S

TOOLKIT DE CONCIENTIZACIÓN DE SEGURIDAD DE DATOS PERSONALES PARA RESPONSABLES DEL SECTOR PRIVADO

MANUAL DE IMPLEMENTACIÓN

Índice

Toolkit de concientización de seguridad de datos personales para responsables del sector privado

MANUAL DE IMPLEMENTACIÓN

Introducción

I. *Antecedentes del proyecto*

Con el objetivo de ayudar a los responsables y encargados del tratamiento de datos personales del sector privado a cumplir con el **deber de seguridad** establecido en la **Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)**, concretamente el referido a la obligación de establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado, el INAI ha convenido elaborar y poner a disposición del público objetivo el **"Toolkit de concientización de seguridad de datos personales para responsables del Sector Privado"** que consiste en una serie de herramientas (recursos gráficos y documentos de referencia) con información práctica especializada que se presentará con un lenguaje claro y sencillo.

II. *OBJETIVOS Y ALCANCES*

La implementación del Toolkit por parte de los responsables y encargados del sector privado permitirá, por una parte, concientizar a su personal sobre la importancia de la protección de datos personales y, por el otro, fomentar una cultura de respeto a la privacidad de las personas usuarias de sus servicios, brindando información relacionada con la legislación mexicana en la materia, con las obligaciones que deben observar y con diferentes elementos para entender y garantizar la seguridad de los datos personales.

Estructura

La carpeta comprimida (.zip) denominada **"Toolkit de concientización de seguridad de datos personales para responsables del Sector Privado"** que podrán descargar las y los interesados incluye materiales de difusión (carteles) y documentos de contenido (presentaciones, buenas prácticas y notas explicativas) sobre las acciones prácticas que se relacionan con el deber de seguridad.

El **"Toolkit de concientización de seguridad de datos personales para responsables del Sector Privado"** consta de cuatro módulos:

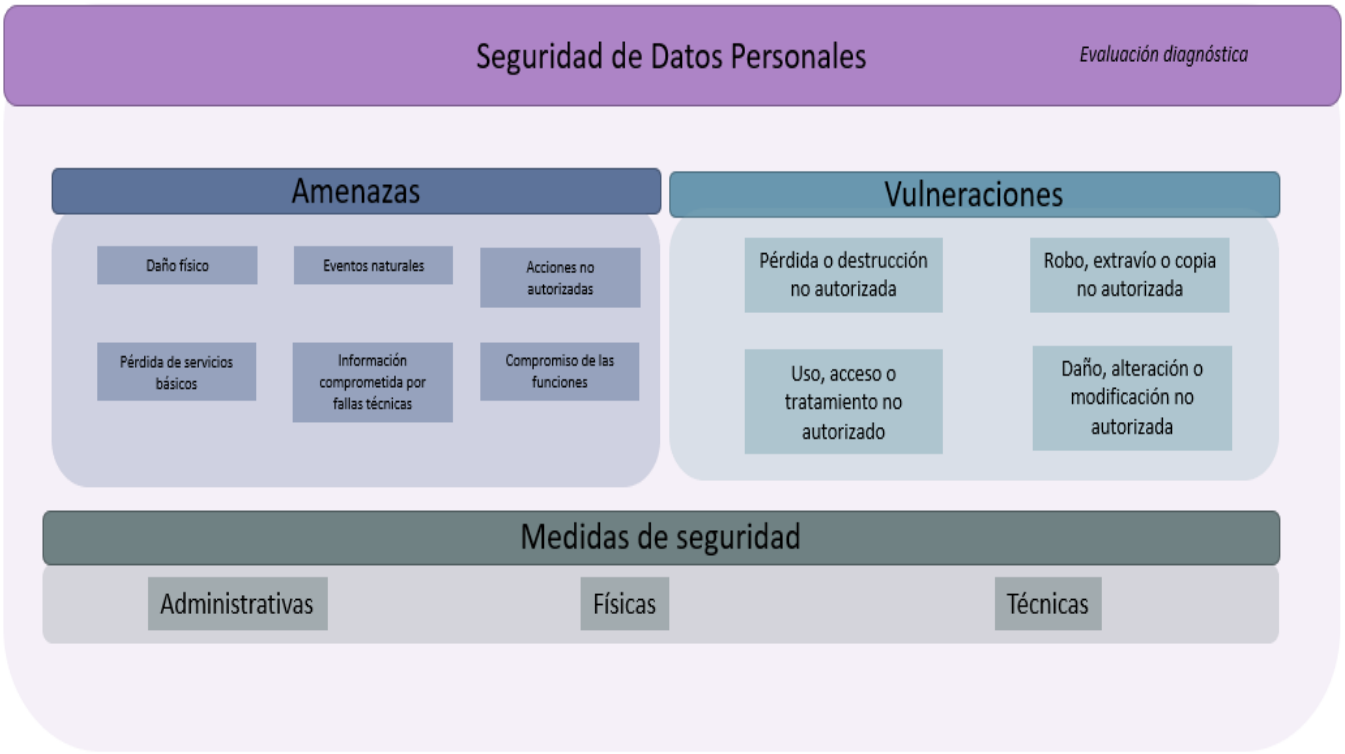
a) ***Seguridad de datos personales:*** en donde los usuarios contarán con información y diferentes recursos que les permita conocer y difundir al interior de su organización, qué es la seguridad de los datos personales, cómo se relaciona con la seguridad de la información y la ciberseguridad y las obligaciones que los responsables del tratamiento de datos personales deben considerar para cumplir con el deber de seguridad establecido en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

