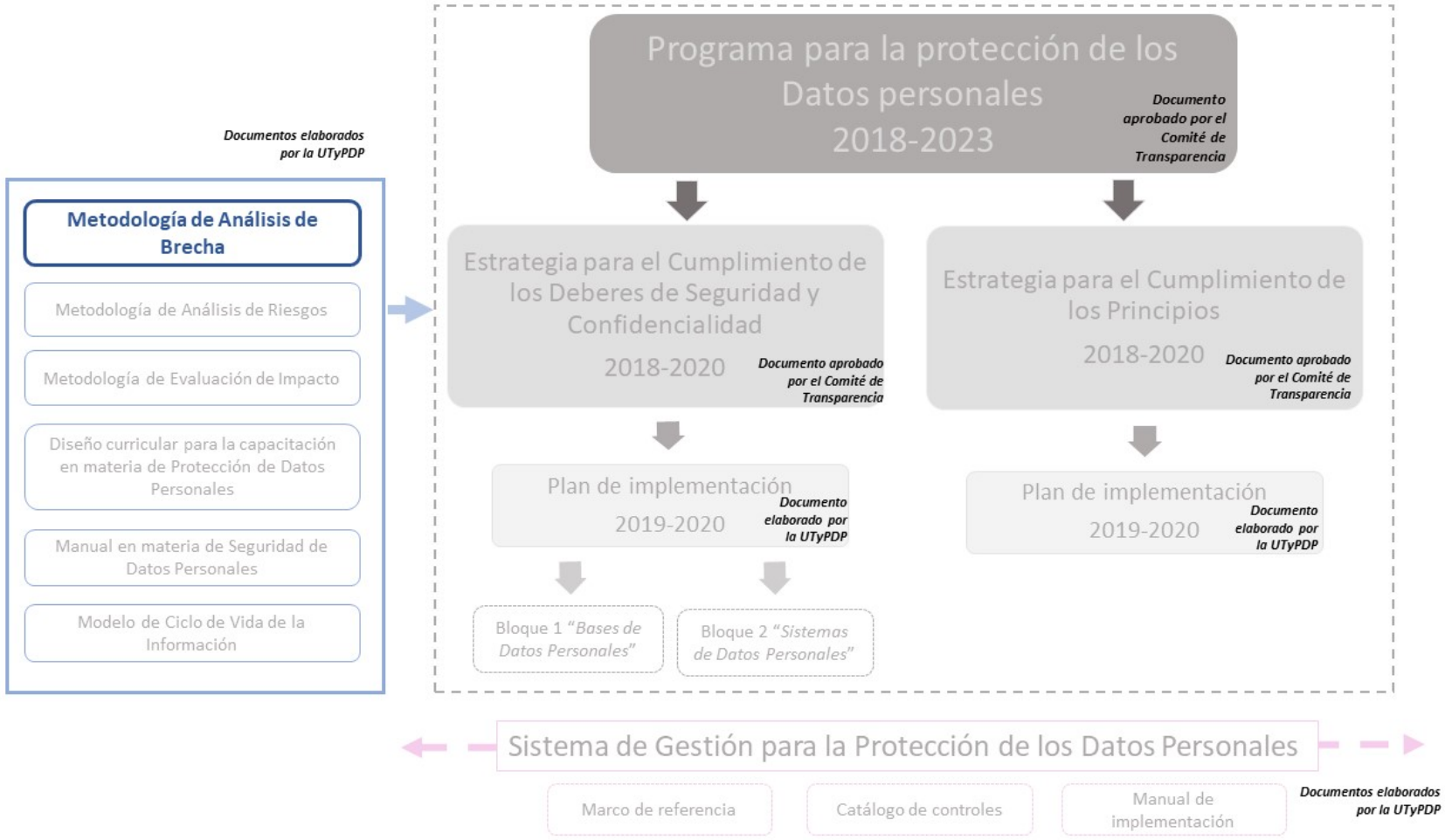
# Metodología

## Análisis de Brecha para la Seguridad Aplicada a los Datos Personales

V 4.0


Documentos elaborados por la UTyPDP
Metodología de Análisis de Brecha
Metodología de Análisis de Riesgos
Metodología de Evaluación de Impacto
Diseño curricular para la capacitación en materia de Protección de Datos Personales
Manual en materia de Seguridad de Datos Personales
Modelo de Ciclo de Vida de la Información
Programa para la protección de los Datos personales 2018-2023
Documento aprobado por el Comité de Transparencia
Estrategia para el Cumplimiento de los Deberes de Seguridad y Confidencialidad 2018-2020
Documento aprobado por el Comité de Transparencia
Estrategia para el Cumplimiento de los Principios 2018-2020
Documento aprobado por el Comité de Transparencia
Plan de implementación 2019-2020
Documento elaborado por la UTyPDP
Plan de implementación 2019-2020
Documento elaborado por la UTyPDP
Bloque 1 "Bases de Datos Personales"
Bloque 2 "Sistemas de Datos Personales"
Sistema de Gestión para la Protección de los Datos Personales
Marco de referencia
Catálogo de controles
Manual de implementación
Documentos elaborados por la UTyPDP

# CONTROL DE VERSIONES

| VERSIÓN | COMENTARIO / DESCRIPCIÓN | RESPONSABLE DE ACTUALIZACIÓN / CREACIÓN / REVISIÓN | FECHA DE ACTUALIZACIÓN / CREACIÓN / REVISIÓN | FIRMA DEL RESPONSABLE |
|---|---|---|---|---|
| 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.<br>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.<br>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.<br>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 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. | Guadalupe Castañeda Solis | Mayo 2020 | |
| 3.0 | Revisión de documento. | Diana Gabriela Noemí Benítez Mejía | Mayo 2020 | |
| 3.1 | Actualización de documento. | Genesis Hernández Otero | Marzo 2021 | |

| | | | | |
|---|---|---|---|---|
| | | Zaira Jiménez Alquicira | | |
| 4.0 | Actualización del Anexo 1. Descripción de la herramienta.<br>Integración de los Analizador de brechas de seguridad de Datos Personales intermedio y básico al Anexo 2. Documentos de apoyo.<br>Ajustes en el formato del documento. | Genesis Hernández Otero<br>Zaira Jiménez Alquicira<br>Fabiola Paulina Vázquez Ramírez | Mayo 2021 | |

# CONTENIDO

# 1 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.

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

**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.

**Propietario:** El área dueña de la información.

**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.

**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.[1]



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

