UNIVERSIDAD SERGIO ARBOLEDA | Colsubsidio

Diplomado de Ciberseguridad y Gestión de Seguridad de la Información

Módulo 3:

Regulación de la Seguridad de la Información y Protección de Datos

Sesión 1:

Introducción a la regulación de seguridad y protección de datos

OBJETIVO DE LA SESIÓN:

Comprender los marcos regulatorios nacionales e internacionales sobre protección de datos y seguridad de la información, su importancia y aplicación general.

UNIVERSIDAD SERGIO ARBOLEDA | Colsubsidio

Fugas de datos afectan al 46% de las empresas en Colombia

La vulneración de información personal es una grave
ciberataques a empresas. En el Día Inte
Personales, los expertos de Kaspersky
cuidarlos.

MEGABASE CON 700 GB DE DATOS PERSONALES DE CIUDADANOS MEXICANOS, A LA VENTA EN FORO DE FILTRACIONES

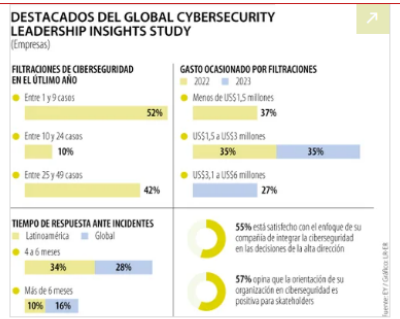
univision NOTICIAS | POLITICA | INMIGRACIÓN | DINERO | EEUU | INFOGRAFÍAS | TRABAJOS

Hackers

"La mayor filtración de datos en la historia": hallan 16,000 millones de contraseñas en la 'dark web'

datos, que incluyen
ría ser explotada por

LR | INICIO / INTERNET ECONOMY / *Más de 60% de las empresas en Latinoamérica ha sido víctima de filtración de datos*



TECNOLOGÍA

Más de 60% de las empresas en Latinoamérica ha sido víctima de filtración de datos

de ESET

DESTA

sábado, 14 de octubre de 2023

GUARD

Privacidad

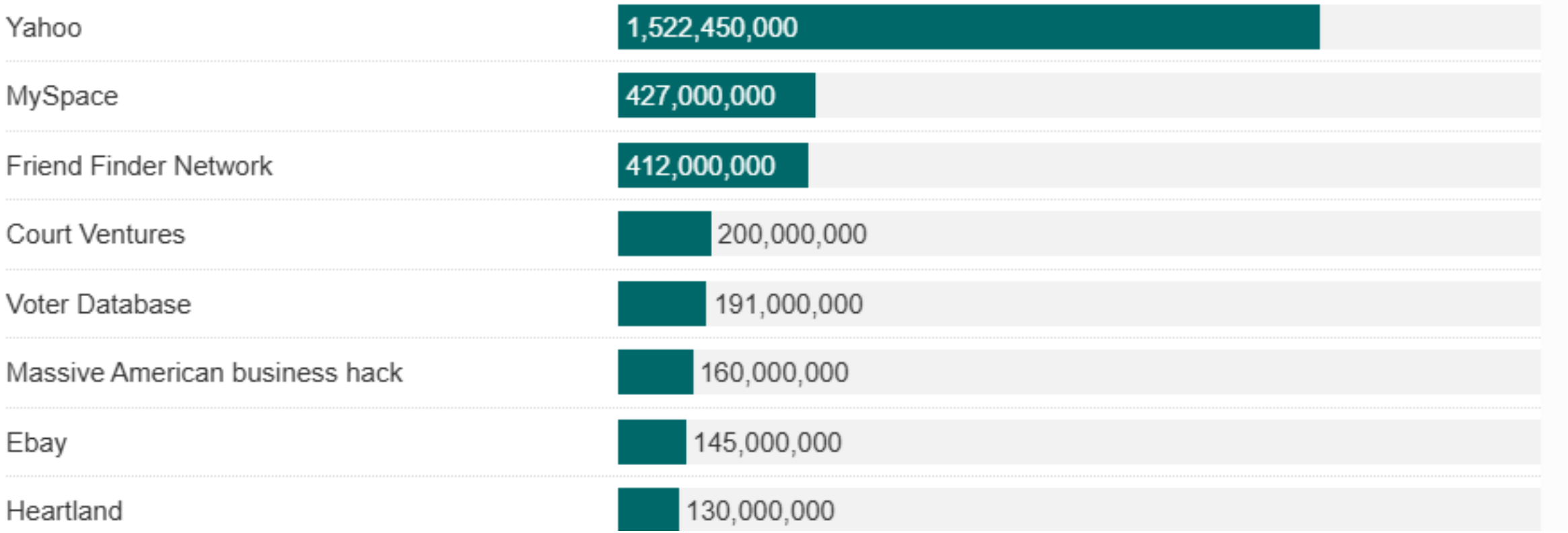
Las filtraciones de datos de 2024 ya se cuentan por miles de millones

Un resumen de las filtraciones de datos más significativas de 2024, con más de 1500 millones de datos filtrados en lo que va del año.

