Sistema Nacional de Transparencia
Acceso a la Información Pública y Protección de Datos Personales

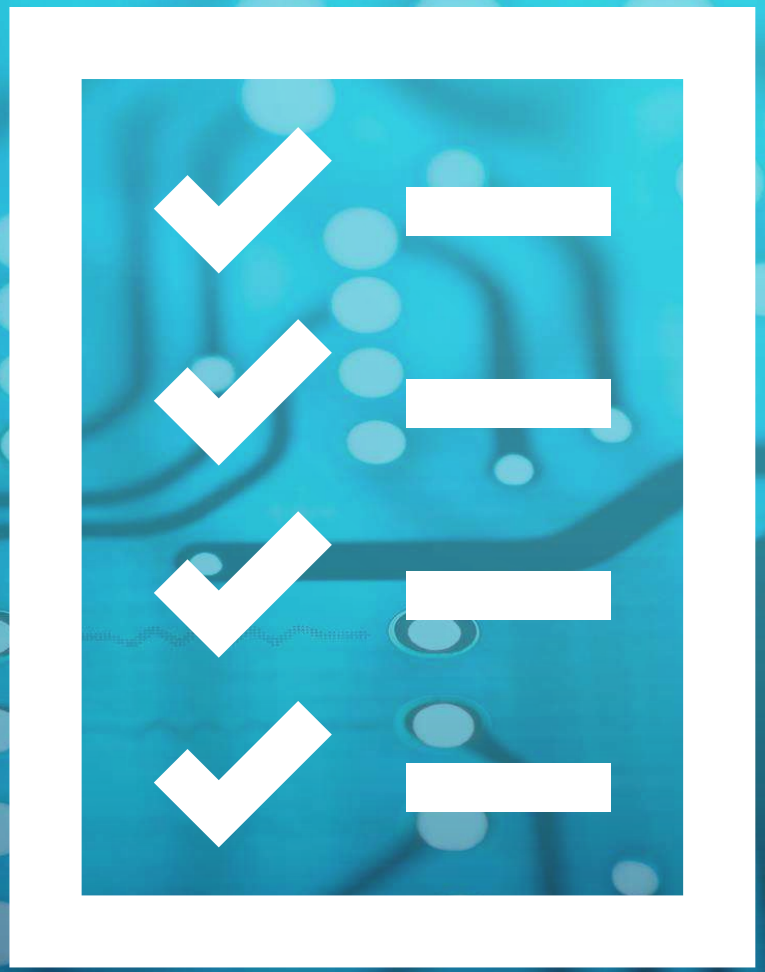
idaip Quintana Roo
Por tu derecho a saber

inai

CURSO TALLER "MEDIDAS DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES EN LOS SUJETOS OBLIGADOS"

SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN GENERAL DE NORMATIVIDAD Y CONSULTA



AGENDA

PRIMER BLOQUE:

Elementos conceptuales (1 hora).

SEGUNDO BLOQUE:

El documento de seguridad en el marco del Sistema de Gestión (2 horas)

TERCER BLOQUE:

Análisis de riesgo y análisis de brecha para la actualización de las medidas de seguridad (1 hora).

ELEMENTOS CONCEPTUALES

PROTECCIÓN DE DATOS PERSONALES

8 Principios

- Licitud
- Proporcionalidad
- Lealtad
- Finalidad
- Consentimiento
- Calidad
- Información
- Responsabilidad

2 Deberes

- **Seguridad**
- **Confidencialidad**

5 Derechos

- **Portabilidad**
- **A**cceso
- **R**ectificación
- **C**ancelación
- **O**posición

IMPORTANCIA DE LA PROTECCIÓN DE DATOS PERSONALES

Es un derecho humano

Disminuye efectos de una vulneración

Evita responsabilidades

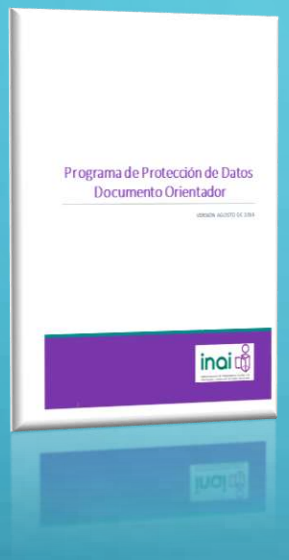
Incrementa confianza

MATERIALES DE FACILITACIÓN

Publicación de documentos, y otras referencias respecto al deber de seguridad

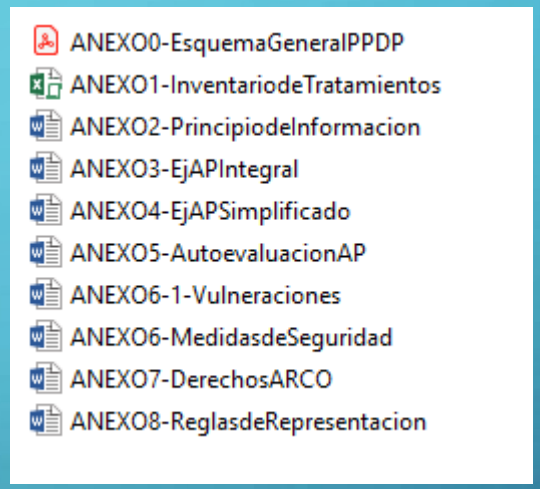
MATERIALES DE FACILITACIÓN

Publicación de documentos, y otras referencias respecto al deber de seguridad (Cont.)



Documento orientador para la elaboración del Programa de Protección de Datos Personales