**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.

# 2 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.

# 3 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.

# 4 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.

# 5 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[2].

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[3].

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.



[2] 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

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

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.

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.

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[4] (en adelante, el Programa).

# 6 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.
- **Propietarios de las bases de datos**. Su tarea es **ejecutar** el análisis de brecha, así como la generación del informe correspondiente.
- **Custodios de la información.** 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.

# 7 Descripción De La Metodología

La metodología de análisis de brecha fue desarrollada analizando los siguientes marcos de referencia:

- ISO/IEC 27002:2013 Information Technology – Security techniques – Code of practice for information security controls.[5]
- The NSA INFOSEC Assessment Methodology (IAM).[6]



[4] https://sidj.ine.mx/restWSsidj-nc/app/doc/2035/INE-CT-ACG-PDP-004-2018_Anexo_DJ
[5] https://www.iso.org/standard/54533.html
[6] https://www.sans.org/reading-room/whitepapers/auditing/application-nsa-infosec-assessment-methodology-1045

- Evaluador de Vulneraciones del Instituto Nacional de Transparencia, Acceso a la información y Protección de Datos Personales (INAI).[7]

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 27002:2013 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 27002:2013 *Information technology –Security techniques – Code of practice for 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. La herramienta se explicará con más detalle en el Anexo 1 de este documento.

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

## 7.1 PASOS DE IDENTIFICACIÓN

La ejecución del análisis de brecha se lleva a cabo a través de 4 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.

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



[7] http://inicio.inai.org.mx/SitePages/Evaluador-Vulneraciones.aspx


Figura 1. Pasos de metodología de brecha.

### 7.1.1 Identificación del área

*Selección de la problemática*

El propietario debe:

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.

### 7.1.2 Definición de los objetivos

*¿Qué se quiere lograr?*

En este paso, los responsables definen los objetivos de cumplimiento normativo, aplicable al proceso al cual pertenece la base de datos. Ej. Seleccionar las bases de datos que contienen datos personales.

### 7.1.3 Determinar el estado actual

*¿Dónde estamos?*

Con apoyo de la herramienta “*Analizador de Brechas de Seguridad para Datos Personales*” el propietario podrá detectar las medidas de seguridad existentes y las faltantes.

