Cuadernillo práctico para integrar de la gestión de riesgos en la elaboración o desarrollo del documento de seguridad

febrero 2025

DIRECTORIO

Adrián Alcalá Méndez
Comisionado Presidente

Josefina Román Vergara
Comisionada

Blanca Lilia Ibarra Cadena
Comisionada

Norma Julieta Del Río Venegas
Comisionada

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

Secretaría de Protección de Datos Personales

Dirección General de Prevención y Autorregulación

Dirección de Seguridad de Datos Personales del Sector Público
Av. Insurgentes 3211,
Colonia Insurgentes Cuicuilco, Alcaldía Coyoacán,
Ciudad de México, C. P. 04530.

Edición febrero de 2025

NOTA

El presente documento desarrolla únicamente la práctica a partir de sugerencias para entender mejor el desarrollo de actividades, la teoría se encuentra en los documentos de facilitación asociados al cumplimiento del deber de seguridad publicados por el INAI.

ÍNDICE

DIRECTORIO *1*

NOTA *2*

ÍNDICE *3*

Primera actividad – Definición del inventario de sistemas de tratamiento *4*

Segunda actividad – Definición de elementos para llevar a cabo la gestión de riesgos *10*

Definición de escalas **10**

Identificación del riesgo **13**

Análisis del riesgo **13**

Evaluación del riesgo **13**

Tratamiento del riesgo **14**

Tercera actividad – Definición de ruta de trabajo a partir de los resultados obtenidos para gestionar el riesgo *16*

Primera actividad – Definición del inventario de sistemas de tratamiento

Un sistema de tratamiento comprende todos los activos físicos y digitales en los que se obtienen, procesan, comunican, transfieren y/o almacenan datos personales, es decir, en todos los elementos en los que se tratan datos personales.

A fin de generar un inventario de sistema de tratamiento, es necesario que inicialmente se identifique el ciclo de vida de los datos personales, dónde se recomienda dar respuesta a las siguientes preguntas:

Módulo 1: Aspectos generales

Pregunta	Respuesta
Nombre del sujeto obligado:	
Nombre de la unidad administrativa que declara el sistema de tratamiento:	
Nombre del tratamiento:	
Fundamento jurídico que habilita el tratamiento:	
Atribuciones de la unidad administrativa para realizar el tratamiento:	
Finalidades de tratamiento:	
¿Qué tipo de consentimiento requieren las finalidades?:	○ Tácito ○ Expreso y por escrito

Módulo 2: Medio de obtención de los datos personales

Pregunta	Respuesta
Como obtiene los datos personales a tratar:	○ Directamente de la persona titular ○ De manera personal con la presencia física del titular de los datos personales o su representante, en su caso ○ Vía telefónica ○ Correo electrónico ○ Sistema informático ○ Escrito o formato presentado directamente por el Responsable del tratamiento de datos personales ○ Escrito o formato enviado al Responsable del tratamiento de datos personales por mensajería ○ Fuente de acceso público ○ Otro ○ Mediante una transferencia ○ De quien recibe la transferencia
¿Qué datos personales trata?:	
Dentro de los datos personales que trata, ¿Existen datos sensibles?:	
¿En qué formato se encuentran los datos personales?:	○ Físico ○ Digital ○ En ambos
¿En qué lugar se encuentran los datos personales tratados?:	Físico ○ Físicamente en un archivero ○ Físicamente en un cajón o espacio designado ○ En una bodega ○ En un archivo Digital ○ En la nube ○ En los servidores de la institución ○ En servidores administrados por un tercero ○ En equipos de computo ○ En dispositivos de almacenamiento extraíble

Módulo 3: Personal con acceso a los datos personales

Puesto de la persona que tiene acceso	Unidad administrativa a la que pertenece	Razones por las que tiene acceso a los datos personales

Módulo 4: Remisiones

Pregunta	Respuesta
Nombre de la o las personas físicas o morales que actúan como encargados en el tratamiento:	
Clave, siglas o identificador del instrumento jurídico que regula la relación con el encargado	

Módulo 5: Transmisiones

Pregunta	Respuesta
Nombre, razón o denominación social de los terceros a los que se transfieren los datos personales:	
Finalidades para las cuales se transfieren los datos personales por cada uno de los terceros:	
¿Qué tipo de consentimiento requieren las finalidades?:	○ No requiere ○ Tácito ○ Expreso y por escrito
Suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico	

Módulo 6: Fin del ciclo de tratamiento

Pregunta	Respuesta
¿Realiza difusión de datos personales?:	
Señale el plazo de conservación de los datos personales, según lo señalado en los instrumentos de clasificación archivística:	
Señale el periodo en el que estarán bloqueados los datos personales:	
Espacio libre para hacer aclaraciones y precisiones:	

Segunda actividad – Definición de elementos para llevar a cabo la gestión de riesgos

Definición de escalas

I. TIPOS DE ESCALA

1. **ESCALA CUALITATIVA:** Los datos cualitativos se expresan en forma de palabras o textos que ayudan a comprender ciertas acciones que no son cuantificables
2. **ESCALA CUANTITATIVA:** Los datos cuantitativos consisten en cualquier información cuantificable que pueda utilizarse para realizar cálculos matemáticos y análisis estadísticos
3. **ESCALA COMBINADA:** Los datos combinados se refieren a una combinación entre las escalas definidas anteriormente.

