



CURSO SOBRE LA LEY DE PROTECCIÓN DE DATOS PERSONALES

MÓDULO VIII

BUENAS PRÁCTICAS Y TENDENCIAS

RECOPILACIÓN:

ÁREA ACADÉMICA ASCPEJ

TEMAS:

1. Buenas Prácticas:

- Recomendaciones y mejores prácticas para la protección de datos.

2. Tendencias y Desafíos:

- Tendencias y desafíos actuales en la protección de datos, incluyendo la inteligencia artificial y el blockchain.

El presente documento corresponde a una investigación, recopilación y elaboración de información relacionada al tema de capacitación, por lo que queda prohibida la reproducción parcial o total, salvo que sea citado conforme su contenido.

Riobamba, octubre de 2025



1. Buenas Prácticas.

En Ecuador, la protección de datos personales se rige por la Ley Orgánica de Protección de Datos Personales (LOPD), aprobada en 2021 y plenamente vigente desde 2023. Esta ley establece los derechos de los titulares de datos y las obligaciones de las empresas y organizaciones que los procesan.

1.1. Recomendaciones y mejores prácticas para la protección de datos.

a. Para organizaciones y empresas

Las organizaciones deben adoptar una serie de medidas administrativas, técnicas y físicas para proteger los datos personales.

- Cumplimiento legal y responsabilidad proactiva

- **Conozca la LOPDP:** Familiarícese con la ley y sus principios, que incluyen la transparencia, la finalidad, la minimización de datos y la seguridad.
- **Obtenga consentimiento explícito:** Recabe el consentimiento inequívoco de los individuos antes de recolectar y procesar sus datos personales, especialmente si son datos sensibles.
- **Demuestre responsabilidad:** Prepare mecanismos que demuestren que su organización cumple con la protección de datos, como evaluaciones de impacto y análisis de riesgos.
- **Designación de un Delegado de Protección de Datos:** Si aplica, designe un Delegado de Protección de Datos (DPO) para supervisar el cumplimiento de la ley.

- Seguridad técnica

- **Cifrado de datos:** Cifre los datos confidenciales tanto en tránsito como en reposo para protegerlos de accesos no autorizados.
- **Contraseñas robustas y autenticación:** Implemente una política de contraseñas seguras y active la autenticación de múltiples factores siempre que sea posible para el acceso a sistemas y cuentas.
- **Control de acceso:** Aplique el principio de "mínimo privilegio", limitando el acceso a los datos únicamente al personal que lo requiera para sus funciones.
- **Protección contra amenazas:** Utilice *firewalls*, software antivirus y sistemas de detección de intrusos para proteger la infraestructura informática.

- Políticas y procedimientos internos

- **Auditorías periódicas:** Realice auditorías y evaluaciones de riesgos de forma regular para identificar y corregir vulnerabilidades en sus sistemas.
- **Retención de datos:** Almacene los datos personales solo por el tiempo necesario para cumplir la finalidad para la cual fueron recopilados.
- **Respuesta a incidentes:** Establezca un protocolo para notificar a la autoridad competente (Superintendencia de Protección de Datos Personales) y a los afectados en caso de una filtración de datos.
- **Capacitación del personal:** Capacite regularmente a sus empleados sobre las mejores prácticas de seguridad y la importancia de proteger los datos personales.

b. Para individuos

Los ciudadanos también pueden tomar medidas para proteger sus datos personales y ejercer sus derechos bajo la LOPDP.

- **Sea consciente al navegar:** Navegue de forma segura en línea y sea cauteloso al proporcionar información personal en sitios web, correos electrónicos o mensajes.
- **Use contraseñas seguras y únicas:** Utilice una contraseña fuerte y diferente para cada servicio en línea y cámbielas con frecuencia.
- **Active la autenticación de dos factores:** Habilite esta función en todas las cuentas que lo permitan para añadir una capa extra de seguridad.
- **Configure su privacidad en redes sociales:** Revise y ajuste la configuración de privacidad en sus perfiles de redes sociales para controlar quién puede ver su información.
- **Proteja sus dispositivos:** Use contraseñas, *pins* o datos biométricos para bloquear el acceso a sus dispositivos personales, y habilite funciones de rastreo y bloqueo remoto en caso de pérdida o robo.
- **Mantenga su software actualizado:** Asegúrese de que su sistema operativo, aplicaciones y antivirus estén siempre actualizados con los últimos parches de seguridad.
- **Descargue aplicaciones de fuentes oficiales:** Evite descargar software o aplicaciones de sitios web no oficiales para prevenir la instalación de programas maliciosos.
- **Cifre su información sensible:** Si tiene archivos o documentos importantes, considere cifrarlos con contraseña.