### 7.1.4 Determinar el estado deseado e Identificar la Brecha

*¿Dónde y cuándo queremos llegar? y ¿Qué tan lejos estamos del estado deseado?*

Hasta este punto, el área responsable identifica:

a) Los controles que le aplican,
b) el estado actual de cada control:
    - los que están implementados
    - los que no están implementados, y
c) las medidas de seguridad para atender cada control.

Posteriormente:

a) De los controles identificados **sin brecha,** el área responsable debe analizar si es posible mejorar las medidas de seguridad actuales
b) De los controles identificados **con brecha**, el área responsable debe identificar qué medidas de seguridad faltan para cubrir la brecha.

Por último, la brecha resultará de:

a) Las medidas de seguridad existentes;
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.

# 8 ANEXOS

## ANEXO 1. DESCRIPCIÓN DE LA HERRAMIENTA

Como se ha mencionado con anterioridad, la presente metodología utiliza como referente el estándar internacional ISO/IEC 27002:2013 *Information Techonology – Security techniques – Code of practice for information security controls*[8]**.** Este estándar internacional está conformado por **14 dominios de seguridad, 35 objetivos de control y 114 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 dedatos personales y que se clasifican en tres tipos como se describe a continuación.

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

La Ley de Datos define[9] 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 en el entorno de trabajo físico, conocidas como medidas de seguridad físicas.** La Ley de Datos[10] considera la protección del entorno físico de 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.

[8] https://www.iso.org/standard/54533.html
[9] Artículo 3, fracción XXI de la Ley de Datos
[10] Artículo 3, fracción XXII de la Ley de Datos

- 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 el caso del mantenimiento eficaz, busca asegurar en los equipos, la disponibilidad y la confidencialidad de datos personales, es decir, que siempre se pueda acceder a ellos y que sólo sean modificados por aquellos que han sido autorizados.

Dentro de las medidas física podríamos encontrar los siguientes ejemplos:

- Candados
- Circuitos Cerrados de Televisión (CCTV)
- Bitácoras de entrada y salida de personal y visitantes.

**C) Medidas de seguridad en el entorno de trabajo digital, conocidas como medidas de seguridad técnicas.** La Ley de Datos[11] considera las acciones y mecanismos tecnológicos relacionados con software y hardware para proteger el entorno digital de datos personales y de los recursos involucrados en su tratamiento. Para ello recomienda considerar al menos lo siguiente:

- Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea 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.
- Gestionar de las comunicaciones, operaciones y medios de almacenamiento de los recursos informático en el tratamiento de datos personales.

Dentro de las medidas técnicas podríamos encontrar los siguientes ejemplos:

- Bloqueo de equipo por inactividad
- Respaldos
- Roles de usuario
- Control de acceso
- Desbloqueo de pantalla con contraseña



[11] Artículo 3, fracción XXIII de la Ley de Datos

En la siguiente tabla se observan el número de objetivos de control y número de controles que corresponden a cada una de las cláusulas de la **ISO/IEC 27002:**

| Anexo Objetivos de control y controles de ISO/IEC 27002:2013 | | | |
|---|---|---|---|
| **Cláusula en ISO/IEC 27002** | **Titulo** | **No. Objetivos de Control** | **No. de Controles** |
| **A.5** | Políticas de Seguridad de la información | 1 | 2 |
| **A.6** | Organización de la Seguridad de la Información | 2 | 7 |
| **A.7** | Seguridad relativa a los Recursos Humanos | 3 | 6 |
| **A.8** | Gestión de activos. | 3 | 10 |
| **A.9** | Control de acceso | 4 | 14 |
| **A.10** | Criptografía | 1 | 2 |
| **A.11** | Seguridad física y del entorno | 2 | 15 |
| **A.12** | Seguridad de las operaciones | 7 | 14 |
| **A.13** | Seguridad de las comunicaciones | 2 | 7 |
| **A.14** | Adquisición, desarrollo y mantenimiento de los Sistemas de Información | 3 | 13 |
| **A.15** | Relación con proveedores | 2 | 5 |
| **A.16** | Gestión de incidentes de Seguridad de la Información | 1 | 7 |
| **A.17** | Aspectos de Seguridad de la Información para la Gestión de la continuidad del negocio | 2 | 4 |
| **A.18** | Cumplimiento | 2 | 8 |