9 agosto 2018

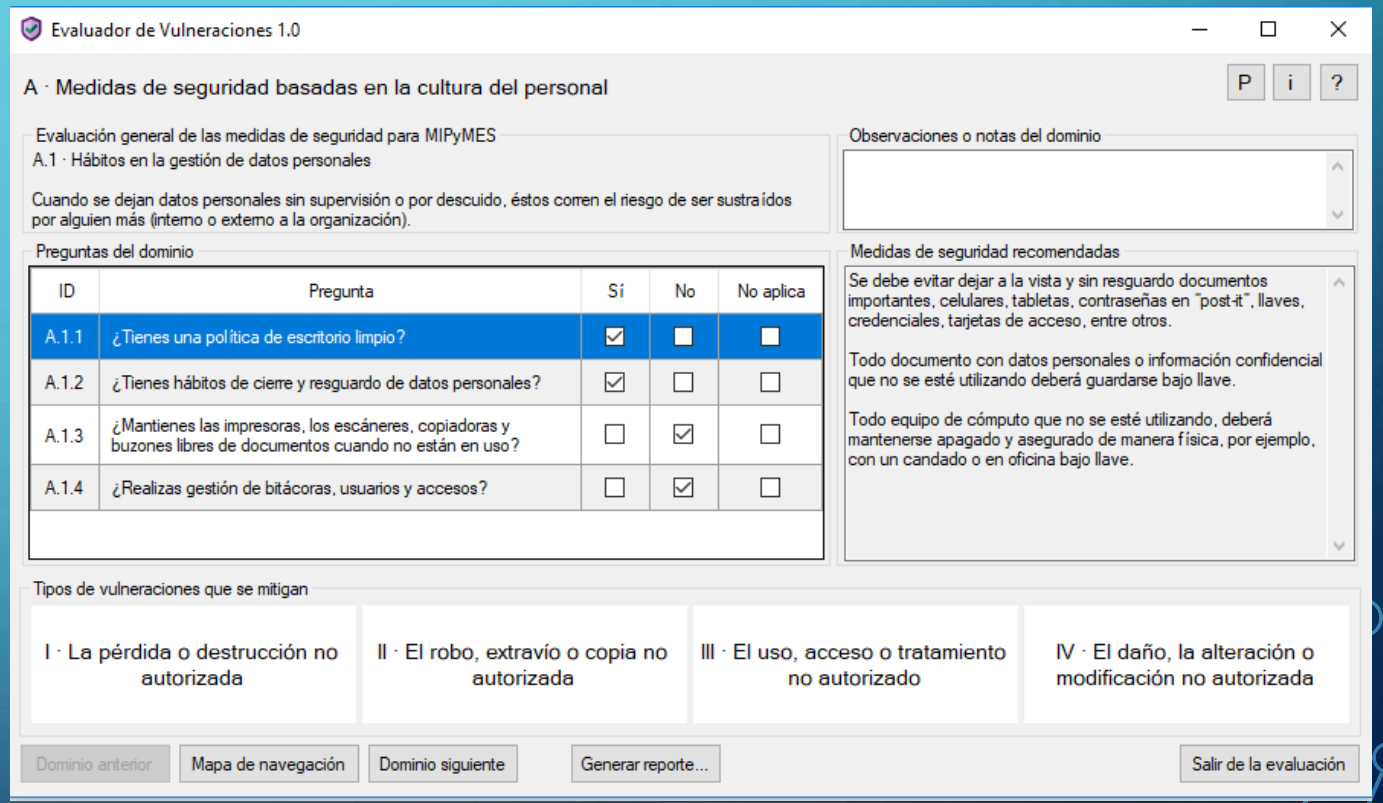


Anexos del documento orientador para la elaboración del Programa de Protección de Datos Personales

9 agosto 2018

HERRAMIENTAS

Evaluador de Vulneraciones



CONCEPTOS DE LA LEY GENERAL

Tratamiento

Medidas de seguridad

Base de datos

Sistema de Tratamiento

CONCEPTO DE DATO PERSONAL

Cualquier información concerniente a una persona física identificada o identificable.

- ✓ **Categorías**
- ✓ **Propiedades o atributos a preservar**

RESPONSABLE Y ENCARGADO

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

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;

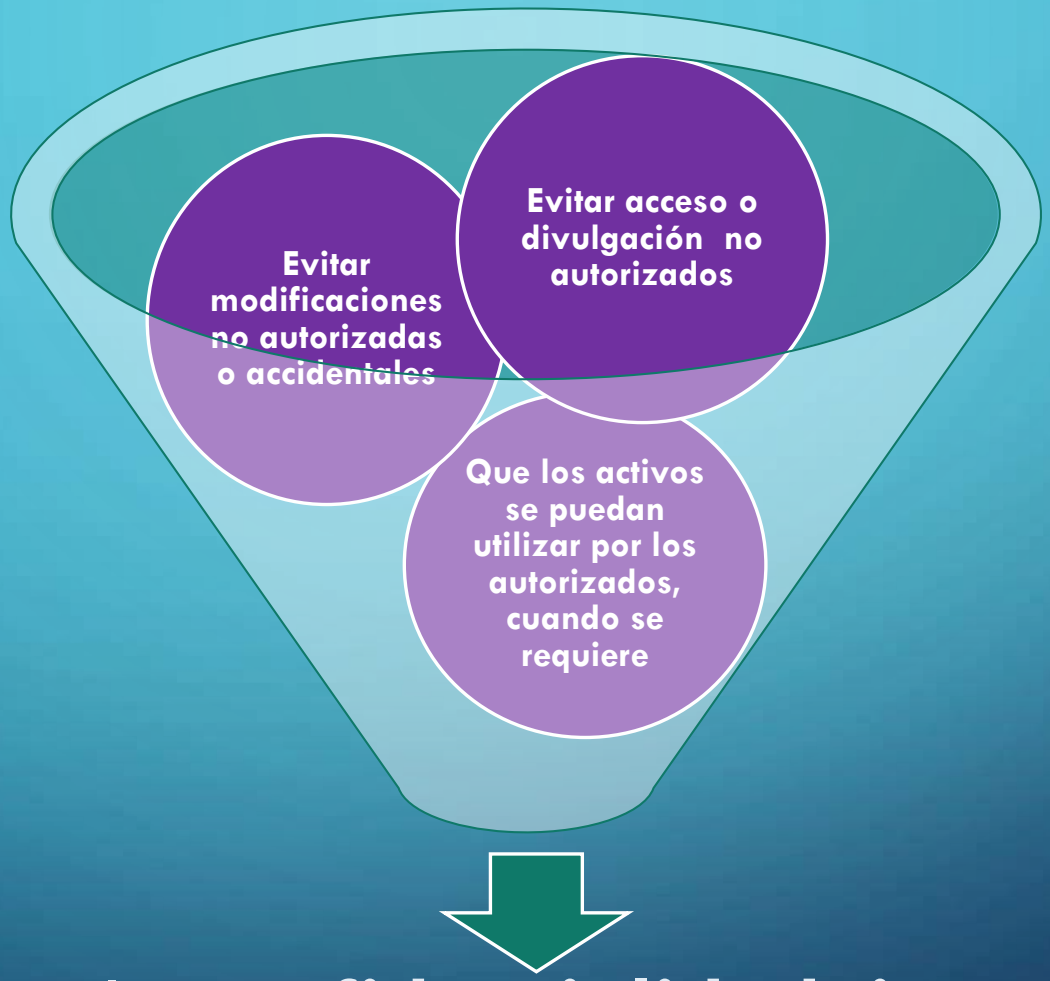
SISTEMA DE GESTIÓN

Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.

Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia.

Un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), generalmente se basa en el ciclo PHVA (Planear-Hacer-Verificar-Actuar).

SEGURIDAD DE LA INFORMACIÓN



Preservar la **confidencialidad, integridad** y **disponibilidad** de los **datos personales**

INTEGRIDAD

La propiedad de salvaguardar **la exactitud y completitud de los activos.**

- Evitar la modificación no autorizada o accidental.

CONFIDENCIALIDAD

Propiedad de la **información** para **no estar a disposición o ser revelada** a personas no autorizadas.

Prevenir la divulgación no autorizada de información.

DISPONIBILIDAD

Propiedad de un **activo** para ser **accesible y utilizable**.

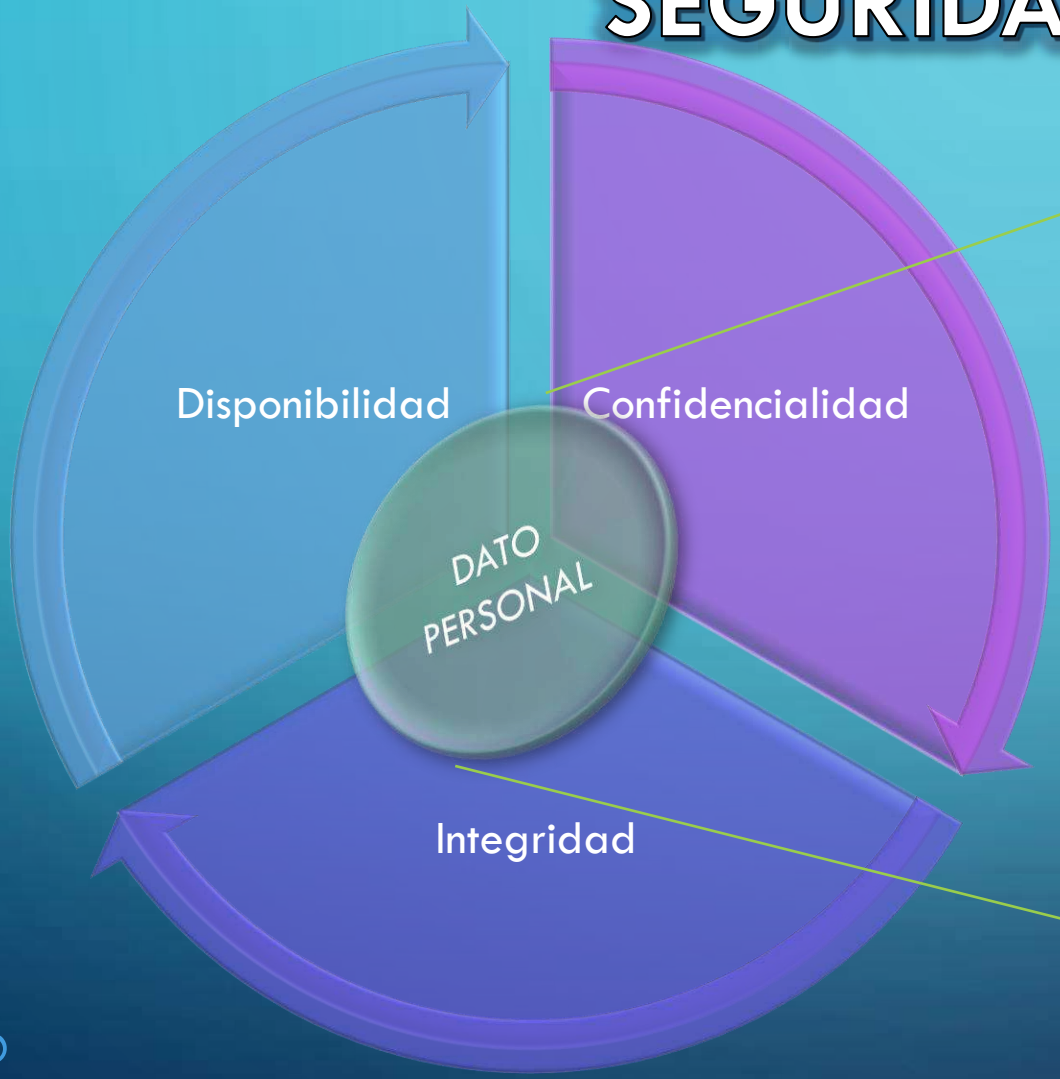
- Controlar las interrupciones de los recursos.
- Prevenir interrupciones no autorizadas.