b) ***Amenazas:*** *a* través de esta sección la organización podrá conocer las principales amenazas que afectan la seguridad de los datos personales, de tal forma que podrá identificar aquellas para las cuales deberá implementar medidas de seguridad adicionales con la finalidad de evitar su materialización.

c) ***Vulneraciones:*** a través de este módulo las organizaciones conocerán el tipo de vulneraciones a la seguridad de los datos personales que establece la LFPDPPP y su Reglamento, así como los elementos que deberán implementar para la gestión adecuada las vulneraciones, considerando las obligaciones que establece el marco legal en la materia.

d) ***Medidas de seguridad:*** en este módulo las organizaciones conocerán las definiciones y ejemplos específicos de las medidas de seguridad administrativas, físicas y técnicas.

A continuación, se presenta un esquema del contenido general de los cuatro módulos que integran el Toolkit.



Cada uno de los módulos se integra de los siguientes elementos:

- **Evaluación diagnóstica inicial** para definir los conocimientos previos del personal sobre la protección de datos y la seguridad de la información y, en cierto modo, conocer sus necesidades para enfatizar en ciertos contenidos y objetivos.
- **Documento explicativo** que incluye la información detallada sobre el tema y que sirve de apoyo para que la persona designada por el responsable pueda impartir la capacitación utilizando la presentación que incluye el Toolkit o cualquier otro material que considere útil para los fines de la actividad. El documento también contiene ejemplos prácticos que ayudarán a asimilar la información.

- Resumen del tema presentado a través de **carteles,** los cuales se podrán difundir al interior de la organización como parte de la estrategia de comunicación interna.
- **Artículos de interés** para complementar el aprendizaje.
- **Examen de evaluación** (preguntas y respuesta) de cada uno de los módulos del Toolkit para verificar el nivel de conocimiento adquirido y asimilado.
- **Evaluación diagnóstica final** para evaluar el conocimiento general del personal una vez que cursaron los cuatro módulos del Toolkit y, de esta manera, corroborar el logro de los objetivos. Esto permitirá determinar si la información proporcionada fue suficiente o si es necesario recurrir a otras estrategias de enseñanza – aprendizaje.
-

Adicionalmente, se incluye una **presentación** que puede servir de apoyo durante la presentación de cada uno de los temas. Cada presentación incluye los conceptos principales y palabras clave que sirven de ayuda memoria tanto para el expositor como para el personal que está siendo capacitado.

Propuesta de implementación

El **"Toolkit de concientización de seguridad de datos personales para responsables del Sector Privado"** está diseñado para seguir un orden lógico en función de los temas que deben conocer los responsables y encargados del tratamiento de datos personales para evitar, al interior de sus empresas e instituciones, vulneraciones de datos o cualquier otra amenaza a la seguridad de la información y de los datos personales y, de este modo, cumplir con los deberes y obligaciones contemplados en la legislación en materia de protección de datos que les resulta aplicable.

