ANÁLISIS DE VULNERABILIDADES EN LA CADENA DE CUSTODIA DIGITAL - CASO PARAMOUNT Y RENAUT.

Este análisis aborda la filtración y el error en cadenas de custodia donde la información es el recurso más valioso.

Recientemente, la industria del entretenimiento y la ciberseguridad han sido testigos de un evento que ilustra a la perfección la fragilidad de las infraestructuras corporativas modernas: la filtración de activos críticos de propiedad intelectual. El caso que ha dominado los medios en abril de 2026 involucra a Paramount Pictures y la exposición no autorizada de la película animada *Avatar Aang, The last airbender*, un proyecto que representa años de desarrollo y decenas de millones de dólares en inversión.

Marco teórico:

La deconstrucción de la confianza y el colapso de la defensa perimetral ante la naturaleza humana.
Fecha 16 de Abril de 2026 | Publicado por Cruger Corp

El actual ecosistema digital en ciberseguridad a nivel de empresas y dependencias opera bajo una premisa que ha demostrado ser estructuralmente deficiente: la dependencia de la defensa perimetral y la confianza implícita en el factor humano. El presente marco teórico se fundamenta en la deconstrucción de la "cadena de custodia digital", entendida no solo como el tránsito de la información entre servidores, sino como el ciclo vital del dato interactuando con usuarios e interfaces operativas. Tradicionalmente, la ciberseguridad ha enfocado sus recursos en blindar el perímetro tecnológico mediante firewalls, monitoreo heurístico y sistemas de detección de intrusos. Sin embargo, este enfoque ignora una vulnerabilidad asimétrica: la capa psicológica del modelo operativo, es decir, la propia naturaleza humana.

La teoría de la "confianza por defecto" postula que, una vez dentro de una red o cadena operativa, las interacciones gozan de legitimidad presunta. Esta falacia arquitectónica es el terreno donde la ingeniería social prospera de manera implacable. La manipulación psicológica —a través de vectores como el *phishing*, el *pretexting* o el *baiting*— no requiere vulnerar el cifrado de un servidor centralizado; simplemente requiere hackear el comportamiento de quien ya posee la llave de acceso. Estadísticamente, la ingeniería social y el error humano se han consolidado como los vectores de ataque primarios y más rentables para los cibercriminales.

Paralelamente, la adopción de la hiperconectividad en la nube ha amplificado el impacto de los errores de configuración técnica. Centralizar activos críticos convierte un error humano periférico —como la mala configuración de permisos en un servidor o el envío accidental de información por canales inseguros— en una brecha sistémica de proporciones catastróficas. Si un dato no está intrínsecamente protegido, su exposición es inevitable.

Frente al colapso evidente de este modelo perimetral, surge la teoría de la Confianza Cero (*Zero Trust*) y el cifrado estructural inherente. Esta doctrina corporativa propone que la única defensa lógica y matemática viable frente a la ingeniería social es asumir la brecha como un estado constante. La verdadera resiliencia no se alcanza intentando erradicar el error de la naturaleza humana, sino aislando el activo criptográficamente para garantizar que, ante cualquier exfiltración, el atacante reciba únicamente un bloque de datos inútil.

Vectores de implementación de análisis, no para este caso sino como metodología de casos relacionados con la filtración, exfiltración y exposición, entre ellos se encuentran:

1- Vulnerabilidades conocidas.
2- Vulnerabilidades en brechas de seguridad.
3- Vulnerabilidades de exposición por actores internos.
4- Vulnerabilidades de explotación de canales inseguros.
5- Vulnerabilidades en la cadena de custodia (error humano).

Las primeras versiones apuntaban a un error humano catastrófico — el supuesto envío accidental del archivo a un usuario aleatorio mediante correo electrónico de nombre **ImStillDissin** —. Sin embargo, tras el análisis y después de la verificación, los reportes sugirieron la intervención de actores maliciosos (hackers o grupos dedicados como PeggleCrew), apuntando a una brecha a través de vulnerabilidades o métodos sofisticados.

En algunos medios se emplea la teoría de que podría tratarse de un fallo en él envió por parte de Paramount Pictures hacia Nickeolodeon y termino por llegar a un usuario de manera aleatoria sin relación con el proyecto, mientras que en comunicados recientes el tema apunta a un hackeo hacia el proyecto relacionado con la película, el tema es una muestra del análisis que empleamos para este caso y otros que han sido pieza clave para entender el comportamiento de los atacantes durante estos eventos. No se puede determinar a esta fecha la naturaleza del ataque o el error, por lo que solamente se emplea como caso de estudio para desglosar incidentes y tendencias de ciberataques.