EN RESUMEN...

Información **exacta y completa**, para ser revelada, accesible y utilizable sólo para las **personas autorizadas**.

Información correcta → para la persona correcta → en el momento correcto

DEBER DE SEGURIDAD Y MEDIDAS DE SEGURIDAD



MEDIDAS DE SEGURIDAD:

ADMINISTRATIVAS
FÍSICAS
TÉCNICAS

MEDIDAS DE SEGURIDAD Y SISTEMA DE GESTIÓN

PLANEAR

DOCUMENTO DE SEGURIDAD

HACER

REGISTROS DE MONITOREO Y SEGUIMIENTO

VERIFICAR

MECANISMOS DE VERIFICACIÓN Y AUDITORÍA

ACTUAR

MEDICIÓN Y MEJORA

EL DOCUMENTO DE SEGURIDAD EN EL MARCO DEL SISTEMA DE GESTIÓN

ACTIVIDADES MÍNIMAS

MEDIDAS DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS PERSONALES

- Políticas gestión y tratamiento de datos personales
- Funciones y obligaciones del personal que trata datos personales
- Inventario datos personales y sistemas de tratamiento
- Análisis de riesgos para datos personales
- Análisis de brecha medidas de seguridad
- Plan de trabajo medidas de seguridad
- Monitoreo y revisión periódica medidas seguridad
- Capacitación basada en niveles

Artículo 33 de la LGPDPPSO

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;

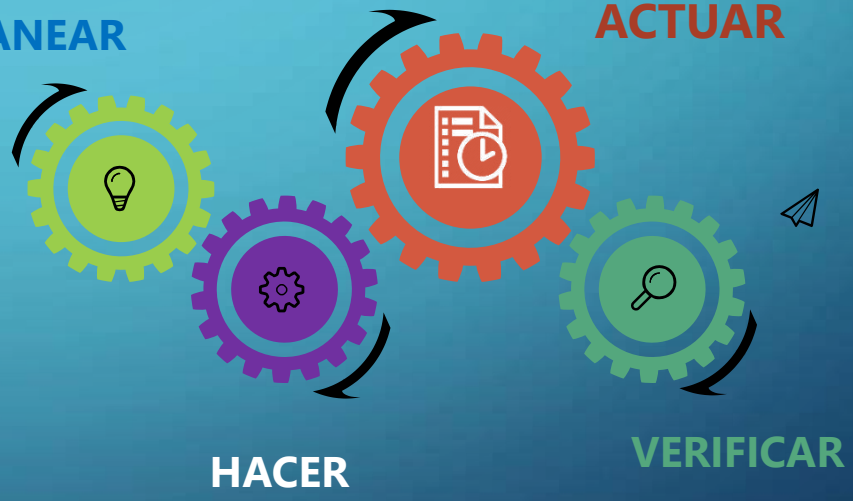
¿DÓNDE EMPIEZO?

SISTEMA DE GESTIÓN Y SISTEMA DE GESTIÓN DE SEGURIDAD

Artículo 34 de la LGPDPPSO

Las acciones relacionadas con las **medidas de seguridad** para el tratamiento de los datos personales deberán estar documentadas y contenidas en un **sistema de gestión**.

Sistema de Gestión



SGS - DATOS PERSONALES

Fase 1. Planear el SGSDP	• **Paso 1.** Establecer el Alcance y los Objetivos • **Paso 2.** Elaborar una Política de Gestión de Datos Personales • **Paso 3.** Establecer Funciones y Obligaciones • **Paso 4.** Elaborar un Inventario de Datos Personales • **Paso 5.** Realizar un Análisis de Riesgo de Datos Personales • **Paso 6.** Identificación de las medidas de seguridad y Análisis de Brecha
Fase 2. Implementar el SGSDP	• **Paso 7.** Implementación de las Medidas de Seguridad Aplicables a los Datos Personales
Fase 3. Monitorear y Revisar el SGSDP	• **Paso 8.** Revisiones y Auditoría
Fase 4. Mejorar el SGSDP	• **Paso 9.** Mejora Continua y Capacitación

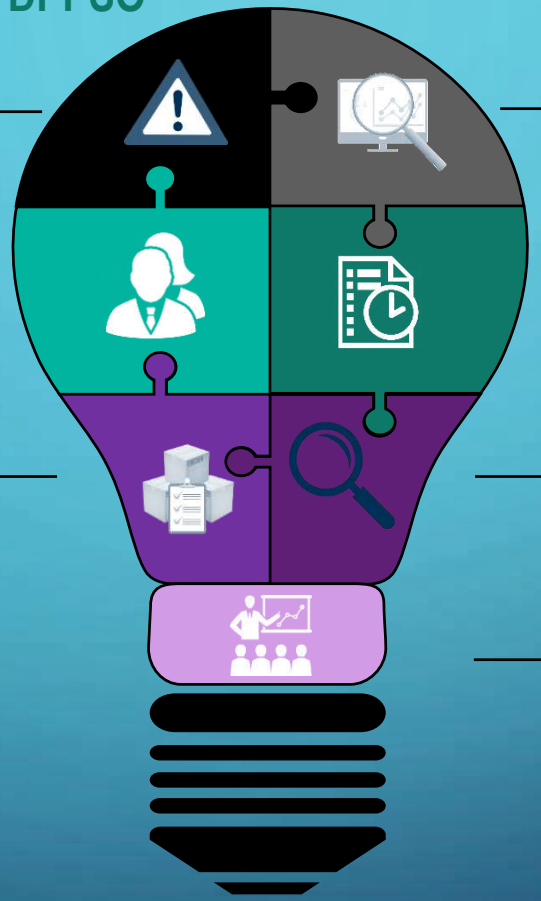
CONTENIDO DEL DOCUMENTO DE SEGURIDAD

Artículo 2 fracción XIV de la LGPDPPSO

Análisis de riesgos

Funciones y obligaciones

Inventario de datos personales



Análisis de brecha

Plan de trabajo

Mecanismos para monitoreo y revision medidas de seguridad

Programa general de capacitación

Artículo 35 de la LGPDPPSO

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;