Si bien cada responsable y encargado es libre de utilizar el material de la manera que convenga a sus intereses, **el INAI propone el siguiente diagrama de flujo**:

En cuanto a la programación de las actividades, se propone el siguiente cronograma. Es importante señalar que los tiempos asignados para cada actividad pueden variar en función de las labores propias de la organización y del número de personal capacitado.

Actividad	año											
	mes				mes				mes			
	1	2	3	4	1	2	3	4	1	2	3	4
Responder la evaluación diagnóstica inicial												
Distribución de carteles e infografías en toda la organización												
Módulo 1												
Módulo 2												
Módulo 3												
Módulo 4												
Responder la evaluación diagnóstica final												

Evaluación diagnóstica

A continuación, se incluye una evaluación diagnóstica que se sugiere aplicar antes de implementar el Toolkit, con la finalidad de identificar los conocimientos previos del personal sobre la seguridad de datos personales, de tal forma que puedan identificar y atender sus necesidades.

Adicionalmente, se recomienda aplicar esta misma evaluación al final de la implementación del Toolkit, con el objetivo de corroborar el logro de los objetivos y determinar si la organización mejoro su nivel de concientización sobre la seguridad de los datos personales.

1. **¿Qué normativa regula la protección de datos personales en el sector privado?**

   a) Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
   b) Ley Federal de Telecomunicaciones
   c) Ley Federal de Protección de Datos Personales en Posesión de los Particulares
   d) Recomendaciones para los sujetos obligados en la designación del oficial de protección de datos personales
   e) Ninguna de las anteriores

2. **¿Cuáles son las vulneraciones de datos?**

   a) La pérdida o destrucción no autorizada
   b) El robo, extravío o copia no autorizada
   c) El uso, acceso o tratamiento no autorizado
   d) El daño, la alteración o modificación no autorizada
   e) Todas las anteriores

3. **¿La seguridad de la información tiene como finalidad esencial resguardar y proteger la información, preservando en todo momento los principios de confidencialidad, disponibilidad, integridad, autenticación, control de acceso, no repudio?**

   a) Verdadero

b) Falso

4. **¿Cuál es el objetivo principal de las medidas de seguridad que debe establecer y mantener todo responsable que lleve a cabo tratamiento de datos personales?**

a) Proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado
b) Garantizar el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (Derechos ARCO)
c) Ayudar a los empleados con la realización de sus actividades
d) Fomentar la confianza de los clientes

5. **¿Cuál es la clasificación de las medidas de seguridad para proteger los datos personales?**

a) Administrativas y técnicas
b) Digitales y físicas
c) Económicas y sociales
d) Administrativas, físicas y técnicas
e) Públicas y privadas

6. **¿Cuáles son los pasos para realizar un análisis de brecha?**

a) Identificar las medidas de seguridad que se implementan en la organización
b) Evaluar la eficacia de dichas medidas
c) Mejorar las medidas vigentes e identificar nuevas medidas a partir de mejores prácticas, estándares, guías y recomendaciones
d) Elaborar un plan de acción para la eventual implementación de las medidas identificadas que incluya tiempos, responsables, procedimientos y demás contenido necesario
e) Todas las anteriores

7. **La siguiente frase es verdadera o falsa: "Las organizaciones deben establecer un sistema de supervisión y vigilancia interna y/o externa para comprobar el cumplimiento de las políticas de**

privacidad (revisiones), así como su eficacia y eficiencia (auditoría objetiva e imparcial)"

a) Verdadera
b) Falsa

8. Un Sistema de Gestión de Seguridad de Datos Personales es:

a) Un programa informático para proteger los dispositivos de cualquier sistema malicioso o *malware*
b) Un sistema de seguridad físico para proteger los dispositivos en los que se almacenan la información, incluyendo los datos personales
c) Un sistema para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales
d) Un sistema de alerta para las vulneraciones de datos personales
e) Ninguna de las anteriores