2. Tendencias y Desafíos.

Las tendencias actuales en la protección de datos giran en torno a una mayor regulación, la adopción de la privacidad como valor central y el uso de tecnologías avanzadas como la inteligencia artificial (IA) y el *blockchain*. Sin embargo, la integración de estas innovaciones también presenta nuevos desafíos, como la gestión de sesgos en la IA y los problemas de privacidad en redes *blockchain* públicas.

2.1. Tendencias y desafíos actuales en la protección de datos, incluyendo la inteligencia artificial y el blockchain.

a. Tendencias en protección de datos

- **Privacidad como ventaja estratégica:** La protección de datos ha dejado de ser un mero requisito normativo para convertirse en un elemento central de la confianza digital y un factor competitivo para las empresas. La transparencia y el empoderamiento del consumidor son prioritarios.
- **Regulaciones más estrictas:** El panorama normativo continúa evolucionando para ponerse al día con el avance tecnológico. Ejemplo de esto son leyes como la Ley de Datos (Uso y Acceso) de 2025 en el Reino Unido, que incluye disposiciones para la gestión de datos digitales.
- **Aumento de ciberataques impulsados por IA:** Las amenazas cibernéticas se vuelven más sofisticadas con el uso de la IA, lo que exige estrategias proactivas y herramientas avanzadas de ciberseguridad.
- **Enfoque en la seguridad de la cadena de suministro:** Con la creciente dependencia de proveedores externos, las cadenas de suministro se han convertido en un objetivo clave. Esto requiere una mayor atención a la seguridad de los datos que se comparten a lo largo de toda la cadena.
- **Defensa de la privacidad de los datos personales en la IA:** La protección de los datos que los sistemas de IA recopilan, utilizan y almacenan es fundamental. Esto está estrechamente ligado a la privacidad de la información, que se basa en el control individual sobre los datos personales.

b. Desafíos y oportunidades de la inteligencia artificial (IA)

La IA representa un doble filo en la protección de datos, ofreciendo herramientas de seguridad avanzadas, pero también creando vulnerabilidades y dilemas éticos.

- Desafíos:

- **Sesgo algorítmico:** Los modelos de IA se entrenan con datos históricos que pueden reflejar y amplificar sesgos existentes, lo que podría llevar a resultados discriminatorios.
- **Opacidad y falta de transparencia:** La "caja negra" de la IA hace que no siempre sea claro cómo los algoritmos toman decisiones. Esta falta de explicabilidad dificulta la rendición de cuentas y la identificación de posibles problemas de privacidad.
- **Recopilación y abuso de datos:** La IA necesita grandes volúmenes de datos para funcionar, lo que plantea riesgos de recopilación excesiva y uso indebido de información sensible.
- **Nuevas vulnerabilidades:** Los sistemas de IA son susceptibles a ciberataques específicos, como la manipulación de modelos, y a filtraciones de datos.
- **Riesgos de desinformación:** La IA puede ser utilizada para generar contenido falso y engañoso, lo que exige una verificación rigurosa de la información.

- Oportunidades

- **Detección avanzada de amenazas:** La IA puede analizar grandes cantidades de datos para identificar patrones y detectar amenazas de ciberseguridad con mayor eficacia que los métodos tradicionales.
- **Análisis de riesgos:** La IA permite una mejor evaluación de los riesgos de privacidad y seguridad, ayudando a las empresas a anticipar posibles vulnerabilidades.

c. Desafíos y oportunidades del *blockchain*

El *blockchain* promete transparencia e inmutabilidad, lo que puede reforzar la seguridad de los datos. No obstante, su naturaleza descentralizada también plantea desafíos de privacidad.

- Desafíos:

- **Privacidad en redes públicas:** En una *blockchain* pública, todos los nodos tienen acceso a los datos, lo que, a pesar del anonimato y el cifrado, dificulta el control sobre quién accede a la información.
- **Riesgos de ataques de *phishing*:** Al igual que en las redes tradicionales, el *phishing* puede usarse para robar claves privadas, comprometiendo la seguridad de la red.
- **Riesgos para la adopción institucional:** Las grandes empresas e instituciones financieras pueden ser reacias a usar *blockchain* si la tecnología no puede garantizar la privacidad de su información confidencial.

- **Desafíos de escalabilidad:** El crecimiento exponencial de la red puede afectar la eficiencia y el tiempo de respuesta, lo que requiere soluciones innovadoras.

d. Oportunidades

- **Trazabilidad inmutable:** La estructura del *blockchain* hace que sea casi imposible manipular datos, lo que es ideal para registros sensibles como los médicos o la gestión de la cadena de suministro.
- **Transparencia y confianza:** En entornos donde múltiples partes necesitan compartir información, el *blockchain* ofrece una gestión de registros compartida sin depender de una autoridad central, lo que fomenta la confianza.
- **Seguridad criptográfica:** Cada nuevo bloque se conecta criptográficamente a los anteriores, lo que garantiza la integridad y veracidad de las transacciones.