Robo de datos

Los mayores robos de datos del siglo XXI

Las cifras representan el número de documentos robados / filtrados



Tomado de 14

Filtración Canva

En mayo de 2019, Canva, la plataforma de diseño gráfico, sufrió una filtración de datos que afectó a sus 137 millones de suscriptores. Los datos expuestos incluían direcciones de correo electrónico, nombres de usuario, nombres, ciudades de residencia y contraseñas almacenadas como hashes bcrypt para usuarios que no utilizaban redes sociales.

Datos comprometidos

- Direcciones de correo electrónico
- Ubicaciones geográficas
- Nombres
- Contraseñas
- Nombres de usuario

Acciones recomendadas

- Cambiar su contraseña
- Habilitar la autenticación de dos factores
- Crea contraseñas con una combinación de letras difícil de averiguar (mayúsculas, minúsculas, números y caracteres especiales).

Canva tomó medidas para proteger las cuentas de los usuarios, incluyendo la invalidación de contraseñas comprometidas y la notificación a los usuarios afectados.

¿Por qué existen leyes y normas sobre seguridad de la información?

La información es un activo valioso. Su mal uso o exposición puede afectar derechos fundamentales (como la privacidad), generar pérdidas económicas o dañar la reputación de personas y organizaciones. Por eso, los países y organismos internacionales han creado normas que:

- Protegen los datos personales
- Establecen requisitos de seguridad mínimos
- Definen sanciones por incumplimiento

Normas y estándares internacionales

ISO/IEC 27001 – Seguridad de la Información

- Estándar internacional que define **requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI).**
- Incluye procesos de identificación de riesgos, implementación de controles, auditorías y mejora continua.

GDPR – Reglamento General de Protección de Datos (Unión Europea)

- Ley europea de protección de datos personales con alcance extraterritorial.
- **Ejemplo:** Si una empresa colombiana ofrece servicios a ciudadanos europeos, debe cumplir GDPR.

Diferencia entre Ley (obligatoria) y Estándar (voluntario)

Ley	Estándar
Es obligatoria, emitida por el Estado	Es voluntario, creado por entidades de estandarización
Su incumplimiento genera sanciones legales	Su incumplimiento no genera sanción legal, pero afecta certificaciones y reputación

ISO 27001: Gestión de la seguridad de la información

- Publicada por primera vez en 2005 (actualizada en 2013 y 2022).
- Forma parte de la familia ISO/IEC 27000, enfocada en la seguridad de la información.
- Estándar certificable → una empresa puede demostrar públicamente que cumple con buenas prácticas.

Propósito:

crear un marco de trabajo que ayude a las organizaciones a:

Identificar riesgos de seguridad

Definir políticas y procedimientos claros.

Establecer controles técnicos, humanos y físicos

Se basa en la idea de que no hay seguridad absoluta, pero sí se pueden gestionar riesgos.

Enfoque basado en riesgos: se identifican amenazas (ej: ataques, fugas de datos, errores humanos).

Controles de seguridad:

- Políticas de acceso.
- Uso de contraseñas seguras.
- Cifrado de datos.
- Copias de seguridad periódicas.

Claves de ISO 27001

Ciclo de mejora continua (PDCA):

- Planificar → Detectar riesgos.
- Hacer → Implementar medidas.
- Verificar → Auditar el SGSI.
- Actuar → Corregir y mejorar.

Beneficios:

- Protege la reputación de la organización.
- Evita sanciones legales por incumplimientos.
- Aumenta la confianza de clientes y usuarios.

Ejemplos de Aplicación ISO27001

Banco

- Riesgo: Robo de información financiera de clientes.
- Aplicación: ISO 27001 exige políticas de acceso y cifrado de datos.
- Ejemplo: El banco define que solo empleados de un área específica pueden acceder a la base de datos de transacciones → si un intruso entra, los datos están cifrados y no sirven sin la clave.

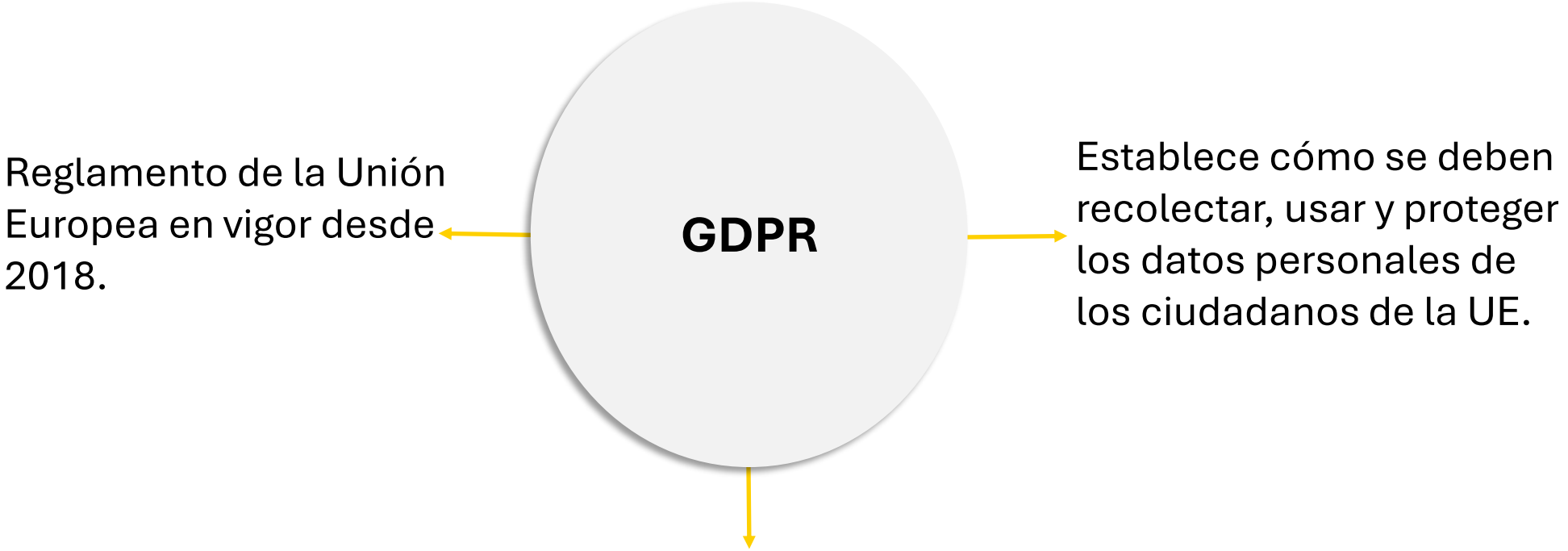
Universidad

- Riesgo: Alteración de calificaciones por un ataque interno.
- Aplicación: Controles de seguridad del SGSI (Sistema de Gestión de Seguridad de la Información).
- Ejemplo: El sistema requiere autenticación de dos factores para que un profesor suba notas, evitando accesos no autorizados.

Comercio electrónico

- Riesgo: Caída del sistema en fechas de alta demanda (Black Friday).
- Aplicación: ISO 27001 incluye planes de continuidad de negocio.
- Ejemplo: La empresa tiene servidores redundantes en la nube que garantizan disponibilidad incluso si falla el servidor principal.

GDPR (Reglamento General de Protección de Datos)



Principios y derechos en GDPR

Principios

- Consentimiento explícito para uso de datos.
- Minimización: recolectar solo los datos necesarios.
- Transparencia: informar al usuario sobre el uso de datos.

Derechos del usuario

- Acceso, rectificación y borrado de sus datos (“derecho al olvido”).
- Portabilidad de datos.
- Derecho a ser informado en caso de fuga de información.

Consentimiento explícito

- Una aplicación de salud pide permiso al usuario para recopilar datos sobre frecuencia cardíaca.
- GDPR exige que el usuario marque una casilla de consentimiento y que pueda retirarlo en cualquier momento.

Minimización de datos

- Una tienda online solicita nombre, correo y dirección para entregar un pedido.
- No puede pedir datos innecesarios como “estado de salud” o “religión”, porque GDPR obliga a recopilar solo lo estrictamente necesario.

Notificación de brechas de seguridad

- Una aerolínea europea sufre una fuga de datos de 200.000 pasajeros.
- Según GDPR, debe notificar a la autoridad de protección de datos en un máximo de 72 horas y avisar a los afectados.