9. Los esquemas de autorregulación se definen como:

a) La posibilidad que tienen los responsables y encargados de establecer y autoimponerse voluntariamente reglas para el debido tratamiento de datos personales que complementen lo previsto por la normativa, elevando los estándares de protección de ésta y considerando las particularidades de los responsables o encargados que desarrollan y adoptan esta clase de reglas
b) La posibilidad que tienen las personas titulares de los datos de establecer y autoimponerse voluntariamente reglas para el debido tratamiento de sus datos personales
c) La posibilidad que tienen las autoridades y el sector público de establecer reglas vinculantes para el debido tratamiento de datos personales que complementen lo previsto por la normativa, elevando los estándares de protección
d) La posibilidad que tienen los órganos garantes de la protección de datos personales de establecer reglas voluntarias para el debido tratamiento de datos personales que complementen lo previsto por la normativa, elevando los estándares de protección
e) Ninguna de las anteriores

10. ¿Cuál es la vigencia de la certificación de los esquemas de autorregulación?

a) Un año
b) Dos años
c) Cinco años
d) Diez años
e) No tienen vigencia

11. Es cualquier valor para la organización que requiera ser protegido. En el caso de la seguridad de los datos personales, deberán ser aquéllos que estén relacionados con el ciclo de vida de los datos personales previamente identificado y sus distintos tratamientos. Los activos se deben identificar y ponderar con suficiente nivel de detalle para proveer información que permita hacer la valoración del riesgo.

a) Activos
b) Hardware
c) Software
d) Hacker
e) Ninguna de las anteriores

12. ¿Qué es un incidente de seguridad?

a) Cualquier violación a las medidas de seguridad físicas, técnicas o administrativas de un responsable, que afecte la confidencialidad, la integridad o la disponibilidad de la información
b) Cualquier evento o circunstancia que han provocado o podrían haber provocado un daño innecesario a un titular de los datos
c) Cualquier evento o circunstancia que afecte la seguridad pública
d) Cualquier problema suscitado en el ámbito laboral que pone en riesgo a los trabajadores
e) Ninguna de las anteriores

13. ¿Cuál es el orden correcto del ciclo de vida de los datos personales?

a) Obtención, uso, almacenamiento, divulgación, cancelación y bloqueo
b) Obtención, almacenamiento, uso, divulgación, bloqueo y cancelación
c) Obtención, uso, divulgación, almacenamiento, bloqueo y cancelación
d) Obtención, almacenamiento, bloqueo, uso, divulgación y cancelación
e) Obtención, bloqueo, cancelación, uso, divulgación y almacenamiento

14. Es una técnica utilizada para obtener información de las personas teniendo como base la interacción social, la manipulación y el engaño, y ocurre típicamente en conversaciones directas entre el delincuente y la víctima

a) Fraude comunicacional
b) Cibercrimen
c) Pirateo
d) Ingeniería social
e) Ninguna de las anteriores

15. A una persona cuya misión es perfeccionar software inédito y que además es contratada para probar el software en busca de errores antes de su lanzamiento se le conoce como:

a) Hacker de sombrero blanco
b) Hacker de sombrero gris
c) Hacker de sombrero negro
d) Hacker de sombrero azul
e) Hacker de sombrero amarillo

16. Las amenazas que tiene el potencial de dañar un activo y causar una vulneración a la seguridad se clasifican por:

a) Tipo de usuario al que afectan
b) Duración del daño
c) Origen y tipo
d) Todas las anteriores
e) Ninguna de las anteriores

17. Son ejemplos de amenazas de origen natural

a) Fenómenos climáticos o meteorológicos
b) Fenómenos sísmicos
c) Fenómenos volcánicos
d) Todas las anteriores
e) Ninguna de las anteriores

18. En materia de seguridad de la información, ¿cuál es la principal consecuencia de las amenazas, sobre todo las de origen humano?

a) Extorsión y chantaje
b) Vulneraciones a la seguridad de los datos personales
c) Abuso en la operación de los sistemas
d) Explotación económica
e) Errores en los sistemas

19. Son posibles consecuencias de una amenaza provocada por un hacker o un cracker:

a) Ingeniería social
b) Intrusión en los sistemas
c) Robo de información
d) Todas las anteriores
e) Ninguna de las anteriores

20. Un incidente de seguridad que involucra datos personales se denomina:

a) Usurpación de identidad

b) Vulneración de seguridad
c) Revelación de información no autorizada
d) Revelación ilegal de información
e) Ninguna de las anteriores

