Instituto Nacional Electoral

Programa de Seguridad de la Información

Aplicado a la protección de datos personales

Introducción

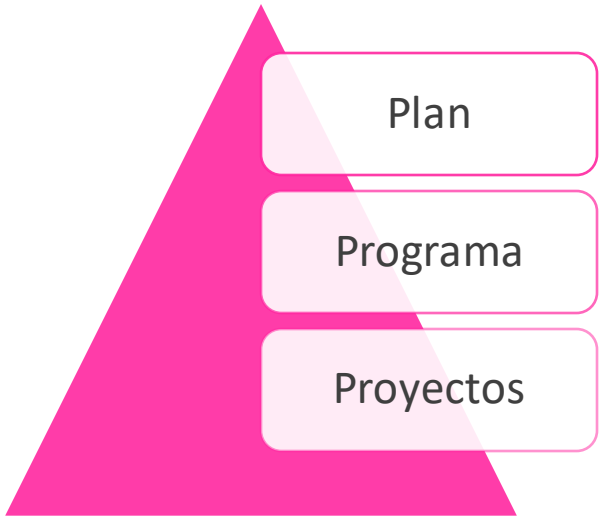
1. Esta presentación es un apoyo para la atención del control **D6.13 Monitoreo y supervisión continuo de las medidas de seguridad implementadas**, correspondiente al **Dominio 6. Gestión de la seguridad en el tratamiento de los datos personales del SiPRODAP.**

2. **Objetivo del control**: *Que la evaluación y medición de los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales sean verificados a través de un Programa de seguridad de la información que incorpore las acciones correspondientes*.

3. Actividades de control. El Programa debe atender, al menos:
   - Nuevos activos que se incluyan en la gestión de riesgos.
   - Modificaciones necesarias a los activos, -cambio o migración tecnológica, entre otras-.
   - Nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas.
   - Posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.
   - Vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.
   - Cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.
   - Incidentes y vulneraciones de seguridad ocurridas.

I. Definiciones

- **Plan.**
  - Documento de trabajo que recopila y concreta los objetivos que se desean alcanzar durante un periodo de tiempo.
  - Tiene como punto de partida un diagnóstico de la situación y detalla un conjunto de acciones a realizar.
  - Engloba un conjunto de programas y proyectos.
- **Programa**:
  - Documento que concreta un conjunto de acciones orientadas a alcanzar metas y objetivos de un plan.
  - Suelen estar compuestos por un conjunto de proyectos.
- **Proyecto**:
  - Conjunto de actividades concretas, interconectadas y coordinadas entre sí, con el fin de satisfacer necesidades o resolver problemas.
  - Tienen fecha de inicio y fin con objetivos específicos.
  - Se caracteriza por contar con recursos (humanos y financieros).
  - Forman parte de un programa.



Fuente: https://talentosreunidos.com/2017/06/20/planes-proyectos-y-programas/

II. Programa

- Es el elemento indispensable en el cual se encuentran acciones, servicios o procesos organizados sistemáticamente, de manera coherente e integrada, con tiempos y responsables definidos.
- Se realiza con el fin de alcanzar las metas y objetivos propuestos a través de un conjunto de proyectos.
- Pueden ser de corto, mediano o largo plazo.

Fuente:
http://ri.uaemex.mx/bitstream/handle/20.500.11799/112123/Conceptos%20y%20diferencias%20de%20plan%20programa%20y%20proyecto.pdf?sequence=1&isAllowed=y

Programa de Seguridad de la Información

- Es el proceso a través del cual se **definen, planean, implementan, operan, miden, monitorean, mantienen y mejoran** los sistemas de seguridad de la organización.

III. Características

- Temporalidad permanente (por ciclos).
- Debe perseguir objetivos concretos a largo plazo que se desean alcanzar.
- Conformado por un conjunto de proyectos, iniciativas y actividades realizadas de manera coordinada para lograr una estrategia de seguridad.
- Pretende dirigir, monitorear, evaluar y mejorar todas las actividades relacionadas con la seguridad, así como brindar información oportuna que permita tomar las mejores decisiones para la protección del negocio, la información y otros activos.

Fuente: https://www.welivesecurity.com/la-es/2017/01/11/desarrollo-programa-de-seguridad-informacion/

IV. Recursos

- **Tiempo**. Es el primer recurso necesario para el Programa, tanto para el desarrollo de la estrategia como su posterior aplicación y ejecución. Por la característica de no tener principio ni fin, el programa puede observarse como un proceso de mejora continua que opera en diferentes ciclos. Para el establecimiento de las prioridades se deben considerar factores como los continuos cambios en los riesgos, las prioridades de la Dirección con respecto a la protección de activos, nuevas amenazas y vulnerabilidades, entre otras. La temporalidad debe estar alineada con el tiempo de atención establecido en el Plan de Trabajo del Documento de Seguridad.
- **Recursos financieros**. Determinar los recursos financieros necesarios para alcanzar el estado deseado en materia de seguridad de la información. Se debe tener en mente que la estrategia puede derivar en la aplicación de controles técnicos, físicos o administrativos.
- **Personas**. La organización debe contar con personal con las habilidades, capacidades o conocimientos necesarios para llevar a cabo las actividades técnicas y administrativas relacionadas con el Programa, por lo que puede optar por capacitar a miembros de la organización o contratar los servicios de personal con estas aptitudes.

V. Elementos para conformar el Programa

El Programa debe contener, al menos, los siguientes apartados:

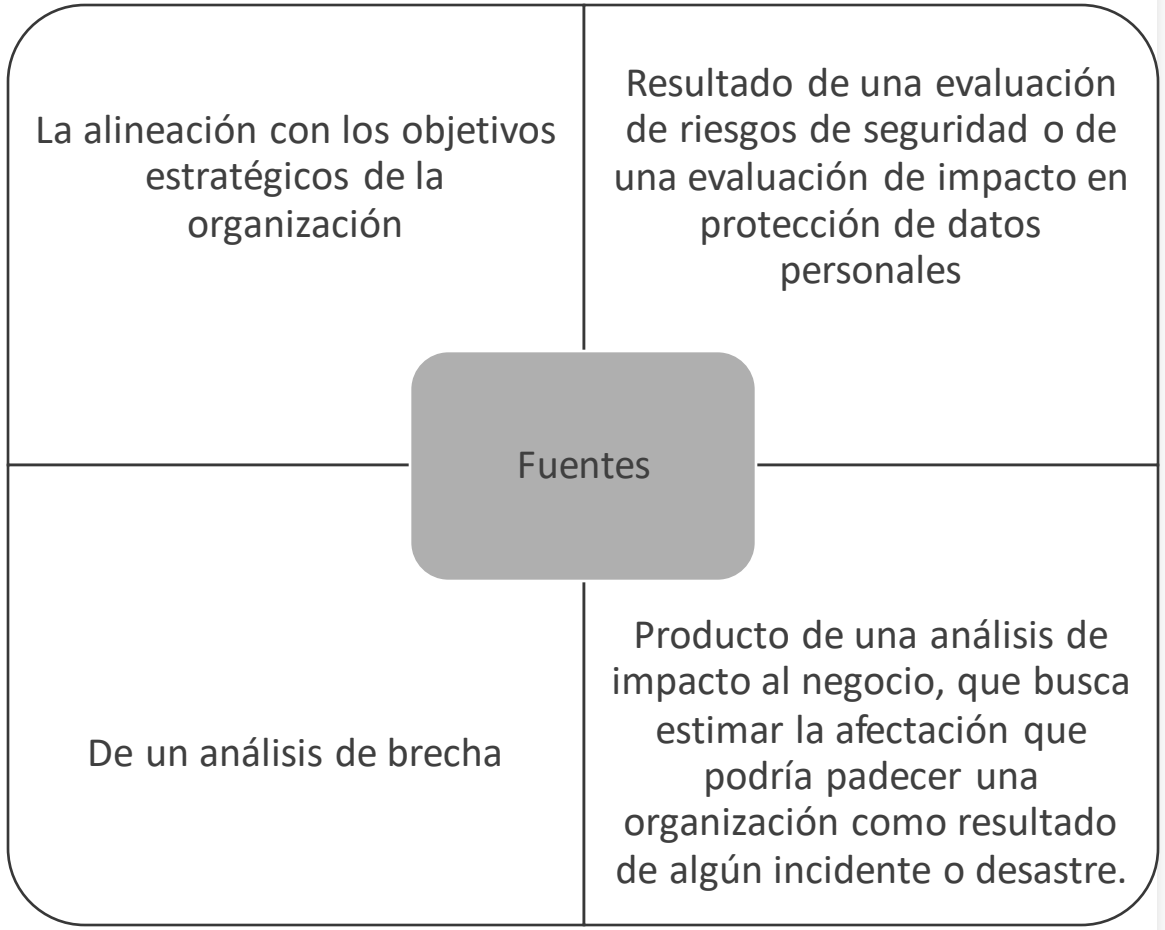
1. Objetivo general
2. Objetivos específicos
3. Alcance
4. Marco legal
5. Medidas de seguridad
6. Mecanismos de monitoreo y supervisión

Descarga la plantilla para conformar el Programa

1. Objetivo general

- Diseñar el objetivo del programa considerando que:
  a) Debe garantizar que los datos y la información no se vean comprometidos por acceso no autorizado, uso indebido o destrucción intencional.
  b) El Programa es un documento que expone las prioridades de implementación de los controles en relación con seguridad de la información enmarcado en el ciclo de mejoramiento continuo PHVA (planear, hacer, verificar y actuar).
  c) Debe dirigir la implementación de controles de seguridad.