Derecho al olvido

- Un exusuario solicita a una red social que borre toda su información.
- La empresa está obligada por GDPR a eliminar sus datos permanentemente en un tiempo razonable.

Concepto de Datos Personales y Datos Sensibles

Datos personales

Información que identifica o puede identificar a una persona.
Ejemplo: nombre, cédula, correo.

Datos sensibles

Información que, de ser expuesta, puede generar discriminación.
Ejemplo: salud, orientación sexual, religión.

Datos Personales

Son cualquier información que identifica o puede identificar a una persona.
No siempre son peligrosos, pero requieren protección porque permiten reconocer al individuo.

- **Nombre completo:** Identifica directamente a la persona.
- **Número de cédula, pasaporte o NIT:** Es un identificador único oficial.
- **Dirección, teléfono, correo electrónico:** Permiten ubicar o contactar a alguien.
- **Fecha de nacimiento:** Puede usarse para validar identidad o perfilar edad.
- **Información académica o laboral (cargo, empresa, título universitario):** Identifica trayectoria personal.

Se protegen porque si se difunden sin control pueden dar lugar a fraudes, suplantaciones o pérdida de privacidad.

Datos Sensibles

Son aquellos que afectan la intimidad más profunda de la persona o pueden dar lugar a discriminación si se usan indebidamente.
La ley exige un nivel mayor de protección y consentimiento explícito.

- **Salud (diagnósticos, historia clínica, resultados médicos):** Pueden generar discriminación laboral o en seguros.
- **Orientación sexual:** Riesgo de discriminación o estigmatización.
- **Creencias religiosas:** Puede dar lugar a exclusión social o laboral.
- **Opiniones políticas:** Puede exponer a persecución o represalias.
- **Datos biométricos (huella, iris, reconocimiento facial, ADN):** Son únicos e irremplazables, si se filtran no se pueden cambiar como una contraseña.
- **Origen étnico o racial** : Riesgo de racismo o exclusión.

Se protegen más porque son altamente sensibles a mal uso y pueden vulnerar derechos fundamentales como la igualdad, la no discriminación y la intimidad.

Ejercicio 1: Clasificación de datos

Instrucción: Clasifica los siguientes como “dato personal común” o “dato sensible”:

1. Correo electrónico personal
2. Diagnóstico médico
3. Dirección de residencia
4. Preferencia religiosa
5. Número de teléfono laboral

¿Qué pasaría sin regulación?

Venta de bases de datos con información médica

- Sin regulación, los datos de salud pueden ser comercializados sin consentimiento.
- Se perdería la confianza en hospitales, EPS y aseguradoras, afectando la disposición de las personas a compartir información médica.

Riesgo de mal uso por aseguradoras (ej: subir primas a pacientes con enfermedades crónicas).

Conclusión: la falta de leyes genera un círculo de desconfianza en el sistema de salud y abre la puerta a abusos económicos.

Discriminación laboral por diagnósticos o creencias religiosas.

- Empresas podrían rechazar candidatos por condiciones médicas o creencias personales.
- Esto afectaría la igualdad de oportunidades y fomentaría la exclusión social.
- Sin regulación, no existiría un marco legal para denunciar estas prácticas.

Conclusión: la ausencia de normas permitiría la discriminación abierta, afectando derechos humanos básicos como la igualdad y la no discriminación.

Ley de Protección de Datos Personales (Habeas Data) (Ley 1581 de 2012)

- Reconoce el derecho fundamental de toda persona a conocer, actualizar y rectificar la información que sobre ella se recoja en bases de datos.
- Regula la manera en que empresas, instituciones y entidades públicas deben recolectar, almacenar, usar y compartir datos personales.
- Asegura que los datos sean tratados con consentimiento previo, expreso e informado.
- La autoridad de control en Colombia es la Superintendencia de Industria y Comercio (SIC).

Principios del Habeas Data

En Colombia (y Latinoamérica), la Ley de Habeas Data garantiza que las personas sean dueñas de su información personal y puedan decidir cómo se usa.

Autorización	Se requiere consentimiento del titular para recolectar o usar sus datos.
Finalidad	Solo pueden usarse para los fines informados.
Veracidad	Los datos deben ser correctos y actualizados.
Acceso y corrección	Las personas pueden conocer y corregir su información.
Seguridad	Quien administra datos debe protegerlos frente a accesos no autorizados o pérdida.