En Cruger Corp, nuestro objetivo es analizar las posibles causas y métodos de seguridad para la prevención de riesgos en materia de ciberseguridad. Por lo qué, utilizamos este incidente —independientemente de si su origen final se dictamina como un error de vector, o un ataque asimétrico dirigido — como un caso de estudio fundamental. Este evento es una muestra de la dependencia de canales de comunicación vulnerables y métodos poco seguros que muchas veces son vulnerados por los atacantes. El verdadero debate no radica en cómo el atacante (o el error) vulneró la puerta, sino en por qué la información sensible se pudo comprometer de manera directa (a través de las filtraciones del propio usuario que ha comenzado a compartir según se reporta en varios medios, parte del material de la productora).

Para definir la manera de este análisis empleamos diferentes enfoques que son los que a menudo enfrentan las empresas, industrias y los corporativos, no siempre se trata de ataques sofisticados que intentan romper los sistemas más seguros empleados por las entidades, sino que emplean practicas más sencillas pero que son irónicamente más efectivas contra los sistemas avanzados. Entre ellos está la ingeniería social, un método que ha tomado fuerza debido a que es más efectivo contra los usuarios independientemente de su nivel de preparación o su puesto dentro de una organización.

¿QUÉ ES LA INGENIERÍA SOCIAL?: Es una práctica de manipulación psicológica diseñada para engañar a los usuarios y lograr que revelen información confidencial, entreguen credenciales de acceso o ejecuten acciones que comprometan la seguridad de una organización, aunque pueden ir en diferentes rutas según el enfoque del vector de ataque, buscando información (Análisis de datos), envió de credenciales (Accesos), suplantación de identidad entre otros.

En términos de arquitectura de sistemas, la ingeniería social es **la explotación del factor más vulnerable de la cadena de custodia de un activo: Es decir, la naturaleza humana.** No importa si un corporativo invierte millones de dólares en firewalls de última generación, monitoreo heurístico o detección de intrusos; si un atacante logra convencer a un empleado (de cualquier eslabón de la cadena ya sea básico o con privilegios) para que le "abra la puerta" desde adentro, todo el perímetro técnico se vuelve absoluta y matemáticamente irrelevante.

El éxito abrumador de la ingeniería social radica en que elude la confrontación directa con la tecnología de defensa. Los atacantes modernos entienden que es infinitamente más barato, rápido y efectivo hackear el comportamiento de la psique humana, que hackear un servidor. Esta práctica se materializa en diversas tácticas que explotan la urgencia, el miedo, la curiosidad o la confianza:

- **Phishing y Spear-Phishing:** El despliegue de comunicaciones fraudulentas (usualmente por correo electrónico) que simulan provenir de fuentes legítimas, diseñadas para robar credenciales. Su evolución (*spear-phishing*) dirige estos ataques a perfiles de alto valor, como directivos o administradores de bases de datos.

- **Pretexting (Creación de escenarios):** La elaboración de una mentira estructurada donde el atacante asume una identidad falsa (ej. soporte técnico de TI, un proveedor de nube o una figura de autoridad interna) para solicitar datos críticos bajo una premisa aparentemente lógica y urgente.

- **Baiting (Cebos):** Aprovechar la curiosidad del usuario, ofreciendo algo atractivo (un archivo descargable, un dispositivo USB abandonado estratégicamente) que al ser ejecutado instala código malicioso dentro de la red que debía estar segura.

Bajo nuestra doctrina, la existencia y eficacia continua de la ingeniería social demuestra el fallo sistémico del modelo actual de ciberseguridad corporativa. Mientras los sistemas asuman "confianza por defecto" hacia las acciones de los usuarios internos, el error humano o la manipulación psicológica seguirán siendo la llave maestra para el secuestro y la exfiltración de activos críticos. No solo eso, además el tema genera ganancias por millones anualmente, en modelos de ataque que buscan obtener información de tarjetas de crédito o cuentas bancarias de los usuarios más básicos (ataques por volumen de la cadena dirigida), mismos que van en aumento según la tendencia de la curva de apreciación desde 2020. Se puede ver reflejado en las quejas de los clientes a sus proveedores de servicios bancarios cuando se efectúan aclaraciones por saldos no reconocidos.