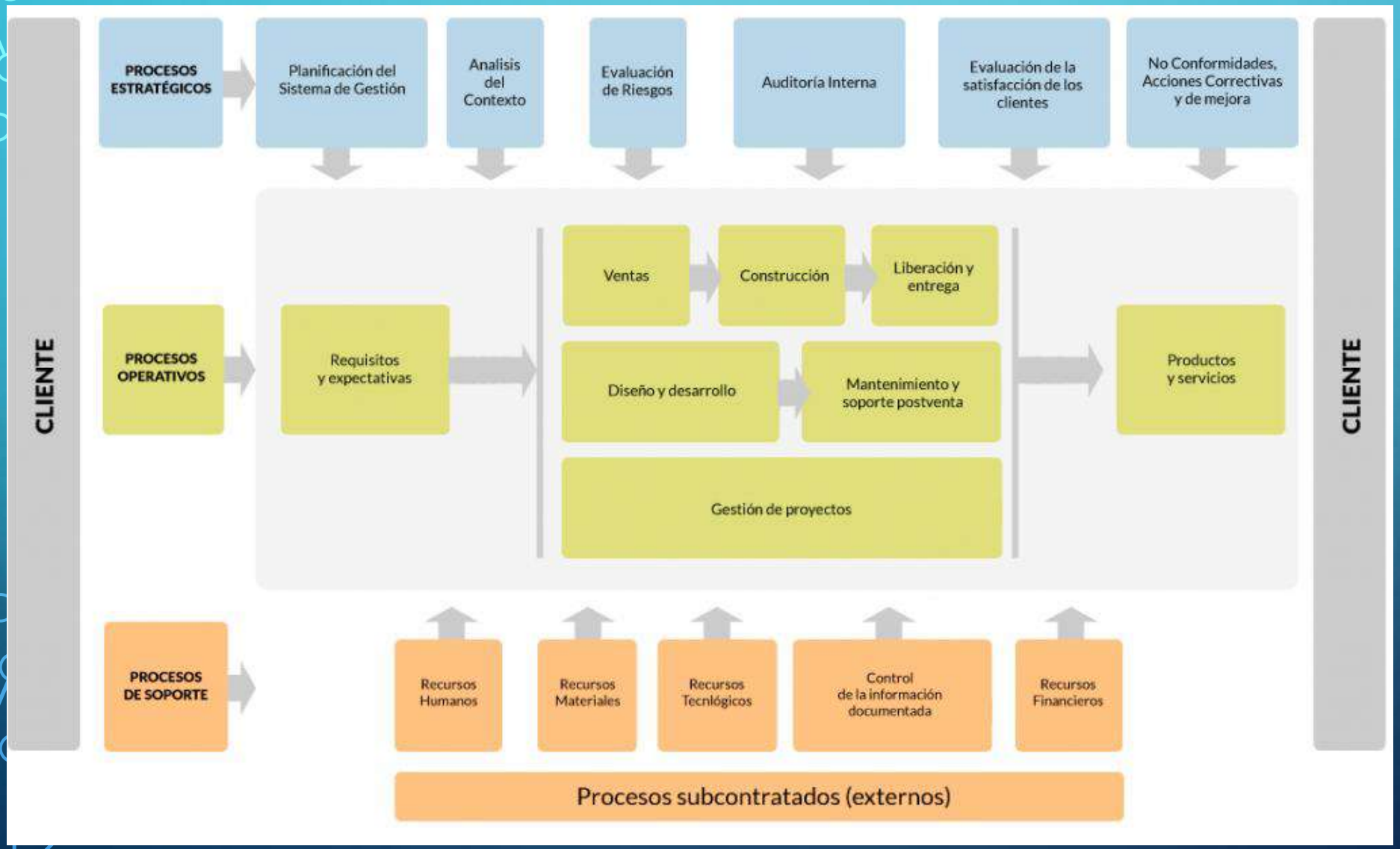
DS

MAPEO DE PROCESOS

PROCESOS ESTRATÉGICOS

PROCESOS OPERATIVOS

PROCESOS DE SOPORTE



Fuente: isotools.org / https://www.isotools.org/2016/05/11/mapa-procesos-nueva-iso-9001-2015/

TRÁMITES Y SERVICIOS

CICLO DE VIDA DEL DATO PERSONAL

TRÁMITE EN VENTANILLA (PETICIÓN CIUDADANA)

TRÁMITE EN VENTANILLA (PETICIÓN CIUDADANA)

Operación	Recepción solicitud en ventanilla	Turno y formación de expediente	Elaboración de respuesta	Notificación a la persona solicitante	Resguardo en archivo de trámite	Resguardo en archivo de concentración	Eliminación del expediente
Tipo de tratamiento	Obtención	Registro	Procesamiento	Disposición	Almacenamiento	Conservación	Supresión

CICLO DE VIDA DEL DATO PERSONAL

PRINCIPIOS

Licitud / Finalidad / Lealtad / Consentimiento / Calidad / Proporcionalidad / Información / Responsabilidad

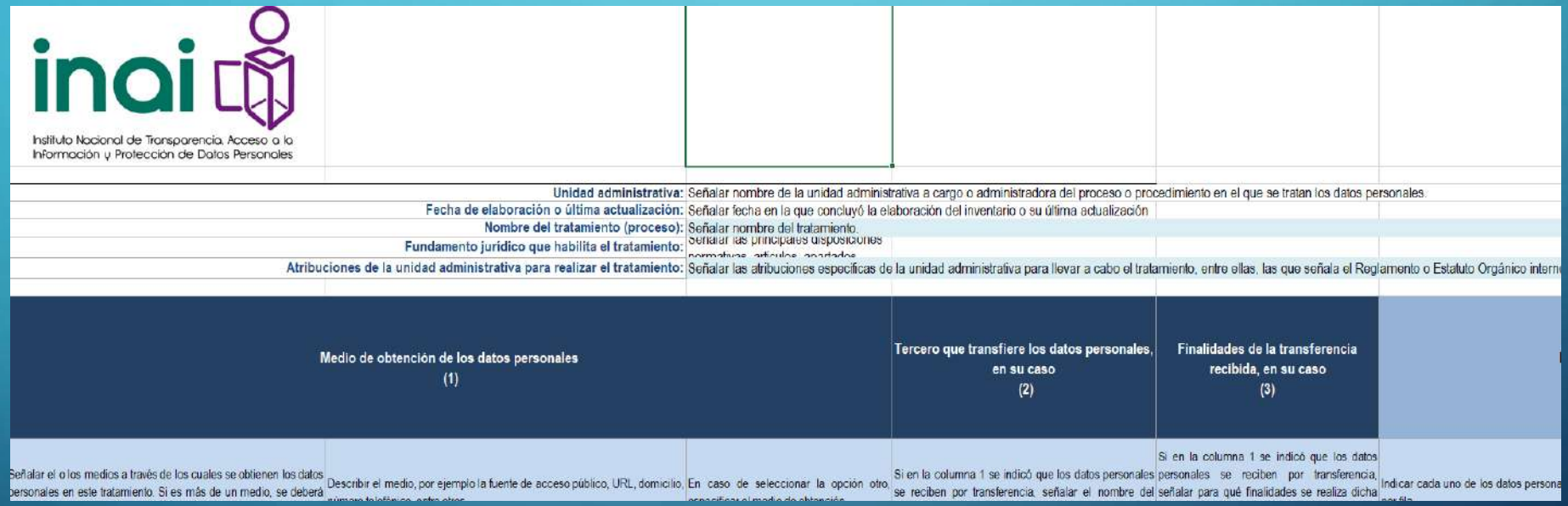
DEBERES

Seguridad / Confidencialidad

DIAGNÓSTICO

DOCUMENTO DE SEGURIDAD

I. El inventario de datos personales y de los sistemas de tratamiento



Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Unidad administrativa:	Señalar nombre de la unidad administrativa a cargo o administradora del proceso o procedimiento en el que se tratan los datos personales.
Fecha de elaboración o última actualización:	Señalar fecha en la que concluyó la elaboración del inventario o su última actualización
Nombre del tratamiento (proceso):	Señalar nombre del tratamiento.
Fundamento jurídico que habilita el tratamiento:	Señalar las principales disposiciones normativas, artículos, apartados
Atribuciones de la unidad administrativa para realizar el tratamiento:	Señalar las atribuciones específicas de la unidad administrativa para llevar a cabo el tratamiento, entre ellas, las que señala el Reglamento o Estatuto Orgánico interno