21. Las vulneraciones a la seguridad de personales son un tipo particular de _____ que pueden ocurrir en cualquier fase del tratamiento de datos personales

f) Incidente de seguridad
g) Alerta de seguridad
h) Brecha de seguridad
i) Violación de seguridad
j) Ninguna de las anteriores

22. ¿Qué es una vulneración a la seguridad de los datos personales?

f) Cualquier violación a las medidas de seguridad físicas, técnicas o administrativas de un responsable, que afecte la confidencialidad, la integridad o la disponibilidad de la información.
g) Pérdida o destrucción no autorizada de los datos, robo, extravío o copia no autorizada, uso, acceso o tratamiento no autorizado, daño, la alteración o su modificación no autorizada.
h) Cualquier problema suscitado en el ámbito laboral que pone en riesgo a los trabajadores y sus datos personales.
i) Ninguna de las anteriores

23. Fases de una vulneración a la seguridad de los datos personales

f) Investigación, ataque, extracción de datos
g) Investigación, análisis, exfriltración de datos
h) Investigación, ataque, cifrado de datos
i) Investigación, ataque, exfriltración de datos

24. Actores relevantes que participan en la gestión de una vulneración a la seguridad de datos personales

f) Responsable del tratamiento, oficial de PDP, personal o departamento de datos personales y encargado.
g) Responsable del tratamiento, autoridad de protección de datos personales, personas titulares y encargados.
h) Responsable, encargado y tercero.
i) Responsable y tercero.

25. **Los _____están relacionados de forma enunciativa más no limitativa, con sus bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados o las cantidades o porcentajes relacionados con la situación económica del titular.**

f) Derechos financieros
g) Derechos patrimoniales
h) Derechos morales
i) Derechos materiales

26. Los _____ se refieren de manera enunciativa más no limitativa, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físicos, consideración que de sí mismo tienen los demás, o cuando se menoscabe ilegítimamente la libertad o la integridad física o psíquica de éste.

f) Derechos humanos
g) Derechos patrimoniales
h) Derechos personales
i) Derechos morales

27. Los _____ del tratamiento de datos personales deberán evaluar el riesgo de una vulneración de seguridad de datos personales.

f) terceros

g) encargados
h) responsables
i) titulares

28. Los _____ tienen la obligación según lo establecido en el artículo 39 de la LGPDPPSO de llevar una bitácora de las vulneraciones a la seguridad en la que se describan, la fecha en la que ocurrió, el monto de éstas y las acciones correctivas implementadas de forma inmediata y definitiva.

f) terceros
g) titulares
h) encargados
i) sujetos obligados

29. Etapas de un plan de respuesta a incidentes de seguridad de datos personales.

f) Preparación, identificación, contención, mitigación, recuperación y mejora continua.
g) Preparación, identificación, eliminación, mitigación, recuperación y mejora continua.
h) Actuación, identificación, eliminación, mitigación, recuperación y mejora continua.
i) Análisis, identificación, eliminación, mitigación, recuperación y mejora continua.

30. **El ____es la apropiación de la identidad de una persona, para hacerse pasar por ella, asumir su identidad frente a terceros públicos o privados, a fin de obtener ciertos recursos o beneficios a su nombre. El robo de identidad implica la obtención y uso no autorizado e ilegal de datos personales.**

f) fraude
g) robo de identidad
h) phishing

i) spamming

31. ¿Para qué son destinadas las medidas de seguridad físicas según lo establecido en el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares?

a) Para prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información.
b) Para proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones.
c) Para proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad.
d) Para garantizar la eliminación de datos de forma segura
e) Todas las anteriores

32. ¿Qué es el cómputo en la nube de acuerdo con el Instituto Nacional de Estándares y Tecnología de Estados Unidos?

a) Una metáfora empleada para hacer referencia a servicios que se utilizan a través de Internet.
b) Un modelo que permite el acceso ubicuo, conveniente y bajo demanda de red a un conjunto de recursos informáticos configurables que puedan ser rápidamente proveídos con esfuerzos mínimos de administración o interacción con el proveedor de servicio.
c) Un enfoque popular de servicios de computación como copias de seguridad.
d) Un sistema informático basado en Internet y centros de datos remotos para gestionar servicios de información y aplicaciones.
e) Un conjunto de servicios ofrecidos a través de Internet.

