UNMSM
Fundación
SAN MARCOS
Por el desarrollo de la Ciencia y la Cultura

DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

RESUMEN EJECUTIVO

GUÍA ORIENTADORA PROTECCIÓN DE DATOS PERSONALES

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

RESUMEN EJECUTIVO

Protección de Datos Personales como herramienta para prevenir la violencia digital

Enfoque ejecutivo y técnico de ciberseguridad, privacidad y gestión del riesgo digital

Documento base	Guía Orientadora “Protección de Datos Personales como herramienta para prevenir la violencia digital”
Institución	Sistema Nacional de Transparencia / INAI – México
Edición	Julio de 2021
Alcance	Síntesis en español de los contenidos centrales de la guía, con lectura técnica desde la ciberseguridad.

Propósito del resumen. Presentar, de forma condensada y profesional, los fundamentos jurídicos y operativos de la protección de datos personales, su relación con la privacidad y la violencia digital, los derechos de las personas y las medidas de prevención aplicables al uso cotidiano de tecnologías de información y comunicación.

Nota metodológica: el documento fuente ya está redactado en español. Por ello, esta versión no realiza una traducción literal, sino una reformulación ejecutiva en español claro, manteniendo el sentido, la terminología y el marco mexicano de la guía.

1. Visión ejecutiva

La guía parte de una premisa central: la transformación digital amplía las oportunidades de comunicación, acceso a servicios e intercambio de información, pero también incrementa la exposición de datos personales y facilita nuevas formas de agresión. La identidad digital se construye con información que identifica o hace identificable a una persona; cuando esa información se publica, comparte o trata sin controles suficientes, puede convertirse en un vector de daño.

Desde una perspectiva de ciberseguridad, la protección de datos no debe entenderse únicamente como cumplimiento normativo. Funciona también como una capa de reducción de riesgo frente a suplantación de identidad, fraude, acoso, vigilancia, exposición de información íntima, extorsión, discriminación y otras conductas que se apoyan en la disponibilidad y permanencia de la información en Internet.

La guía enfatiza que la violencia digital puede producir efectos psicológicos, emocionales, patrimoniales, reputacionales y físicos. El riesgo es especialmente relevante cuando se tratan datos sensibles, imágenes íntimas, información de menores de edad o datos que permiten localizar, perfilar o identificar a una persona.

2. Conceptos fundamentales

Concepto	Síntesis	Implicación de seguridad
Dato personal	Información vinculada con una persona física identificada o identificable: nombre, imagen, edad, domicilio, teléfono, correo, identificadores, trayectoria académica o laboral, patrimonio, entre otros.	Su exposición permite identificar, perfilar, contactar o correlacionar información de una persona.
Dato sensible	Información de la esfera más íntima cuyo uso indebido puede generar discriminación o riesgo grave: salud, origen étnico o racial, creencias, opiniones, preferencias sexuales,	Requiere un nivel reforzado de cuidado por la severidad potencial del impacto.

	datos biométricos, entre otros.	
Privacidad	Ámbito de la vida personal y familiar que una persona puede preservar frente a injerencias injustificadas.	La configuración de servicios y los hábitos de uso pueden ampliar o reducir ese ámbito.
Protección de datos	Derecho fundamental que permite controlar el tratamiento de la información personal y exigir reglas para su obtención, uso, conservación, transferencia y eliminación.	Traslada el control del dato hacia principios, derechos y obligaciones verificables.

3. Principios para el tratamiento responsable de datos

El marco expuesto por la guía exige que el tratamiento de datos personales se someta a principios que limitan la discrecionalidad del responsable y permiten evaluar si el uso de la información es legítimo. En términos de gobernanza de seguridad, estos principios constituyen controles de diseño y de operación:

Principio	Aplicación práctica
Licitud	Los datos deben obtenerse y tratarse conforme a la ley, sin métodos engañosos o fraudulentos.
Finalidad	El tratamiento debe responder a propósitos concretos, lícitos, explícitos y legítimos.
Lealtad	El responsable debe privilegiar los intereses y expectativas razonables de privacidad del titular.
Consentimiento	Como regla, el tratamiento está sujeto a la voluntad del titular; los datos sensibles demandan consentimiento reforzado, salvo excepciones legales.
Calidad	Los datos deben ser pertinentes, correctos y actualizados para la finalidad que justificó su obtención.
Proporcionalidad	Solo deben tratarse los datos necesarios, adecuados y relevantes para la finalidad prevista.
Información	El titular debe conocer, mediante el aviso de privacidad, qué información se recaba, para qué se utiliza y las características esenciales del tratamiento.
Responsabilidad	El responsable debe adoptar medidas suficientes para demostrar y garantizar el cumplimiento, incluso frente a terceros relacionados.