2. Objetivos específicos



3. Alcance

- Determinar el alcance considerando los resultados de análisis de brecha (señalando la norma ISO/IEC aplicable), análisis de riesgos y en su caso evaluaciones de impacto.
- Incluir las áreas involucradas (pueden ser diferentes Unidades administrativas, Direcciones de área o subdirecciones)

4. Marco legal

Marco normativo aplicable:

Leyes

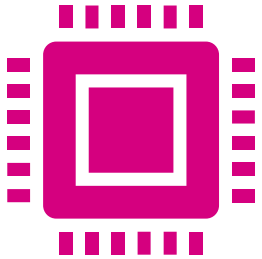
Lineamientos

Reglamentos

Manuales

Guías

Procedimientos



En caso de aplicar, estándares especializados de la industria, como:

Cómputo en la nube

Biometría

Financieros

Entro otros

5. Medidas de seguridad

- Incluir:
  - Un resumen de las medidas de seguridad del Plan de trabajo que incluirá el programa.
  - Una descripción detallada de las medidas de seguridad del punto anterior.

5. Medidas de seguridad

Medidas de seguridad por implementar o mejorar	Periodo		
	Corto plazo (hasta 6 meses)	Mediano plazo (de 7 meses a 1 año)	Largo plazo (más de 1 año)
Físicas	*0*	*1*	*3*
Técnicas	*1*	*0*	*2*
Administrativas	*3*	*1*	*1*
Total	***4***	***2***	***6***

ID	Medida de seguridad	Tipo	Descripción	Periodo	¿Requiere proyecto?	Detalles del proyecto	
						Estado	Año
1	*Contratación de un Circuito Cerrado de televisión (CCTV)*	*Técnica / física / administrativa*	*Contratación de un servicio para la instalación de cámaras de videovigilancia en las oficias de la unidad responsable donde son tratados datos personales.*	*Corto / mediano / largo plazo*	*Sí / No*	*Programado*	*2024*

6. Mecanismos de monitoreo y supervisión de las medidas de seguridad

- Nuevos activos que se incluyan en la gestión de riesgos.
- Modificaciones necesarias a los activos, -cambio o migración tecnológica, entre otras-.
- Nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas.
- Posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.
- Vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.
- Cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.
- Incidentes y vulneraciones de seguridad ocurridas

6. Mecanismos de monitoreo y supervisión de las medidas de seguridad

- El monitoreo y la supervisión se realizarán a través de un Cuadro de resultados, debiendo elaborar un cuadro por año (de acuerdo con el periodo que abarca el Programa).

Cuadro de resultados 202x					
Datos generales de las medidas de seguridad		Resultado del monitoreo y supervisión			
ID	Medida de seguridad	Nivel de implementación	Eficacia	Fecha de implementación	Justificación en caso de que la medida no esté implementada
1	*Contratación de un Circuito Cerrado de televisión (CCTV)*	*Implementada parcialmente*	*Moderada*	*enero de 2024*	

Cuadro de resultados

Nivel de implementación

- No implementada: la medida de seguridad no existe (0 al 15%).
- Parcialmente implementada: Incompleta (16-50%).
  - Características: Hay múltiples oportunidades de mejora; no se encuentra documentada.
- Ampliamente implementada: implementada en su mayor parte (51-85%).
  - Características: La medida de seguridad se encuentra documentada; cuenta con recursos suficientes para su mantenimiento.
- Completamente implementada totalmente: Completa (86-100%)
  - Características: la medida de seguridad está alineada a las políticas (u otras directivas institucionales); son asignadas responsabilidades, con rendición de cuentas identificada; el personal que opera la medida de seguridad cuenta con las habilidades y conocimientos adecuados; la efectividad de la medida de seguridad es evaluada y, en su caso, optimizada.

Eficacia

- Muy baja: Solo protege contra el 2% inferior de una amenaza promedio.
- Baja: Solo protege contra el 16% inferior de una amenaza promedio.
- Moderada: Protege contra una amenaza promedio.
- Alta: Protege contra todo, menos el 16% superior de amenaza promedio
- Muy alta: Protege contra todo, menos el 2% superior de amenaza promedio.

Instituto Nacional Electoral

Gracias

Subdirección de Gobierno de Datos Personales

DAIPDP-UTTyPDP