Medio de obtención de los datos personales (1)			Tercero que transfiere los datos personales, en su caso (2)	Finalidades de la transferencia recibida, en su caso (3)	
Señalar el o los medios a través de los cuales se obtienen los datos personales en este tratamiento. Si es más de un medio, se deberá	Describir el medio, por ejemplo la fuente de acceso público, URL, domicilio, número telefónico, entre otros	En caso de seleccionar la opción otro, especificar el medio de obtención	Si en la columna 1 se indicó que los datos personales se reciben por transferencia, señalar el nombre del	Si en la columna 1 se indicó que los datos personales se reciben por transferencia, señalar para qué finalidades se realiza dicha	Indicar cada uno de los datos persona perfil

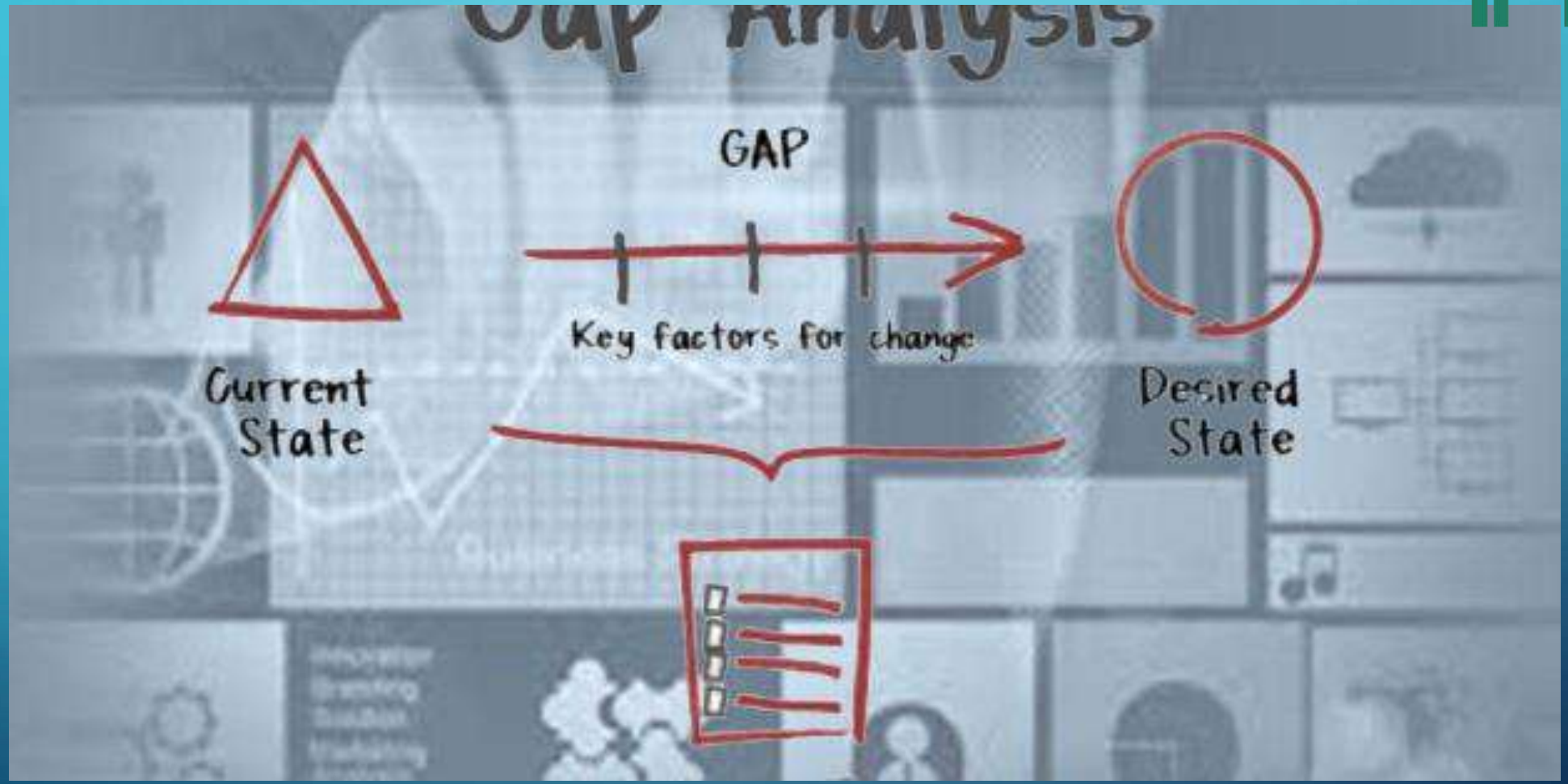
DOCUMENTO DE SEGURIDAD

II. Las funciones y obligaciones de las personas que traten datos personales

DOCUMENTO DE SEGURIDAD

III. El análisis de riesgos.

DOCUMENTO DE SEGURIDAD



IV. El análisis de brecha

DOCUMENTO DE SEGURIDAD

V. El Plan de trabajo

DOCUMENTO DE SEGURIDAD

VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y

DOCUMENTO DE SEGURIDAD

VII. Programa general de capacitación

ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

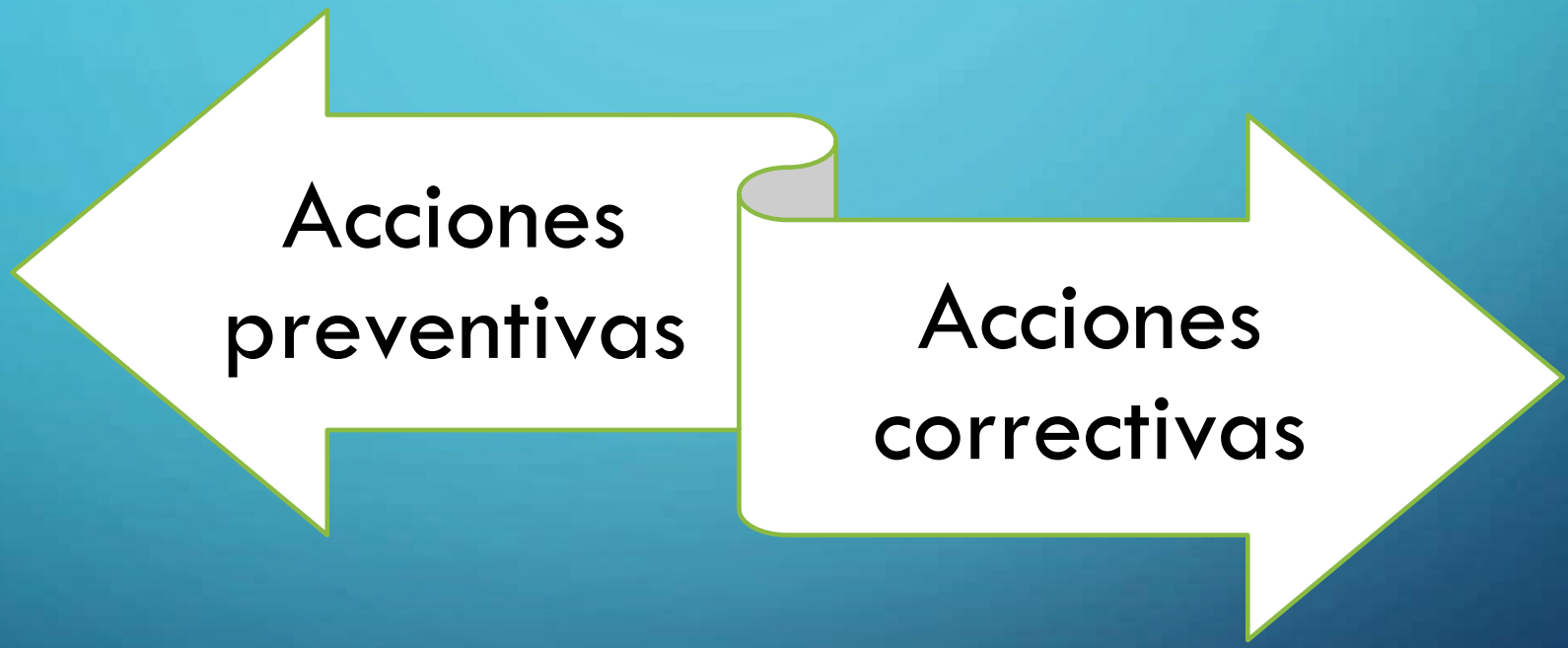
3 Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