4. Privacidad, TIC y superficie de exposición

Las tecnologías digitales no son neutrales respecto de la privacidad: su diseño puede facilitar la recolección, almacenamiento y análisis de conductas, mientras que las decisiones del usuario determinan cuánto expone de sí mismo. Redes sociales, aplicaciones, navegadores y servicios digitales pueden registrar actividades, preferencias y relaciones. La guía advierte que esta transparencia

puede ser consciente o inadvertida y está condicionada por factores culturales, educativos y sociales.

Una vez difundida, la información puede ser copiada, indexada, redistribuida y permanecer disponible durante largos periodos. Esta persistencia incrementa el impacto de una publicación impulsiva y dificulta la eliminación completa del contenido.

5. Marco institucional y diferencias entre sector público y privado

La guía describe un esquema mexicano de doble regulación: una ley general para datos en posesión de sujetos obligados del sector público y una ley federal para datos en posesión de particulares. Aunque ambos regímenes persiguen la protección de la persona, presentan diferencias procedimentales e institucionales.

- En el sector público se contempla expresamente la portabilidad, evaluaciones de impacto, un Programa Nacional de Protección de Datos y la posibilidad de designar un oficial de protección de datos en tratamientos relevantes o intensivos.
- Los procedimientos de verificación, auditoría, medios de impugnación, medidas de apremio y régimen sancionador presentan reglas distintas según el sector.
- La guía destaca que el sector privado cuenta con disposiciones específicas sobre delitos por tratamiento indebido de datos, mientras que el régimen público articula otras vías de responsabilidad y control.

Para un responsable de seguridad de la información, esta distinción implica que la respuesta ante un incidente no puede limitarse a controles técnicos: debe considerar quién trata los datos, la base jurídica aplicable, los mecanismos de reclamación y la autoridad competente.

6. Violencia digital: alcance y manifestaciones

La violencia digital se presenta como una conducta dolosa realizada mediante TIC que expone, distribuye, difunde, exhibe, transmite, comercializa, ofrece, intercambia o comparte imágenes, audios o videos -reales o simulados- de contenido íntimo o sexual sin consentimiento, cuando con ello se causa daño psicológico, emocional, a la privacidad, dignidad o imagen. La guía también aborda una noción más amplia de violencia en línea, que comprende conductas que dañan reputación, integridad o participación pública.

No toda violencia digital es idéntica a un delito cibernético. Algunas conductas son formas de hostigamiento o violencia; otras pueden constituir ilícitos penales. La clasificación depende de la conducta y del marco jurídico aplicable.

7. Principales riesgos y conductas en el entorno digital

- Críticas o ataques por apariencia o condición social.
- Suplantación o robo de identidad.
- Monitoreo, acecho y vigilancia no consentida.
- Contacto mediante identidades falsas.
- Mensajes y llamadas ofensivas.
- Publicación de información personal, fotografías o contenido íntimo sin consentimiento.
- Provocaciones dirigidas a generar una reacción negativa.
- Insinuaciones o propuestas sexuales y recepción no solicitada de contenido sexual.
- Discriminación, amenazas, agresiones, extorsión, desprestigio o difamación.
- Acceso o control no autorizado de dispositivos de terceros.

8. Por qué la protección de datos reduce la violencia digital

La violencia digital suele aprovechar tres condiciones: facilidad de acceso a la información, rapidez de difusión y dificultad para eliminar definitivamente lo publicado. Reducir la cantidad de información expuesta, conocer el propósito del tratamiento, restringir accesos y ejercer derechos sobre los datos disminuye las oportunidades de abuso.

La guía conecta la prevención con la educación digital: una persona que comprende qué datos entrega, quién puede tratarlos, cuánto tiempo permanecerán disponibles y qué mecanismos tiene para retirar u oponerse a su uso se encuentra en mejores condiciones para prevenir daños o reaccionar tempranamente.

Desde la óptica de ciberseguridad, este enfoque se alinea con la minimización de datos, el control de acceso, la gestión de identidades, la reducción de superficie de exposición y la respuesta temprana ante incidentes. Esta lectura técnica es coherente con la guía, aunque estos términos operativos se emplean aquí para sintetizar sus implicaciones.

9. Derechos ARCO y control sobre la información

Derecho	Qué permite	Utilidad ante un riesgo digital
Acceso	Conocer qué datos posee el responsable, su finalidad, origen, tratamiento y, según corresponda, obtener copia.	Permite dimensionar la exposición y conocer quién dispone de la información.
Rectificación	Corregir datos inexactos, incompletos o desactualizados.	Reduce riesgos derivados de información errónea o manipulada.
Cancelación	Solicitar la supresión o eliminación de datos cuando corresponda.	Ayuda a limitar la permanencia de información que ya no debe tratarse.
Oposición	Impedir o limitar determinados tratamientos cuando proceda.	Permite frenar usos no deseados que puedan afectar a la persona.

10. Actuación cuando existe violencia digital

La guía recomienda utilizar los mecanismos de protección de datos como parte de la respuesta. Las redes sociales y servicios digitales deben disponer de canales que permitan solicitar la cancelación o limitación del tratamiento y denunciar contenidos o perfiles abusivos. Cuando el responsable no atiende una solicitud o realiza un tratamiento indebido, pueden activarse procedimientos ante las autoridades garantes competentes.

- Conservar mensajes, publicaciones y demás elementos relevantes como evidencia.
- Reportar perfiles, páginas o contenidos que impliquen abuso o exposición indebida.
- Ejercer los derechos ARCO cuando resulten aplicables.
- Acudir al órgano garante competente si existe tratamiento indebido de datos o falta de atención a los derechos.
- Cuando la conducta pueda constituir delito, la investigación y persecución corresponde a las autoridades penales; la autoridad de protección de datos no sustituye esa vía.

11. Medidas preventivas priorizadas

La guía reúne recomendaciones de higiene digital que, vistas como controles de ciberseguridad, buscan reducir la probabilidad de exposición, acceso no autorizado y uso abusivo de información personal:

- Leer condiciones de uso y avisos de privacidad antes de utilizar servicios digitales.
- Usar contraseñas robustas, mantenerlas en reserva y evitar el almacenamiento o conexión automática cuando incremente el riesgo.
- Apagar o bloquear equipos cuando no se utilicen y evitar accesos no autorizados a cámara o dispositivo.
- Desactivar Bluetooth y geolocalización cuando no sean necesarios.
- Instalar y mantener actualizados antivirus y firewalls.
- Evitar redes públicas o abiertas para operaciones sensibles y no realizar transacciones desde conexiones inseguras.
- Verificar el uso de HTTPS antes de realizar transacciones.
- Cerrar sesiones y limpiar información temporal cuando corresponda.
- Configurar la privacidad de redes sociales y limitar la visibilidad a personas conocidas.
- No entregar correos, teléfonos u otros datos personales a desconocidos sin una razón legítima.
- Evitar compartir contenido íntimo o información cuya divulgación pueda generar daño.
- Aplicar controles parentales y acompañamiento en el caso de menores de edad.
- Revisar estados de cuenta y señales de actividad anómala.
- Denunciar abusos, conservar evidencia y ejercer los derechos ARCO.

12. Lectura de ciberseguridad: controles por capa

Capa	Riesgo principal	Control recomendado
Personas	Sobreexposición, engaño, contacto abusivo	Concientización, privacidad por defecto, criterio antes de publicar y canales de denuncia.
Identidad y acceso	Suplantación, acceso no autorizado	Contraseñas seguras, cierre de sesión y restricción de accesos.
Dispositivos	Captura o extracción de información	Actualización, antivirus/firewall, bloqueo de equipos, control de cámara, Bluetooth y geolocalización.
Red y servicios	Intercepción, exposición en redes abiertas	Conexiones seguras, HTTPS y cautela en redes públicas.
Datos	Difusión, persistencia y tratamiento indebido	Minimización, finalidad, consentimiento, configuración de privacidad y ejercicio de derechos.

13. Implicaciones para organizaciones

Aunque la guía tiene un enfoque orientador para la ciudadanía, sus contenidos permiten identificar obligaciones organizacionales relevantes. Una institución que trata datos personales debe informar de forma comprensible, limitar la recolección a lo necesario, definir finalidades, mantener la calidad de los datos, establecer medidas de seguridad y responder ante solicitudes de los titulares.

En contextos de atención a víctimas, la protección de datos adquiere una dimensión adicional: la propia institución puede provocar una segunda afectación si recopila información excesiva, expone expedientes, comparte datos sin necesidad o no preserva la confidencialidad. La guía subraya que las autoridades deben explicar qué información se recaba, con qué finalidad, quién es responsable del tratamiento y cómo pueden ejercerse los derechos correspondientes.

Para la gestión de ciberseguridad, esto exige integrar privacidad y seguridad desde el diseño de procesos: inventariar datos, asignar responsabilidades, restringir accesos, revisar terceros, conservar únicamente lo necesario y establecer mecanismos de respuesta ante incidentes y solicitudes de titulares.

14. Conclusiones ejecutivas

- La protección de datos personales es un derecho fundamental y, al mismo tiempo, un mecanismo práctico de prevención frente a riesgos digitales.
- El dato personal es un activo de alto impacto: su valor no depende solo de su sensibilidad aislada, sino de la posibilidad de combinarlo con otras fuentes para identificar, perfilar o afectar a una persona.
- La privacidad y la ciberseguridad son complementarias. La primera define el control legítimo sobre la información; la segunda aporta medidas para preservar ese control frente a amenazas y accesos no autorizados.
- La violencia digital se potencia por la velocidad, alcance, replicabilidad y persistencia de Internet. La prevención debe actuar antes de la publicación y continuar durante todo el ciclo de vida de la información.
- Los derechos ARCO proporcionan mecanismos concretos para recuperar control sobre datos tratados por terceros, aunque no sustituyen las acciones penales o de otra naturaleza cuando existe un delito.
- La educación digital, la configuración de privacidad, el uso de controles técnicos básicos y la capacidad de denunciar constituyen barreras complementarias frente al abuso.
- Las organizaciones deben evitar la revictimización mediante tratamientos innecesarios o inseguros de la información de quienes solicitan apoyo.

15. Matriz ejecutiva de riesgos y respuesta

Escenario	Impacto	Prevención	Respuesta
Sobreexposición en redes	Pérdida de privacidad, perfilamiento, acoso	Limitar audiencia, minimizar datos, revisar privacidad	Eliminar/restringir contenido, reportar, ejercer ARCO.
Suplantación de identidad	Fraude, daño reputacional, engaño a terceros	Proteger credenciales y reducir datos públicos	Conservar evidencia, reportar cuenta, solicitar cancelación/rectificación.
Difusión no consentida de contenido íntimo	Daño psicológico, reputacional y a la dignidad	Evitar exposición, controlar destinatarios y dispositivos	Denunciar contenido, preservar evidencia y acudir a vías de protección y penales cuando corresponda.
Acceso no autorizado a dispositivos	Robo de datos, vigilancia, captura de imágenes	Bloqueo, actualizaciones, antivirus/firewall, control de cámara	Cambiar credenciales, cerrar sesiones, revisar accesos y documentar incidente.
Tratamiento indebido por una organización	Uso incompatible, transferencia o conservación excesiva	Aviso de privacidad, finalidad, proporcionalidad y controles	Ejercer ARCO y acudir al órgano garante competente.

16. Consideraciones sobre el alcance del documento

La guía fue publicada en México en julio de 2021 y desarrolla su análisis con base en la Constitución y legislación mexicana vigente al momento de su elaboración, además de estadísticas y referencias disponibles hasta esa fecha. Por tanto, su valor principal para un diplomado o programa de ciberseguridad está en los principios, conceptos y prácticas de prevención; las referencias normativas específicas deben interpretarse dentro de ese contexto temporal y territorial.

Este resumen no incorpora normas posteriores ni sustituye una revisión jurídica actualizada. Tampoco amplía el documento con legislación de otros países, ya que el objetivo solicitado es sintetizar fielmente el archivo adjunto.

17. Síntesis para aplicación académica y profesional

La principal enseñanza de la guía es que la seguridad de la información personal comienza antes del incidente. El usuario debe conocer qué comparte y con quién; el responsable debe justificar por qué lo recolecta y protegerlo durante su tratamiento; y las autoridades deben ofrecer mecanismos efectivos para restituir el control cuando existe un uso indebido.

En un programa de formación en ciberseguridad, el documento resulta especialmente útil para conectar tres dimensiones que a menudo se estudian por separado: derechos fundamentales, gestión de datos y amenazas digitales. La violencia digital demuestra que una falla de privacidad puede convertirse en un incidente de seguridad y, posteriormente, en un daño humano concreto.

Por ello, una estrategia madura debe combinar gobernanza, controles técnicos y conducta responsable. Las contraseñas, actualizaciones, firewalls y conexiones seguras son necesarias, pero no suficientes: también se requiere minimización de datos, transparencia, consentimiento, derechos de los titulares, configuración de privacidad, evidencia y rutas claras de denuncia.

En términos ejecutivos, proteger datos personales significa reducir la información disponible para el agresor, limitar usos no autorizados, detectar exposiciones, responder con rapidez y preservar la dignidad de la persona. Esa es la contribución central de la guía a la prevención de la violencia digital.

Fuente base

Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (SNT) / Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Guía Orientadora “Protección de Datos Personales como herramienta para prevenir la violencia digital”. Primera edición, julio de 2021.

Documento elaborado como resumen ejecutivo. Se preserva el enfoque del texto fuente y se condensan sus contenidos para fines académicos y profesionales.