33. ¿Cuáles son los modelos principales de aprovisionamiento de servicios de cómputo en la nube?

a) Acceso amplio, reservas de uso común y servicio medido de la red
b) Nube pública, privada, híbrida y comunitaria
c) Infraestructura, plataforma y software como servicio
d) Autoservicio de demanda y reservas de uso común
e) Ninguna de las anteriores

34. De acuerdo con esta característica esencial de cómputo, los sistemas de nube controlan y optimizan el uso de los recursos de manera automática utilizando una capacidad de medición en un cierto nivel de abstracción adecuado para el tipo de servicio.

a) Rápida elasticidad
b) Acceso amplio desde la red
c) Reservas de recursos en común
d) Servicio medido
e) Autoservicio por demanda

35. Gracias a ello, la información está disponible con acceso instantáneo donde quiera que se esté y siempre que se necesite a través de la Web.

a) Protección de datos en la nube
b) Seguridad en la nube
c) Privacidad de datos en la nube
d) Almacenamiento de la nube
e) Todas las anteriores

36. Es el estándar internacional de privacidad en la nube que proporciona orientación destinada a garantizar que los proveedores de servicios en la nube puedan ofrecer controles adecuados de seguridad de información con el objetivo de proteger la privacidad de los clientes

a) ISO 27001
b) ISO 27000

c) ISO 27017
d) ISO 27701
e) ISO 27018

37. Establece objetivos de control y lineamientos comúnmente aceptados para implementar medidas de protección para los datos personales para ambientes públicos de cómputo en la nube.

a) Norma mexicana NMX-I-27018-NYCE-2016
b) Cloud data protection
c) Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los particulares
d) Lineamientos generales de protección de datos personales en posesión de sujetos obligados
e) Ninguna de las anteriores

38. Es un ejemplo de medida de seguridad específica para la protección de datos durante el uso de la computación en la nube.

a) Establecer Contraseñas y cifrar datos
b) Limitar y clasificar la información
c) Revisar las configuraciones por defecto
d) Poseer un adecuado sistema de seguridad
e) Todas las anteriores

39. El INAI publicó este documento con el objetivo de identificar las condiciones de prestación de servicio de infraestructura, plataforma y software de cómputo en la nube que ofrecen algunos proveedores y, de esta manera, ayudar a los responsables a elegir y decidir aquellos que más se ajusten a sus necesidades de prestación del servicio de cómputo en la nube.

a) Conformidad de contratos de adhesión de servicios de cómputo en la nube vs los criterios mínimos para la contratación de

servicios de cómputo en la nube que impliquen el tratamiento de datos personales

b) Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales
c) Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales
d) Guía para instrumentar medidas compensatorias en el sector público
e) Ninguna de las anteriores

40. ¿Cómo se denomina a las personas que violan la seguridad y privacidad de los datos personales en la nube?

a) Cibernéticos
b) Informáticos
c) Hackers y crackers
d) Violadores de nube
e) Programadores

Encuesta

Una vez que el "Toolkit de concientización de seguridad de datos personales para responsables del Sector Privado" se haya implementado en su organización y para mejora de este, le solicitamos su apoyo para dar respuesta a la siguiente encuesta y enviarla por correo electrónico a la dirección miriam.padilla@inai.org.mx

Le recordamos que sus respuestas son confidenciales y serán utilizadas únicamente para la mejora de este material.

1. ¿A qué sector pertenece su organización?

Sector		
Educación	☐	
Salud	☐	
Financiero	☐	
TI	☐	
Otro	☐	¿cuál?

2. ¿Número de empleados?

Número	
Menos de 100	☐
100- 150	☐
151-300	☐
301-450	☐
451-600	☐
Más de 600	☐

3. Valore la utilidad de los diferentes materiales que forman parte del Toolkit.

Material	Poco útil	Algo útil	Normal	Bastante útil	Muy útil
Manual de implementación	☐	☐	☐	☐	☐
Carteles	☐	☐	☐	☐	☐
Presentaciones	☐	☐	☐	☐	☐
Documentos explicativos	☐	☐	☐	☐	☐

4. ¿Qué otros temas le gustarían que se incluyeran en una versión actualizada del Toolkit?

5. Comentarios o sugerencias: