Protección de Datos

Javier Varela
Miguel ángel lles
Daniel ramos

Introducción:

En esta era digital los Marketplace han transformado la manera en que hacemos comprar por internet, sin embargo, la recopilación de datos personales ha generado demasiada duda a los usuarios y desconfianza de que se hace con esos datos. En este informe se redacta de una manera detallada como las compañías utilizan tus datos, las estrategias legales y tecnológicas que

utilizan para protegerlos y las mejores practicas para manejar esta información.

Las grandes compañías como Amazon y los mas grandes Marketplace utilizan los datos por diversos fines, entre ellos:

Personalización de Experiencia: Adaptación de anuncios y mejores recomendaciones de productos

Análisis de Mercado: Estudio de las tendencias y los comportamientos de compra

Seguridad y Prevención de Fraude: Detención de algunas actividades que suelen ser demasiado sospechosas o delictivas

Optimización Logística: Mejora envíos y la gestión de inventarios

Desarrollo de Nuevos Servicios:

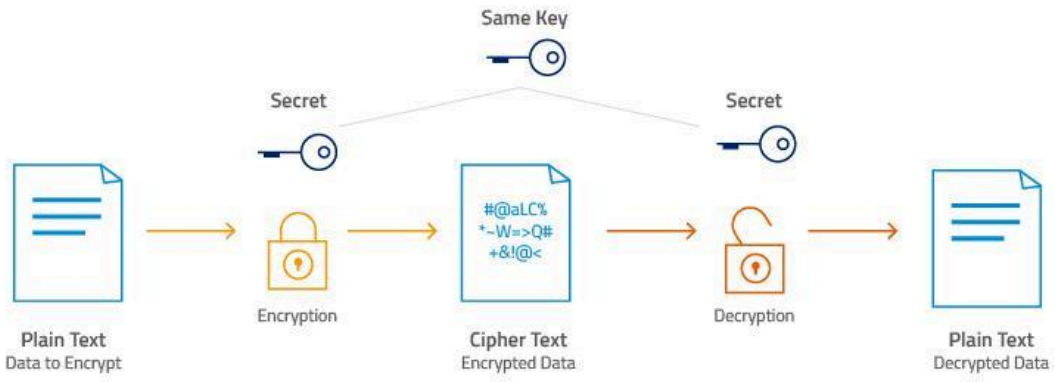
Análisis de datos para innovación y mejora continua

Publicidad Segmentada: Uso de información para dirigir una información especifica al usuario

Protección de Datos:

Las compañías utilizan distintos métodos para proteger la información de los usuarios entre ellos:

Cifrado de datos: Uso de algoritmos de cifrado como AES-256 para proteger datos sensibles



Autenticación Multifactor (MFA):

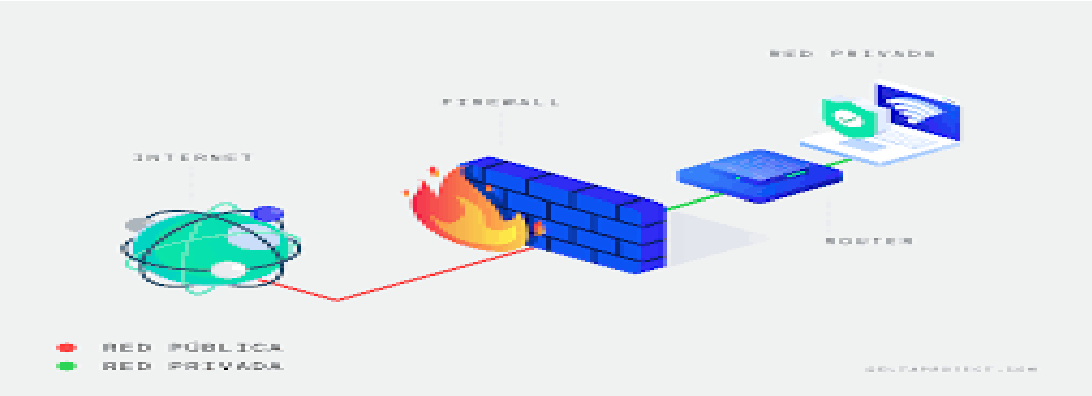
Requerimiento de múltiples credenciales para acceder a cuentas

Monitoreo y detección de intrusos: Implementación de inteligencia artificial para detectar actividades que son sospechosas

Políticas de Retención de Datos:

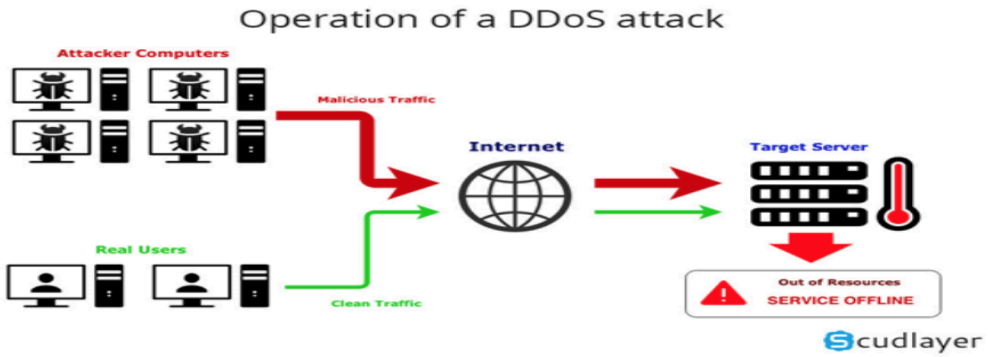
Eliminación de datos innecesarios para minimizar riesgos

Firewalls y Sistemas de Detección de Intrusos: Capas adicionales de seguridad para evitar accesos no autorizados



Protección contra Ataques DDoS:

Implementación de medidas de mitigación ante ataques de denegación de servicio.



Uso de Datos en Casos de Violaciones de Seguridad:

Cuando ocurre una violación de datos, las empresas pueden utilizar la información recopilada para:

Rastrear la Fuente del Ataque:

Identificar vulnerabilidades explotadas.

Notificar a las personas afectadas

Cumplir con regulaciones como el GDPR y CCPA

Colaborar con Autoridades:

Dar y proporcionar evidencias a las autoridades correspondientes

Reforzar la Seguridad: Implementar medidas adiciónales para prevenir futuras violaciones

Registro de Actividades Sospechosas: Documentar eventos para mejorar la protección de la información

Simulaciones de Ataques: Implementación de ejercicios de ciberseguridad para mejorar la respuesta ante alguna de estos incidentes

Recomendaciones para la Protección de Datos en un Marketplace

Implementación de Políticas de Privacidad Claras: Informar en cada momento a los usuarios como y en que se están utilizando sus datos ya que esto generara mas confianza en el usuario y ganara mayor credibilidad la empresa

Uso de Protocolos de Seguridad Avanzados: Implementación de SSL/TLS en todas las transacciones.

Limitación del Acceso a Datos Sensibles: Uso del principio de privilegio mínimo

Auditorías de Seguridad Regulares: Evaluaciones periódicas para detectar vulnerabilidades

capacitación en ciberseguridad: Educar a los usuarios y empleados sobre las buenas practicas

Respaldo periódico de datos: Copias de seguridad para evitar pérdida de información.

Uso Adecuado de los Datos en un Marketplace

Minimización de Datos: Recopilar los datos estrictamente necesarios

Anonimización de Datos: Que estos datos no puedan ser identificables

Consentimiento Explícito: Obtener autorización clara del usuario antes de usar su información

Cumplimiento de Normas Internacionales: Para garantizar estándares de calidad, alguna de estas normas internacionales es:

🎬 Reglamento General de Protección de Datos (GDPR) - Unión Europea

- **Aplicable a cualquier empresa que maneje datos de ciudadanos de la UE, sin importar su ubicación.**
- Establece principios clave como el consentimiento explícito, el derecho al olvido y la portabilidad de datos.
- Requiere notificación obligatoria de violaciones de datos en un plazo máximo de 72 horas.