1 Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;

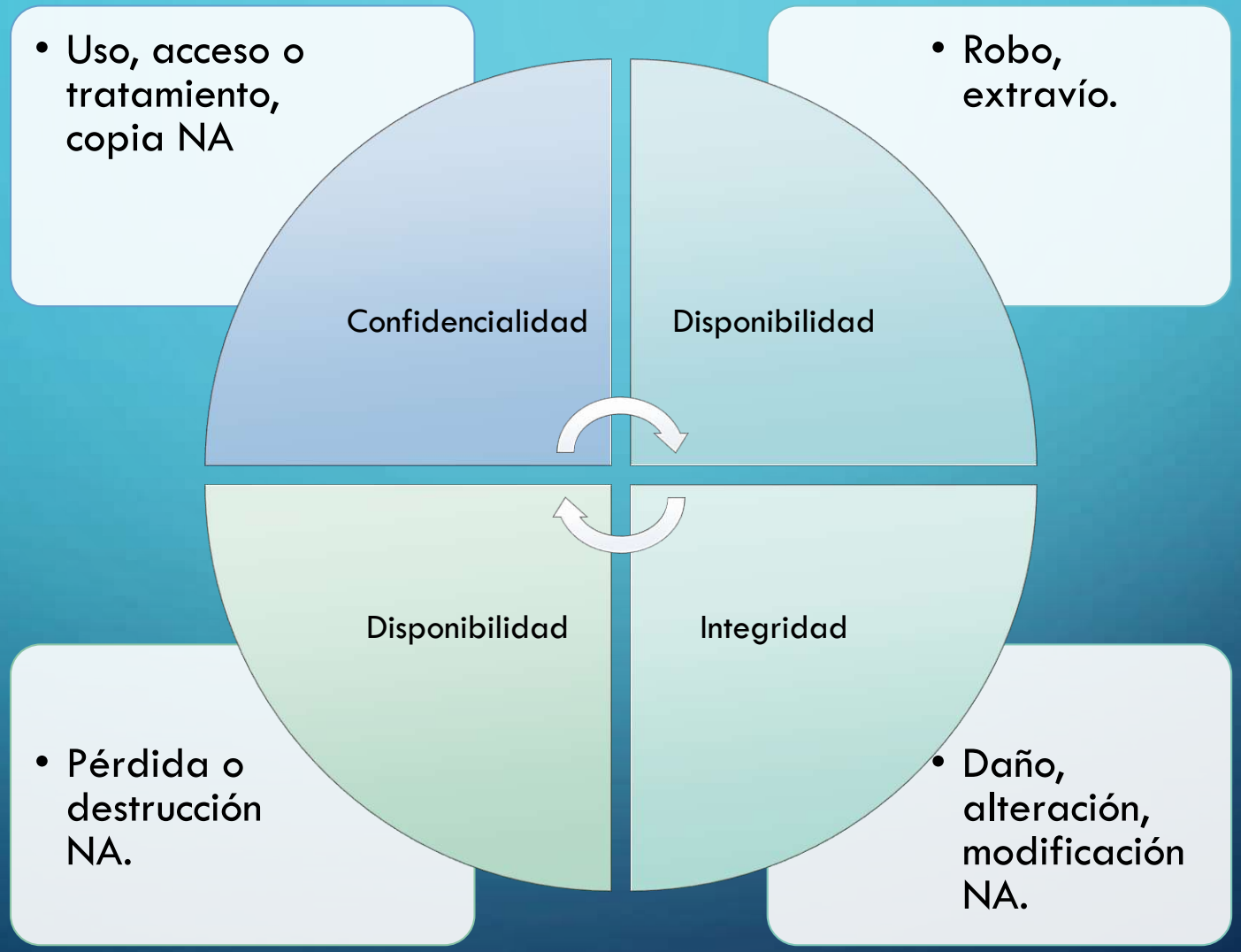
2 Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y

4 Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;

ACCIONES ANTE VULNERACIONES DE SEGURIDAD



VULNERACIONES DE SEGURIDAD



BITÁCORA DE VULNERACIONES E INCIDENTES

- Descripción.
- Fecha en la que ocurrió.
- Motivo
- Acciones correctivas implementadas de forma inmediata y definitiva

NOTIFICACIÓN

El responsable deberá informar sin dilación alguna al titular, y al Instituto las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

CONTENIDO DE LA NOTIFICACIÓN

- Naturaleza del incidente
- Datos personales comprometidos
- Medidas para proteger intereses
- Acciones correctivas inmediatas
- Medios donde puede obtener más información

SGS - DATOS PERSONALES

Fase 1. Planear el SGSDP	• **Paso 1.** Establecer el Alcance y los Objetivos • **Paso 2.** Elaborar una Política de Gestión de Datos Personales • **Paso 3.** Establecer Funciones y Obligaciones • **Paso 4.** Elaborar un Inventario de Datos Personales • **Paso 5.** Realizar un Análisis de Riesgo de Datos Personales • **Paso 6.** Identificación de las medidas de seguridad y Análisis de Brecha
Fase 2. Implementar el SGSDP	• **Paso 7.** Implementación de las Medidas de Seguridad Aplicables a los Datos Personales
Fase 3. Monitorear y Revisar el SGSDP	• **Paso 8.** Revisiones y Auditoría
Fase 4. Mejorar el SGSDP	• **Paso 9.** Mejora Continua y Capacitación

SGS - DATOS PERSONALES

Fase 1. Planear el SGSDP	• **Paso 1.** Establecer el Alcance y los Objetivos • **Paso 2.** Elaborar una Política de Gestión de Datos Personales • **Paso 3.** Establecer Funciones y Obligaciones • **Paso 4.** Elaborar un Inventario de Datos Personales • **Paso 5.** Realizar un Análisis de Riesgo de Datos Personales • **Paso 6.** Identificación de las medidas de seguridad y Análisis de Brecha
Fase 2. Implementar el SGSDP	• **Paso 7.** Implementación de las Medidas de Seguridad Aplicables a los Datos Personales
Fase 3. Monitorear y Revisar el SGSDP	• **Paso 8.** Revisiones y Auditoría
Fase 4. Mejorar el SGSDP	• **Paso 9.** Mejora Continua y Capacitación

SGS - DATOS PERSONALES

Fase 1. Planear el SGSDP	• **Paso 1.** Establecer el Alcance y los Objetivos • **Paso 2.** Elaborar una Política de Gestión de Datos Personales • **Paso 3.** Establecer Funciones y Obligaciones • **Paso 4.** Elaborar un Inventario de Datos Personales • **Paso 5.** Realizar un Análisis de Riesgo de Datos Personales • **Paso 6.** Identificación de las medidas de seguridad y Análisis de Brecha
Fase 2. Implementar el SGSDP	• **Paso 7.** Implementación de las Medidas de Seguridad Aplicables a los Datos Personales
Fase 3. Monitorear y Revisar el SGSDP	• **Paso 8.** Revisiones y Auditoría
Fase 4. Mejorar el SGSDP	• **Paso 9.** Mejora Continua y Capacitación

ACTUALIZACIÓN DE MEDIDAS DE SEGURIDAD

EVALUACIÓN DEL RIESGO

CONTEXTO E IDENTIFICACIÓN DEL RIESGO

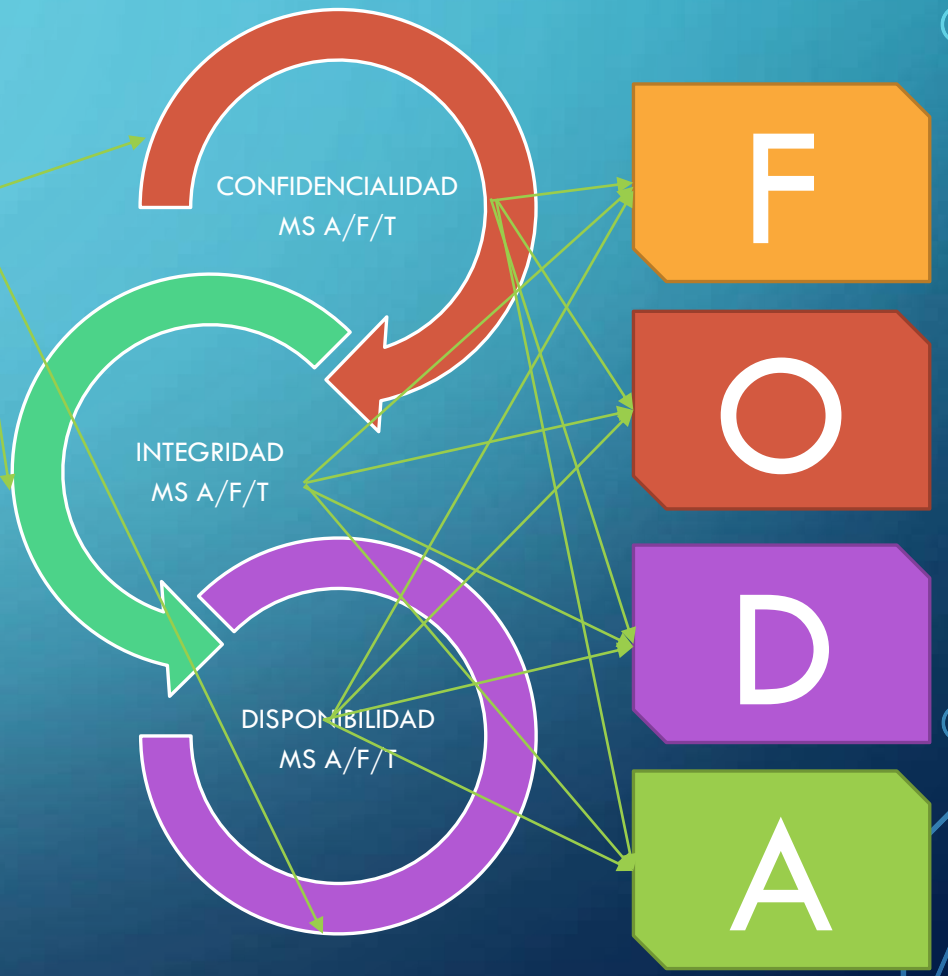
ASPECTOS A CONSIDERAR

- Riesgo inherente
- Sensibilidad de los datos
- Desarrollo tecnológico
- Consecuencias de vulneraciones
- Transferencias
- Número de titulares
- Vulneraciones previas
- Valor potencial

TRATAMIENTO DP´S Y ATRIBUTOS

- TRATAMIENTOS GENERALES DE LA ORGANIZACIÓN (PROCESOS O MACROPROCESOS PRINCIPALES)
- TRATAMIENTO ESPECÍFICO
- TRATAMIENTO ESPECÍFICO
- TRATAMIENTO ESPECÍFICO

DESCRIPCIÓN



ANÁLISIS DEL RIESGO

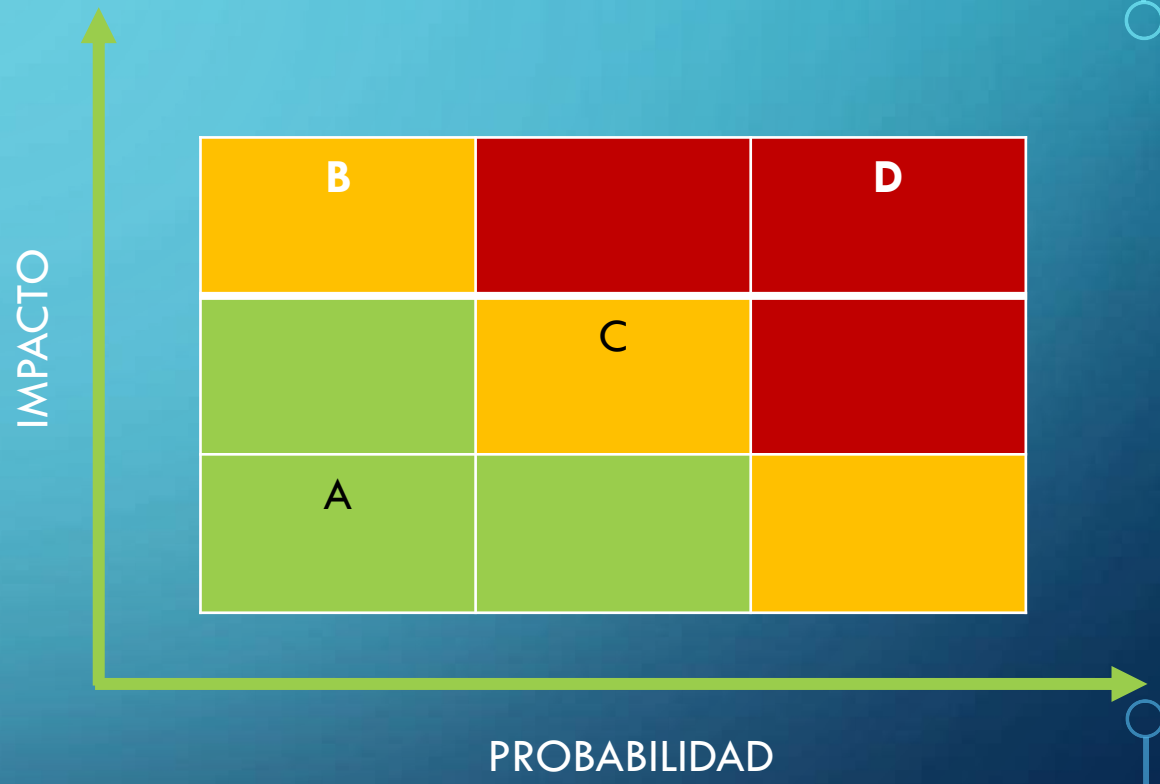
ELEMENTOS A CONSIDERAR
TIPO DE ANÁLISIS
TÉCNICA(S) DE ANÁLISIS
DETERMINACIÓN DE NIVELES DE RIESGO
DETERMINACIÓN DE ENFOQUE BASADO EN CONSECUENCIAS

- CUALITATIVO / CUANTITATIVO
- GENERALES / PARTICULARES /MIXTAS
- SEMAFORIZACIÓN (BAJO/MEDIO/ ALTO)
- PROBABILIDAD / IMPACTO