Los dominios y objetivos de control -que componen cada dominio- se listan a continuación:

**A.5 Políticas de seguridad.**

1. Directrices de gestión de la seguridad de la información

**A.6 Aspectos organizativos de la seguridad de la información**

1. Organización interna
2. Dispositivos para movilidad y teletrabajo

**A.7 Seguridad relativa a recursos humanos**

1. Antes del empleo
2. Durante el empleo
3. Finalización del empleo o cambio en el puesto de trabajo

**A.8 Gestión de activos**

1. Responsabilidad sobre uso de los activos
2. Clasificación de la información
3. Manejo de los soportes de almacenamiento

**A.9 Control de accesos**

1. Requisitos de negocio para el control de acceso
2. Responsabilidades del usuario
3. Control de acceso a sistemas y aplicaciones

**A.10 Cifrado**

1. Controles criptográficos

**A.11Seguridad física y ambiental**

1. Áreas seguras
2. Seguridad de los equipos

**A.12 Seguridad en la operación**

1. Responsabilidades y procedimientos de operación
2. Protección contra código malicioso
3. Copias de seguridad
4. Registro de actividad y supervisión
5. Control de instalación de software en producción
6. Gestión de vulnerabilidades técnicas
7. Consideraciones en las auditorias de los sistemas de información

**A.13 Seguridad en las comunicaciones**

1. Gestión de la seguridad en las redes
2. Intercambio de información con partes externas

**A.14 Adquisición, desarrollo y mantenimiento de sistemas de información**

1. Requisitos de seguridad de los sistemas de información
2. Seguridad en los procesos de desarrollo y soporte
3. Datos de prueba

**A.15 Relaciones con proveedores**

1. Seguridad de la información en las relaciones con proveedores
2. Gestión de la prestación del servicio con proveedores

**A.16 Gestión de incidentes de seguridad de la información**

1. Gestión de incidentes de seguridad de la información y mejoras

**A.17 Aspectos de seguridad de la información en la continuidad del negocio**

1. Continuidad de la seguridad de la información
2. Redundancias

**A.18 Cumplimiento**

1. Cumplimiento de los requisitos legales y contractuales
2. Revisiones de la seguridad de la información

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 tipos de analizadores de brecha, dependiendo del proceso a través del cual se tratan datos personales, se determinará cual es aplicable atendiendo a lo siguiente:

A. **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. Contiene 572 preguntas.

B. **Intermedio**
Cuando en el tratamiento de datos se utilizan herramientas tecnológicas como Word, Excel, PDF, etc.; sin incluir un sistema informático automatizado. Contiene 188 preguntas.

C. **Básico**
Cuando el tratamiento se lleva a cabo únicamente en papel sin el uso de herramientas informáticas. Contiene 151 preguntas.

A continuación, se describe la estructura de los analizadores.

a) **Introducción.** Esta sección contiene:

- Información introductoria, la cual da sustento a la ejecución del análisis de brecha.
- Instrucciones de uso de la herramienta, las cuales dan, de manera general, una explicación de los campos que se deben responder en la sección *Controles.*

b) **Generales.** Conformada por información general que el propietario de la base de datos debe llenar para dar identificar a que base de datos se realiza el análisis de brecha, los apartados son:

- Proceso: proceso de negocio al que apoya la base de datos.
- Base de Datos: nombre de la base de datos (a nivel técnico).
- Área: Área a la cual pertenece el propietario de la Base de Datos.
- Responsable: Responsable de los datos contenidos en la Base de Datos.
- Fecha de elaboración: Fecha en la que se terminó de realizar el análisis de brecha.
- Fecha de última actualización: Fecha de la última actualización al análisis de brecha.

c) **Controles.** Esta sección está conformada por diversos apartados que tienen la finalidad de determinar si una medida de seguridad es aplicable o no a datos personales. Los campos que conforman la sección se dividen en ***no editables*** (apartados con información predefinida) y ***editables*** (apartados destinados a obtener las respuestas necesarias para la finalidad de la herramienta).