La ciberseguridad tradicional se ha enfocado en construir muros perimetrales cada vez más altos. Las corporaciones gastan millones en firewalls, sistemas de detección de intrusos (IDS) y monitoreo basado en Inteligencia Artificial. Sin embargo, los atacantes modernos rara vez intentan "romper" el muro por la fuerza bruta; simplemente le piden la llave al guardia.

Aquí es donde entra la ingeniería social y el phishing. Un ataque sofisticado a menudo comienza con el eslabón menos sofisticado de la cadena: el factor humano. Un empleado fatigado que hace clic en un enlace que simula ser una directiva de Recursos Humanos, un ejecutivo que es víctima de *spear-phishing* y el atacante ya tiene acceso a su red comprometida, un simple carácter cambiado en un correo electrónico podría suplantar la identidad de una empresa reconocida y llevar al usuario hacia una página artificial donde sea el mismo quien exponga su información, personal, bancaria o de acceso a redes.

Empíricamente, los errores humanos y la manipulación psicológica (ingeniería social) son estadísticamente los vectores de ataque más rentables para los cibercriminales. Cuestan fracciones de centavo ejecutar un correo de phishing, pero los daños por la exfiltración de los datos comprometidos

escalan a millones de dólares. Con la IA lejos de resolver estos ataques, han creado puertas de entrada de granjas automatizadas de ataques que simplifican las acciones de suplantación, como creación de páginas, envíos masivos de correos electrónicos o incluso clonación de voz, algunos más sofisticados emplean videollamadas donde cambian su rostro por el de la identidad suplantada para facilitar la confianza con el usuario, y aunque hay medidas para detectar estos fallos, son los propios usuarios los que omiten verificarlos, dientes, manos, fondos o incluso falta de parpadeo y una interacción antinatural delataba las primeras muestras de estos procesos. Hoy con la IA cada vez más revolucionaria como modelo que busca reinventarse a sí misma, se busca corregir estos errores por lo que lejos de facilitar la detección estarían ayudando a sofisticar los ataques de suplantación. Herramientas que permitan visualizar si se está haciendo uso de filtro son parte de los desarrollos que se busca generar para mitigar estos casos.

EL COSTO DE LA FALTA DE CIFRADO: CASOS HISTÓRICOS Y LECCIONES IGNORADAS

Para entender la magnitud del problema, debemos analizar el historial corporativo, donde errores de configuración o engaños al personal resultaron en desastres financieros que podrían haberse mitigado casi en su totalidad con una arquitectura de cifrado estructural (cifrado en reposo y en tránsito).

1. EL HACKEO A SONY PICTURES ENTERTAINMENT (2014) - EL PRECEDENTE DE LA PROPIEDAD INTELECTUAL. Uno de los casos más paralelos al incidente actual de Paramount fue el ataque a Sony Pictures. Los atacantes utilizaron correos de *spear-phishing* dirigidos a empleados clave para robar credenciales de acceso. Una vez dentro de la red, los atacantes tuvieron acceso libre durante meses. El resultado fue la filtración de películas aún no estrenadas, guiones, datos financieros y miles de correos electrónicos confidenciales de ejecutivos.

- **El fallo:** La información crítica (películas, correos, bases de datos) estaba almacenada en texto plano o con protecciones perimetrales básicas, no bajo cifrado robusto independiente.

- **El costo:** Más de 15 millones de dólares solo en costos de investigación y remediación inmediata, sumado a un daño reputacional incalculable y la renuncia de altos directivos. Si los archivos hubieran estado cifrados con llaves gestionadas fuera de esa red, los hackers habrían robado terabytes de ruido criptográfico inútil.

A esto sumamos el tema de las empresas por mantener sus datos críticos en servidores interconectados, donde un acceso es capaz de comprometer la red completa donde todos los sistemas conectados a la misma red o interconectados entre si son considerados vulnerables.

Observatorio Ciberseguridad (2025). Ciberataque a Sony Pictures de 2014. Recuperado el 13 de Abril de 2026. De Observatorio Ciberseguridad. Website: https://observatoriociber.org/ciberataque-sony-pictures-de-2014/

Wikipedia La enciclopedia libre (2025). Hackeo a Sony Pictures en 2014. Recuperado el 13 de Abril de 2026. De Wikipedia La enciclopedia libre. Website: https://en.wikipedia.org/wiki/2014_Sony_Pictures_hack

FBI Federal Bureau of Investigation (2014). Actualización sobre la investigación de Sony. Recuperado el 13 de Abril de 2026. De FBI Federal Bureau of Investigation. Website: https://www.fbi.gov/news/press-releases/update-on-sony-investigation

2. LA VULNERABILIDAD DE LA NUBE POR ERROR HUMANO: VERIZON Y NICE SYSTEMS (2017). El error humano no siempre implica ser engañado por un hacker; a menudo es un error de configuración técnica. En 2017, un empleado de Nice Systems, un proveedor externo de Verizon, configuró incorrectamente un servidor en la nube (un *bucket* de Amazon S3) dejándolo abierto al público.

- **El fallo:** Ningún hacker tuvo que vulnerar contraseñas. Un simple error de parámetros expuso los nombres, direcciones, números de teléfono y PINs de cuentas de 14 millones de clientes de Verizon.

- **La solución ausente:** Aunque el error humano (dejar la puerta abierta) es casi imposible de erradicar matemáticamente, si esa base de datos hubiera estado fuertemente cifrada (donde la llave no reside en el mismo servidor público), el error humano no habría provocado una exposición de datos. Cualquiera que entrara al servidor público solo habría visto código ilegible.

The Hacker News (2017). Over 14 Million Verizon Customers' Data Exposed On Unprotected AWS Server. Recuperado el 13 de Abril de 2026. De The Hacker News. Websiite: https://thehackernews.com/2017/07/over-14-million-verizon-customers-data.html#:~:text=Verizon%2C%20the%20major%20telecommunications%20provider,%2C%20data%20security%2C%20and%20surveillance.

Notimex (2017). Filtran datos de 6 millones de usuarios de Verizon Recuperado el 13 de Abril de 2026. De El Economista. Website: https://www.eleconomista.com.mx/tecnologia/Filtran-datos-de-6-millones-de-usuarios-de-Verizon-20170712-0141.html

3. TWITCH Y EL ERROR DE CONFIGURACIÓN DEL SERVIDOR (2021) La plataforma de streaming Twitch sufrió una filtración masiva (más de 100 GB de datos) que incluyó su código fuente completo y los reportes de pagos financieros de sus creadores de contenido. La compañía admitió que la brecha se debió a "un error en un cambio de configuración del servidor" ejecutado por su propio equipo. Un error humano interno le dio acceso a

terceros maliciosos a la columna vertebral de la empresa. El tema incluso fue explicado a detalle por su propia empresa: *Twitch (2021). Actualización sobre el incidente de seguridad de Twitch. Recuperado el 16 de abril de 2026. De Blog Twitch. Website: https://blog.twitch.tv/es-mx/2021/10/15/updates-on-the-twitch-security-incident/*

LA PARADOJA DE LA CONFIANZA Y LA CARGA FINANCIERA

Estos incidentes, junto con el reciente caso de la película animada de Paramount, demuestran que las políticas de seguridad basadas en la "confianza" tienen sesgos. Depender de que un empleado no cometerá un error tipográfico al enviar un correo, o confiar en que nadie caerá en una campaña de ingeniería social, es una trampa en el ecosistema digital de 2026. La implementación de la interconexión entre datos importantes y conexiones compartidas dentro de una infraestructura como reflejan muchos ejemplos históricos y de análisis, es sin duda una respuesta de que el modelo de la ¨conexión¨ para facilitar la comodidad no es un modelo funcional. No se puede determinar si la película al estar en un servidor de datos conectado a una misma red fue el vector, o un error humano, o bien un fallo en la cadena de custodia por filtración o facilitación de un empleado interno, mientras no exista una investigación formal la incertidumbre solo sirve para documentar las practicas que han marcado los fallos en estas situaciones.

Las filtraciones no solo cuestan el valor del activo robado (una película, una patente, una base de datos). Conllevan daños paralelos devastadores:

- **Pérdida de ventaja competitiva y sabotaje industrial.**
- **Extorsión directa** (como las amenazas de liberar los datos obtenidos o secuestrados).
- **Costos legales y multas regulatorias** por no proteger información de terceros en casos de datos críticos.
- **Destrucción de la confianza del consumidor y de los inversionistas.**

EL CASO RENAUT (REGISTRO NACIONAL DE USUARIOS DE TELEFONÍA MÓVIL) 2008-2011 LA CENTRALIZACIÓN COMO VECTOR DE RIESGO

El programa fue creado en 2008, su propósito era obligar a todos los ciudadanos a vincular su número de teléfono celular con su CURP (Clave Única de Registro de Población) para, en teoría, combatir los delitos de extorsión telefónica y secuestro. Sin embargo, el proyecto fue reportado por medios como un fracaso arquitectónico y de seguridad desde su concepción hasta su fin:

- **VULNERABILIDAD DE ENTRADA (INGENIERÍA SOCIAL INVERSA):** Al depender de un sistema de registro simplificado (enviar un SMS con la CURP), el sistema carecía de validación estricta. El resultado fue que casi dos millones de líneas fueron registradas con datos falsos. Hubo personas que, a modo de burla o encubrimiento, registraron sus teléfonos a nombre de figuras políticas, funcionarios y empresarios e incluso del propio presidente.