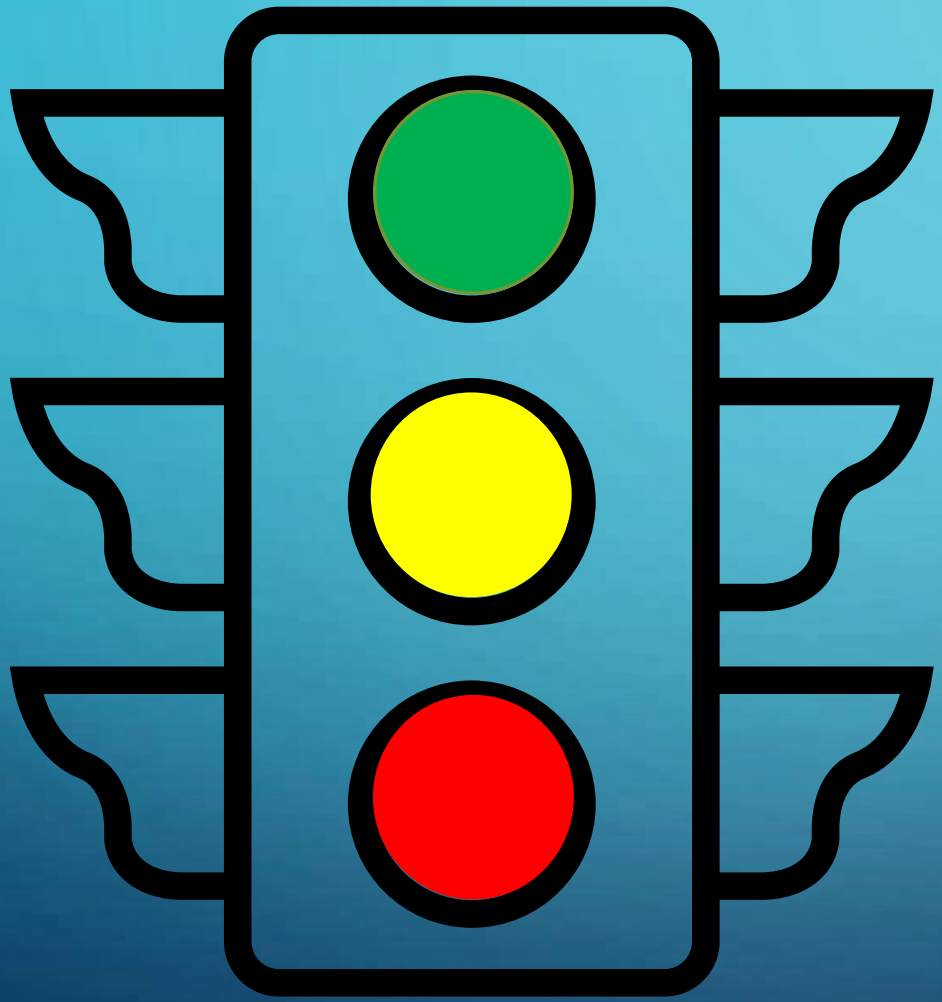
ANÁLISIS DEL RIESGO

EJEMPLO DE RIESGO
A. DIVULGACIÓN DE DATOS PERSONALES EN OFICINAS
B. DIVULGACIÓN DE DATOS PERSONALES EN RECURSOS DE REVISIÓN
C. DIVULGACIÓN DE DATOS PERSONALES EN VERSIONES PÚBLICAS
D. DIVULGACIÓN DE DATOS PERSONALES EN SUS SISTEMAS INFORMÁTICOS EN RED

PROBABILIDAD	IMPACTO	RESULTADO
BAJA (1)	BAJA (1)	BAJO (1)
BAJA (1)	ALTA (3)	BAJA (3)
MEDIA (2)	MEDIA (2)	MEDIO (4)
ALTA (3)	ALTA (3)	ALTA (9)



VALORACIÓN Y TRATAMIENTO DEL RIESGO



ANÁLISIS - VALORACIÓN

ACEPTAR / EXPLOTAR

MONITOREAR

CONTROLAR / EVITAR / TRASLADAR

¿Se puede gestionar?

No

Sí

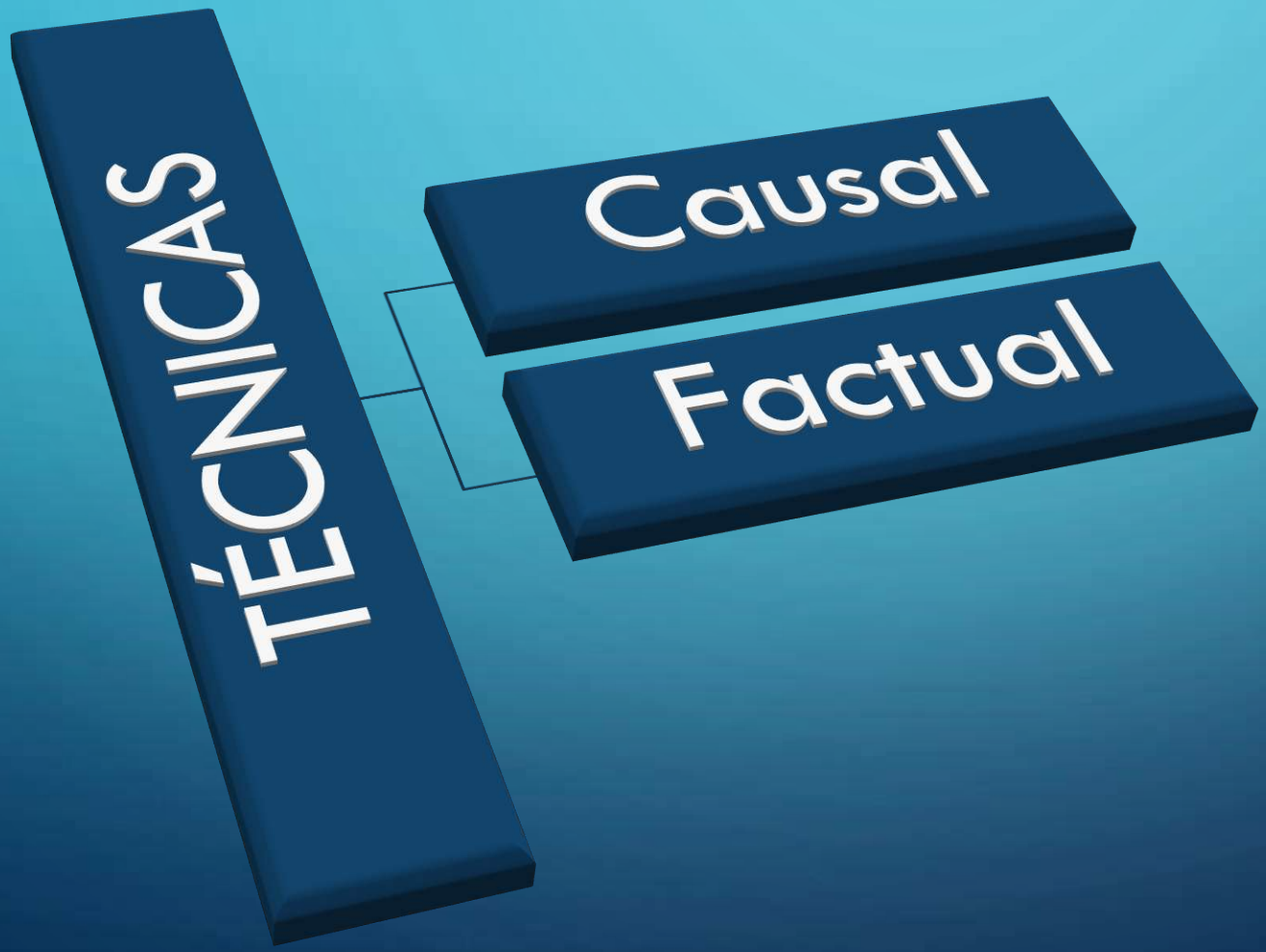
Análisis de brecha

PLAN DE TRABAJO

DOCUMENTO DE SEGURIDAD
MS- ADTIVAS
MS- FÍSICAS
MS- TÉCNICAS

TRATAMIENTO DEL RIESGO

TRATAMIENTO DEL RIESGO (ANÁLISIS DE BRECHA)



MONITOREO Y REVISIÓN DEL RIESGO

PROGRAMA DE TRABAJO

- PLAN DE TRABAJO
- PLAN DE TRABAJO
- PLAN DE TRABAJO
- PLAN DE TRABAJO
- PLAN DE TRABAJO
- PLAN DE TRABAJO

DOCUMENTO DE SEGURIDAD

@INAImexico

inicio.inai.org.mx

atencion@inai.org.mx

¡GRACIAS!

MDTIC. Luis Ricardo Sánchez Hernández, Director General de Normatividad y Consulta
normatividadyconsulta@inai.org.mx