II. ESCALA PARA PROBABILIDAD

- **Probabilidad por frecuencia:** Es la valoración más recomendable ya que incluye una evidencia que sustenta el cálculo realizado.
- **Probabilidad por factibilidad:** Es la evaluación de la magnitud de las consecuencias de un evento en caso de que ocurriera, la asignación de un valor a las consecuencias asociadas; esta probabilidad surge como una alternativa, cuando no se tienen datos registrados. Para esta probabilidad se pueden hacer estimaciones subjetivas que reflejen el grado de creencia de un individuo o grupo con respecto a la probabilidad de ocurrencia de un evento o resultado particular.

Factibilidad definida	Valor asignado
Hay pocos elementos que permitan determinar una posibilidad real	Poco probable
Hay elementos que permiten determinar una posibilidad media	Medianamente probable
Hay muchos elementos que permiten determinar una posibilidad alta	Bastante probable

Frecuencia definida	Valor asignado
Ha ocurrido entre una y tres veces en un periodo de un mes	Poco probable
Ha ocurrido entre cuatro y seis veces en un periodo de un mes	Medianamente probable
Ha ocurrido más de seis veces en un periodo de un mes	Bastante probable

III. ESCALA PARA IMPACTO

El impacto determina la diferencia entre las estimaciones del estado de seguridad del activo antes y después de materializar las amenazas, es decir, las consecuencias de la materialización de una amenaza. El impacto se puede evaluar en términos financieros, daño reputacional, interrupción operativa, entre otros.

Estos impactos se pueden dividir en tres grandes apartados:

- **Confidencialidad.** Ocurre cuando los datos personales son divulgados a otras partes no autorizadas.
- **Integridad.** Se produce cuando los datos personales dejan de ser completos y exactos, es decir, se modifican de forma no autorizada.
- **Disponibilidad.** Implica que los datos personales que deberían estar disponible en un momento dado no lo están y esto causa interrupciones en la actividad, ya sea interna o por parte de un tercero.

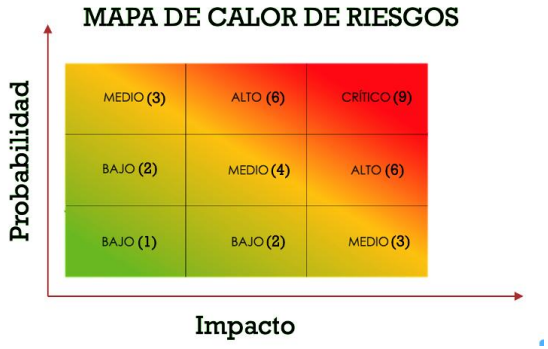
Impacto
Bajo
Medio
Alto

IV. ESCALA PARA DETERMINAR EL VALOR DEL RIESGO

Los riesgos de seguridad de la información corresponden con la asignación del valor de la probabilidad que tienen ciertas amenazas de explotar las vulnerabilidades que presentan los activos y causar un impacto.

NIVEL DE RIESGO	ACCIÓN REQUERIDA
ALTO	Inaceptable: acciones deben tomarse inmediatamente
MEDIO	Razonablemente aceptable: acciones requeridas y que deben tomarse en plazo razonable
BAJO	Aceptable: no se requieren acciones de inmediato

El cruce de valores de probabilidad e impacto permite identificar el valor del riesgo en un mapa de calor a partir de la siguiente escala de ejemplo.



Impacto		Probabilidad		Nivel de riesgo	
Cuantitativo	Cualitativo	Cuantitativo	Cualitativo	Cuantitativo	Cualitativo
1	Bajo	1	Bajo	1	Bajo
1	Bajo	2	Medio	2	Bajo
2	Medio	1	Bajo	2	Bajo
1	Bajo	3	Alto	3	Medio
3	Alto	1	Bajo	3	Medio
2	Medio	2	Medio	4	Medio
2	Medio	3	Alto	6	Alto
3	Alto	2	Medio	6	Alto
3	Alto	3	Alto	9	Critico

Identificación del riesgo

En esta fase se busca encontrar, reconocer y describir los riesgos a los que se enfrentan los activos, buscando contestar a las preguntas ¿qué puede suceder? y ¿cómo puede suceder?