Ejemplo práctico: Una universidad recolecta datos de estudiantes. Debe:

- Pedir autorización para usarlos.
- Usarlos solo para fines académicos o administrativos (no para vender bases de datos).
- Protegerlos con claves y permisos adecuados.

Casos de aplicación del Habeas Data

Comercio electrónico
Una tienda online no puede vender tu información de contacto a terceros sin tu consentimiento.

Redes sociales
Si solicitas la eliminación de tu perfil y datos, la plataforma debe atender tu petición.

Banco
Solo puede consultar tu historial crediticio si le diste autorización y debe corregir errores si los reportas

Clínica
Debe pedir tu autorización para usar tu historia clínica en estudios de investigación.

Ejercicio 2: Recolección de datos sensibles en campaña de salud

Situación:

Una empresa recolecta datos de sus empleados para una campaña interna de salud, incluyendo información sobre enfermedades crónicas.

Preguntas:

1. ¿Qué tipo de datos recolecta?
2. ¿Qué precauciones debe tener según la Ley de Protección de Datos y la ISO/IEC 27001:2022?

Tipo de datos: Datos sensibles

- Salud
- enfermedades crónicas

Precauciones

- Solicitar autorización expresa de cada empleado.
- Garantizar que los datos se usen solo para la campaña de salud.
- Proteger la información con acceso restringido y cifrado.
- Evitar compartir la base con terceros sin consentimiento.

Ejercicio 3: Consecuencias de la falta de regulación y protección de datos

¿Qué crees que pasaría si las empresas pudieran usar tu información sin autorización o fines claros?

Actividad: Protección de datos sensibles con cifrado César

Objetivo

- Comprender cómo los datos sensibles (como salud y religión) deben tratarse de manera especial, cifrándolos para que no queden expuestos en texto plano, y que solo puedan ser vistos bajo autenticación.

Instrucciones

- Cree un DataFrame con datos personales (nombre, edad, correo, diagnóstico médico, religión).
- El programa cifrará solo los datos sensibles (Diagnóstico Médico, Religión).
- Los datos cifrados se guardan en el DataFrame.
- El usuario solo podrá ver los datos descifrados si ingresa un usuario y contraseña correctos.

Referencias

1. Bishop, M. (2003). *Computer Security.*
2. Briceño, E. (2021). *Seguridad De La Información*
3. Kremer, E. Et al. (2019). *Ciberseguridad*
4. Ozkaya, E. (2019). *Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity*
5. *NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA 27001*
6. *General Data Protection Regulation (GDPR)*
7. *LEY ESTATUTARIA 1581 DE 2012. Link: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981*
8. *Bravo, C. A. (s/f). ¿Cómo nos afectan las filtraciones de datos? Welivesecurity.com. Recuperado el 21 de agosto de 2025, de https://www.welivesecurity.com/es/concientizacion/como-nos-afectan-las-filtraciones-de-datos/*
9. *Filtran gratis base con datos de más de 2 millones de tarjetas de crédito y débito. (s/f). Eset.com. Recuperado el 21 de agosto de 2025, de https://www.eset.com/py/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/filtran-gratis-base-con-datos-de-mas-de-2-millones-de-tarjetas-de-credito-y-debito0/*
10. *Marín, M. (2025, junio 21). 16 mil millones de credenciales al descubierto: ¿el robo del siglo o un espejismo? Una Al Día; Hispasec. https://unaaldia.hispasec.com/2025/06/filtrados-16-000-millones-de-credenciales-procedentes-de-infostealers-la-megalista-que-multiplica-el-riesgo-de-phishing-y-secuestro-de-cuentas.html*
11. *Naranjo, D. H. (2025, junio 9). Estas son las formas en las que puede ser víctima de un fraude de seguros. Portafolio. https://www.portafolio.co/economia/finanzas/fraudes-en-seguros-mas-de-30-000-casos-en-colombia-en-2024-y-asi-puede-evitarlos-632416*
12. *Sadylko, A. (2024, septiembre 4). RockYou2024 y las otras cuatro filtraciones de datos más grandes de la historia. Kaspersky. https://www.kaspersky.es/blog/top-five-data-breaches-in-history/30364/*
13. *Sánchez, S. (2017, enero 28). Más de 5 mil millones de documentos y 229 empresas afectadas: así han sido los mayores robos de datos de la historia. Xataka.com; Xataka. https://www.xataka.com/privacidad/mas-de-5-mil-millones-de-documentos-y-229-empresas-afectadas-asi-han-sido-los-mayores-robos-de-datos-de-la-historia*