🎬 Ley de Privacidad del Consumidor de California (CCPA) - EE. UU.

- Otorga a los residentes de California el derecho a conocer, eliminar y optar por no vender sus datos personales.
- Exige transparencia en la recopilación y el uso de información por parte de las empresas.

🎬 Ley de Protección de Información Personal y Documentos Electrónicos (PIPEDA) - Canadá

- Regula cómo las organizaciones privadas pueden recopilar, usar y divulgar datos personales.

- Obliga a las empresas a obtener consentimiento para el procesamiento de datos.

🎬 Ley de Protección de Datos Personales (LGPD) - Brasil

- Similar al GDPR, otorga a los ciudadanos brasileños control sobre sus datos personales.
- Impone sanciones severas por el incumplimiento de la normativa.

🎬 Norma ISO/IEC 27001 - Gestión de Seguridad de la Información

- Establece un marco de mejores prácticas para la protección de información sensible.

- Requiere que las empresas implementen controles de seguridad y evaluaciones de riesgos.

Acciones en Caso de Violación de Datos:

Detección y Contención: Detectar el origen y cerrar vulnerabilidades

notificación inmediata: Informar a los usuarios y autoridades según la legislación vigente.

investigación Forense: Investigar la magnitud y el impacto de la violación de datos

Refuerzo de Seguridad: Implementar medidas adicionales para evitar reincidencias

Evaluación de Responsabilidad: Analizar posibles fallos internos y determinar responsabilidades

Revisión y Mejora de Protocolos:

Actualizar políticas de seguridad para prevenir futuras violaciones.

Métodos Tecnológicos y Legales para la Protección de Datos:

Las empresas deben combinar estrategias tecnológicas y legales tales como:

Normativas y Regulaciones:

Tratamiento de Datos en Chats de Ecommerce o Marketplace:

En Colombia, la Ley 1581 de 2012 protege la privacidad de las comunicaciones entre usuarios.

- Los administradores de un Marketplace no deberían acceder a los chats sin consentimiento expreso de los usuarios o sin una orden judicial.

- La persistencia de estos datos debe ser regulada mediante políticas de retención y eliminación seguras.

- Se recomienda implementar cifrado de extremo a extremo para garantizar la privacidad.

- El cumplimiento de GDPR, CCPA, y otras leyes de protección de datos.

GDPR (General Data Protection Regulation): Reglamento europeo que protege la privacidad y seguridad de los datos personales de los ciudadanos de la UE.

CCPA (California Consumer Privacy Act): Ley de privacidad en California que otorga a los consumidores mayor control sobre sus datos personales.

Contratos de Confidencialidad:

Acuerdos con empleados y terceros

Implementación de Inteligencia Artificial: automatización en detección de amenazas

Blockchain para Seguridad: Uso de tecnológica descentralizada para proteger datos sensibles

Asesoramiento Legal Especializado: Consultoría jurídica para garantizar cumplimiento normativo.

Monitoreo en Tiempo Real: Implementación de sistemas de alerta ante posibles brechas de seguridad.

Pruebas de Penetración:
Evaluaciones periódicas para identificar vulnerabilidades.

Compensación y Reputación:
Ofrecer soporte a los afectados y mejorar la confianza del publico

Conclusión : La protección de datos en Ecommerce y Marketplace son importante para evitar fraudes, ciberataques y garantizar la confianza de los usuarios , las empresas deben de aplicar estrategias tecnológicas avanzadas ,

cumplir con regulaciones legales y fomentar la cultura de la seguridad en toda la organización Implementar medidas de protección adecuadas no solo resguarda la información de los usuarios, sino que también fortalece la reputación y sostenibilidad del Marketplace a largo plazo