IDENTIFICACIÓN DEL RIESGO			
NOMBRE DEL ACTIVO	TIPO DE ACTIVO	VULNERABILIDAD	AMENAZA
Escriba el nombre del activo	Seleccione el tipo de activo con la flecha de selección	Describa la vulnerabilidad	Describa la amenaza

Análisis del riesgo

Con el paso previo, se retoman los riesgos identificados, sus amenazas y vulnerabilidades, se determina la probabilidad de ocurrencia, las consecuencias de su materialización y finalmente a calcular el nivel de riesgo a partir de la integración de escenarios.

Evaluación del riesgo

Para retomar el nivel de riesgo obtenido y comparar contra los criterios definidos de aceptación a fin de establecer prioridades para atender.

ANÁLISIS DE RIESGO					EVALUACIÓN DE RIESGO
PROBABILIDAD	Confidencialidad	Integridad	Disponibilidad	IMPACTO	RIESGO INHERENTE
Seleccione el valor de probabilidad con la flecha de selección	Seleccione el valor de Confidencialidad con la flecha de selección	Seleccione el valor de Integridad con la flecha de selección	Seleccione el valor de Disponibilidad con la flecha de selección	Valor	Valor

Tratamiento del riesgo

En esta etapa se identifica la distancia que existe entre las medidas recomendadas y las medidas implementadas para cada uno de los tratamientos de datos personales que se declaran, esta actividad se puede dividir en las siguientes etapas:

- **Etapa 1 – Identificación de las medidas de seguridad.** En esta etapa se debe identificar si se cuenta o no con controles de seguridad de los riesgos identificados, se recomienda contar con un documento comparativo que ayude a identificar diversos controles de seguridad que permita atender de mejor manera los riesgos (por ejemplo, la metodología utilizada).

- **Etapa 2 – Valoración de las medidas de seguridad.** En este paso se valora si el control identificado mitiga el riesgo de alguna manera, es decir, se procede a hacer una nueva valoración del riesgo en las condiciones definidas en el análisis de riesgos, pero ahora con nuevos elementos que permiten determinar la disminución del riesgo en probabilidad o impacto.

- **Etapa 3 – Asignación del nivel de madurez.** En esta etapa se detalla el nivel de madurez de un control, es decir, se cuenta con un indicador que mide el grado en que el control está implementado y se ha integrado, para este paso se puede utilizar una escala a partir de la documentación obtenida por la implementación de los controles.

Escalas de nivel de madurez

Niveles			Descripción
0%	L0	Inexistente	No se cuentan con medidas de seguridad.
20%	L1	Inicial/ad hoc	Se realiza cuando se detecta un problema, no existe previsión, es una medida reactiva.
40%	L2	Repetible pero intuitivo	Una persona, la realiza de forma preventiva y constante de acuerdo con su criterio, no está documentada.
60%	L3	Proceso definido	Está documentada, hay una persona asignada para implementarla.
80%	L4	Gestionado y medible	Está documentada y funcionando, y además es medible y hay quien vigile su cumplimiento.
100%	L5	Optimizado	Además de ser medible, está automatizada.

ANALISIS DE BRECHA										
¿Tiene medidas de seguridad?	CATEGORÍA	OBJETIVO DE CONTROL	DESCRIPCIÓN DE LA O LAS MEDIDAS DE SEGURIDAD	NIVEL DE MADUREZ	NUEVA PROBABILIDAD	Nueva Confidencialidad	Nueva Integridad	Nueva Disponibilidad	NUEVO IMPACTO	RIESGO RESIDUAL
Responda la pregunta	Valor	Valor	Describa la medida de seguridad	Valor	Seleccione el valor de probabilidad con la flecha de selección	Seleccione el valor de Confidencialidad con la flecha de selección	Seleccione el valor de Integridad con la flecha de selección	Seleccione el valor de Disponibilidad con la flecha de selección	Valor	Valor

Tercera actividad – Definición de ruta de trabajo a partir de los resultados obtenidos para gestionar el riesgo

El plan de Trabajo es la hoja de ruta para la implementación de las medidas de seguridad que se detectaron en el análisis de brecha; esto es: las mejoras a las existentes, así como la implementación de las faltantes.

El plan de trabajo debe **reflejar los recursos disponibles, humanos, económicos, de conocimiento y de tiempo** con los que se cuenta.

PLAN DE TRABAJO						
ACTIVIDAD A REALIZAR	TIEMPO ESTIMADO PARA SU EJECUCIÓN	FECHA DE INICIO	ENCARGADO DE EJECUCIÓN	VALIDADOR DE IMPLEMENTACION	PRESUPUESTO ESTIMADO	COMENTARIOS ADICIONALES
Escriba la actividad a realizar	Indique el tiempo estimado para la ejecución de la medida de seguridad	Indique la fecha de inicio	Nombre al encargado de la ejecución de la Medida de seguridad	Nombre al validador de la ejecución de la Medida de seguridad	Indique el presupuesto estimado para la ejecución	Describa si tiene un comentario adicional