- **LA FILTRACIÓN MASIVA (EL ERROR ESTRUCTURAL):** Tal como recuerdas, la base de datos centralizada fue vulnerada rápidamente debido a la falta de aislamiento y políticas de cifrado robustas. La base de datos completa con millones de registros privados se filtró y terminó siendo vendida en el mercado negro (en foros de internet e incluso se reportó en algunos foros que podía ser adquirida en tianguis como el de Tepito) por cantidades irrisorias, llegando a costar apenas 500 pesos.

- **EL IMPACTO NEGATIVO:** En lugar de reducir el crimen, el RENAUT lo facilitó. Durante el periodo de vigencia del registro, los delitos de extorsión y secuestro repuntaron en un 40% y un 8%, respectivamente. La base de datos filtrada se convirtió en el directorio perfecto para actores maliciosos.

- **DESTRUCCIÓN TOTAL:** El desastre fue tan insostenible que en abril de 2011 el Senado aprobó la desaparición del registro, y en junio de 2012 se ordenó la destrucción definitiva de la base de datos, esto permitió el libre tránsito de las líneas telefónicas, tema que vuelve a resonar con la nueva reforma a las telecomunicaciones en México donde se pide a los usuarios registrar su línea telefónica con fecha hasta 30 de Junio de 2026 como plazo límite, impulsada por el Gobierno y la Comisión Reguladora de Telecomunicaciones (CRT). En 2021 se intentó implementar el **PANAUT (Padrón Nacional de Usuarios de Telefonía Móvil)** como parte de las reformas a la Ley Federal de Telecomunicaciones y Radiodifusión, en este caso se incluyen biométricos, aunque fue frenado por la Suprema Corte de Justicia de la Nación (SCJN) en 2022, declarándolo inconstitucional por representar un riesgo desproporcionado a la seguridad de los ciudadanos sin una garantía real de efectividad contra el crimen.

LA EFECTIVIDAD DE LO SIMPLE SOBRE LO SOFISTICADO

No siempre se trata de ataques de alta complejidad diseñados para romper los sistemas más seguros; irónicamente, se emplean prácticas más sencillas que resultan más efectivas contra los sistemas avanzados. Entre ellas destaca la **Ingeniería Social**, un método que ha tomado fuerza debido a que es más efectivo contra los usuarios, independientemente de su nivel de preparación o su puesto dentro de una organización.

COMPARTIMENTACIÓN Y CIFRADO INHERENTE

En Cruger Corp, nuestro análisis de estos vectores concluye en una doctrina inquebrantable: **No se puede parchear la naturaleza humana, pero se puede —y se debe— aislar la información de los errores humanos.**

Si asumimos que las credenciales serán robadas, que los correos electrónicos de *phishing* serán abiertos y que los servidores serán mal configurados, la única defensa lógica restante es el **cifrado estructural y la adopción estricta de una arquitectura de Confianza Cero (Zero Trust)**.

Un desastre corporativo de exfiltración de datos puede evitarse si la información es tratada como un activo hostil hasta que se demuestre lo contrario. Si un estudio de cine, un banco o una entidad gubernamental cifra sus archivos antes de su almacenamiento o envío, un error en la cadena de custodia pierde su letalidad. Si un atacante intercepta un correo electrónico enviado por error, o extrae datos mediante credenciales robadas por ingeniería social, el destinatario final solo recibe un bloque de datos inútil.

Las buenas prácticas de ciberseguridad y el cifrado robusto no son herramientas reactivas para los departamentos de TI; son estrategias fiduciarias para proteger la existencia misma de la empresa. La filtración reciente en la industria del cine es un recordatorio severo: el valor de tus datos no se mide por cuánto te costó crearlos, sino por cuánto te costará perderlos por no haberlos cifrado a tiempo.