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

| **Sección**<br><br>Nomenclatura del Estándar de Seguridad **APARTADO NO EDITABLE** | **Controles de Seguridad de la Información**<br><br>Corresponde a los controles de seguridad<br><br>**APARTADO NO EDITABLE** | **Análisis del control**<br><br>Preguntas que proveerán información para conocer el estado de seguridad actualmente implementada en el tratamiento de los datos personales<br><br>**APARTADO NO EDITABLE** | **1. Seleccionar el área que debe contestar la pregunta**<br>Seleccionar el filtro dependiendo de si:<br>a) es un área responsable; b) es un área de TI; o c) es área de personal<br>**APARTADO NO EDITABLE** | **Rol**<br><br>Es el rol que corresponde a las áreas involucradas<br><br>**APARTADO NO EDITABLE** | **4. ¿La medida de seguridad se debe realizar?**<br><br>Contestar con base en sus funciones y atribuciones **APARTADO NO EDITABLE** | **En caso de que su respuesta sea negativa indicar cuáles son los motivos APARTADO NO EDITABLE** | **¿El control está implementado? Resultado dado por la UTTyPDP APARTADO NO EDITABLE** |
|---|---|---|---|---|---|---|---|

Figura 3: Apartados no editables de la herramienta "Analizador de brechas de seguridad de datos personales"

Donde:

- **Sección:** Corresponde a la nomenclatura del estándar internacional ISO/IEC 27002:2013.
- **Controles de seguridad de la información:** Corresponde a las 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.
- **Seleccionar el área que debe contestar la pregunta:** Apartado que permite seleccionar las preguntas a responder dependiendo si: a) es un área responsable, b) es un área de TI, c) es un área de personal o alguna combinación entre estas.

- **Rol:** Indica el rol que corresponde a las áreas involucradas en el apartado anterior.

- **¿La medida de seguridad se debe realizar?:** 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".

  El analizador contempla la respuesta ***Se desconoce***, misma que es temporal en tanto el área responsable identifique la información para dar respuesta, ya sea de manera interna o con otras áreas del Instituto que pudieran proporcionarla; por lo que no será considerada para determinar si el control está o no implementado.

- 

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

Figura 4: Apartados editables de la herramienta "Analizador de brechas de seguridad de datos personales"

| **¿Se lleva a cabo la actividad?** | **3. Espacio para comentarios / respuestas a preguntas abiertas** |
|---|---|
| Seleccionar de la lista desplegable: Sí, No, No aplica o Se desconoce | Apartado para responder a las preguntas abiertas o comentarios que considere importantes |

- **¿Se lleva a cabo la actividad?:** indica la respuesta que, a través de un menú desplegable, se eligió.
- **Espacio para comentarios / respuestas a preguntas abiertas:** Apartado para responder las preguntas abiertas o colocar comentarios que considere importantes.

### d) 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.

### e) 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.

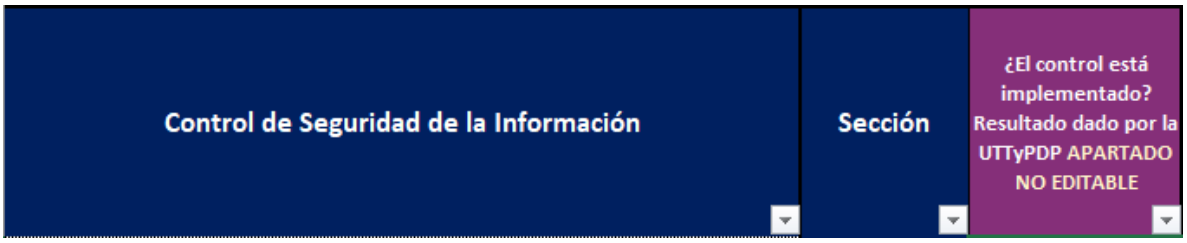



Figura 5. Apartados no editables de medidas del "Analizador de brechas de seguridad de datos personales".

En los apartados no editables, se muestran los controles de seguridad de la información y la sección a la que corresponden del ISO/IEC 27002:2013, el apartado "*¿El control está implementado?*" identifica con un "SÍ", los controles que deberán ser documentados con las medidas de seguridad.

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.

| 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 6. Apartados editables de medidas del "Analizador de brechas de seguridad de datos personales".

**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_ completo v3.0.xlsx |
| Analizador de Brechas de Seguridad de Datos Personales intermedio | Analizador_brecha_ intermedio v1.0.xlsx |
| Analizador de Brechas de Seguridad de Datos Personales básico | Analizador_brecha_ básico v1.0.xlsx |
| Informe Ejecutivo | Plantilla_informeAB_v 1.1.doc |