CITAS Y REFERENCIAS:

ANMTV (12/04/2026). Avatar - La Leyenda de Aang: filtran un fragmento de la película. Recuperado el 12/04/2026. Website: https://www.anmtvla.com/2026/04/avatar-la-leyenda-de-aang-filtran-un.html

Avatar Wiki (12/04/2026). Acaban de filtrar escenas de la película animada del Avatar Aang. Recuperado el 12/04/2026. Website: https://www.facebook.com/avatarwikies/posts/acaban-de-filtrar-escenas-de-la-pel%C3%ADcula-animada-del-avatar-aang-esto-no-es-un-s/953374927049374/

Reportes de la Industria (12/04/2026). Filtración de Paramount: Usuario amenaza con filtrar película completa de Avatar Aang tras recibirla por error. Información en desarrollo en redes sociales y medios especializados.

TVAzteca Laguna (16/04/2026). 30 años de prisión para el que filtró la película de Avatar: The Last Airbender. Recuperado el 16 de Abril de 2026. Website: https://www.aztecalaguna.com/espectaculos/notas/filtracion-pelicula-avatar-30-anos-carcel/

Cruge, Angel (2026). DARK ZONE – METODOLOGÍA DE INTELIGENCIA VOLUMEN I VULNERABILIDADES SISTÉMICAS Y UN NUEVO PARADIGMA DE LA SOBERANÍA DIGITAL BASADA EN HARDWARE. Recuperado el 14 de Abril de 2026. De Cruger Corp / Zenodo. Website: https://zenodo.org/doi/10.5281/zenodo.18415821

Twitch (2021). Actualización sobre el incidente de seguridad de Twitch. Recuperado el 16 de abril de 2026. De Blog Twitch. Website: https://blog.twitch.tv/es-mx/2021/10/15/updates-on-the-twitch-security-incident/

Ramos, Rolando (2012). El fracaso del Renaut llevó a su desaparición. Recuperado el 16 de abril de 2026. De El Economista. Website: https://www.eleconomista.com.mx/politica/El-fracaso-del-Renaut-llevo-a-su-desaparicion--20120304-0049.html

RS MAZA (2010) Caso: El Registro Nacional de Usuarios de Telefonía Móvil. Recuperado el 15 de Abril de 2026. De Dialnet. Website: https://dialnet.unirioja.es/descarga/articulo/7679459.pdf

r3d Red en Defensa de los Derechos Digitales (2020). Legisladores buscan revivir el RENAUT con el Registro de Usuarios de Telefonía Móvil. Recuperado el 15 de Abril de 2026. De r3d Red en Defensa de los Derechos Digitales. Website: https://r3d.mx/2020/12/03/legisladores-buscan-revivir-el-renaut-con-el-registro-de-usuarios-de-telefonia-movil/

Muñoz, Ivonne (2009). Por fin… las reglas del RENAUT. Recuperado el 15 de Abril de 2026. De Blog Derecho Informático. Website: https://blog.derecho-informatico.org/2009/05/13/por-fin-las-reglas-del-renaut/

Suprema Corte de Justicia de la Nación (2021). Acción de Inconstitucionalidad 82/2021. Recuperado el 14 de Abril de 2026. De Suprema Corte de Justicia de la Nación. Website: https://www2.scjn.gob.mx/juridica/engroses/cerrados/Publico/Proyecto/AI82_2021y86_2021acumuladaPL.pdf

Gobierno de Mexico (2025). La CRT aprueba y emite los Lineamientos para la identificación de líneas telefónicas móviles. Recuperado el 14 de Abril de 2026. De Gobierno de Mexico. Website: https://www.gob.mx/crt/prensa/la-crt-aprueba-y-emite-los-lineamientos-para-la-identificacion-de-lineas-telefonicas-moviles

r3d Red en Defensa de los Derechos Digitales (2026). Inicia registro obligatorio de líneas telefónicas sin salvaguardas contra abusos. Recuperado el 14 de Abril de 2026. De r3d Red en Defensa de los Derechos. Website: https://r3d.mx/2026/01/12/inicia-registro-obligatorio-de-lineas-telefonicas-sin-salvaguardas-contra-abusos/

Grifaldo, Javier (2025). EL ESLABÓN MÁS DÉBIL: CÓMO EL ERROR HUMANO ORIGINA MÁS DEL 90% DE LOS CIBERATAQUES. Recuperado el 13 de Abril de 2026. De Revista Mundo Empresarial. Website: https://revistamundoempresarial.com/compliance-empresarial-2025-2/