Cuándo se puede realizar borrados de documentación electrónica asociada a un conflicto.

PARTE PRIMERA: EL EVENTO DESENCADENANTE.

Escrito por **Carlos Rozen** y **Martín Elizalde**

BDO

Carlos Rozen

Carlos Rozen es socio de BDO en Argentina y responsable para la Región de las prácticas de Compliance & Forensic Services.
Ha capacitado a más de 2000 responsables de compliance y ha contribuido en la creación de más de 50 áreas de compliance.
Fue socio fundador y Presidente de la AAEC Asociación Argentina de Ética y Compliance.
Dirige la CEC Certificación Internacional en Ética y Compliance (AAEC-Universidad del Cema – IFCA International Federation of Compliance Associations). Es profesor en temas de Compliance en 5 universidades de Argentina y 4 del exterior, incluyendo España. Especialista en tecnologías aplicadas a Compliance. Autor de 5 libros en temas de compliance e investigaciones.

Martín Elizalde

Abogado. Master in Law, LLM, Washington College of Law, American University, Washington D.C.
Certification de Kroll Ontrack , Minneapolis.
Profesor de Seguridad Informática en distintas universidades de la Región (Argentina, Colombia, Ecuador y Panamá). Socio Fundador de Foresenics.

Una ruta sin señales de tránsito

El Presidente Nixon se vió forzado por la justicia a hacer públicas 7000 grabaciones, presuntamente ilegales, pero borró 20 minutos - desde luego todo el mundo habló solamente de esos 20 minutos, antes que se viera forzado a renunciar[1]. Rebekah Brooks fue la más entusiasta: cuando avizoran problemas legales, la editora estrella ordenó borrar millones de correos electrónicos de los servidores del News International[2]; al hacerlo, borró su carrera. Sin embargo, en el caso Barcenas[3], el Juez no encontró delito en hacer pedazos discos rígidos (antes borrados) que contenían información que sería evidencia legal, cuando quien dio los martillazos ya podía razonablemente haberlo sabido. No todo está tan claro, parece.

---

1 Ver **"Las grabaciones secretas que se guardaban en un sótano de la Casa Blanca y desencadenaron el derrocaramiento de Nixon"**

2 Ver **"Rebekah Brooks 'ordered deletion of millions of News International emails"**

3 Ver **"Caso Barcenas"**

En la búsqueda

Entonces, la pregunta que nuestros clientes se hacen y más en estos días en nuestro país, es cuándo y cómo eliminar la información susceptible de ser considerada como evidencia en un juicio. Para poder dar algunas certezas, otra vez, mancomunadamente los autores, ayudaremos a definir el punto en que borrar documentación deja de ser un procedimiento de descarte de datos inútiles, para convertirse en una actividad delictiva. Y antes de empezar a hacerlo, nuevamente señalamos la importancia de un trabajo en equipo entre los sectores de tecnología, de legales, de compliance, y, de un total conocimiento de los hechos por parte del Directorio: la eventual responsabilidad en que se incurriría sería fácilmente extensible a esos jugadores.

El evento más esperado

El hecho que separa un borrado "inocente", cuyo objetivo es eliminar una sobreabundancia o duplicación de data electrónica y un intento consciente de deshacerse o hacer inalcanzable información electrónica antes que un juez la requiera, se llama "evento desencadenante", suena a diagnóstico médico temible; y no lo es. Un evento desencadenante es un indicador de la probabilidad de un conflicto, litigio o una investigación regulatoria[4].

Como casi poéticamente lo describe un autor: (que no es poeta) "considérese (al evento desencadenante) un momento crucial, cuando los vientos de los procedimientos legales empiezan a soplar, lo que indica la necesidad de afianzar las medidas de seguridad y salvaguardar la Información Almacenada Electrónicamente (ESI)"[5]. Más prosaicamente, a partir de su ocurrencia no se puede negar el conocimiento de esa probabilidad.

En términos de seguros, vendría a ser como el siniestro. Una vez que se conoce, hay que tomar una medida, en ese caso denunciarlo a la aseguradora, acá preservar la documentación. El deber de preservar los datos luego de reconocido el evento desencadenante es crítico. Si una parte no reconoce un evento desencadenante y no implementa medidas de preservación con la suficiente rapidez, se pueden perder o destruir pruebas documentales.

En realidad, es un deber doblemente conveniente: si el cliente es condenado, al menos no lo será por obstrucción y si no lo es, la evidencia en su favor lo va a ayudar - una cosa es que el cliente pierda un juicio y otra que sus integrantes sean condenados a título personal. Así que, a tomar nota.

---

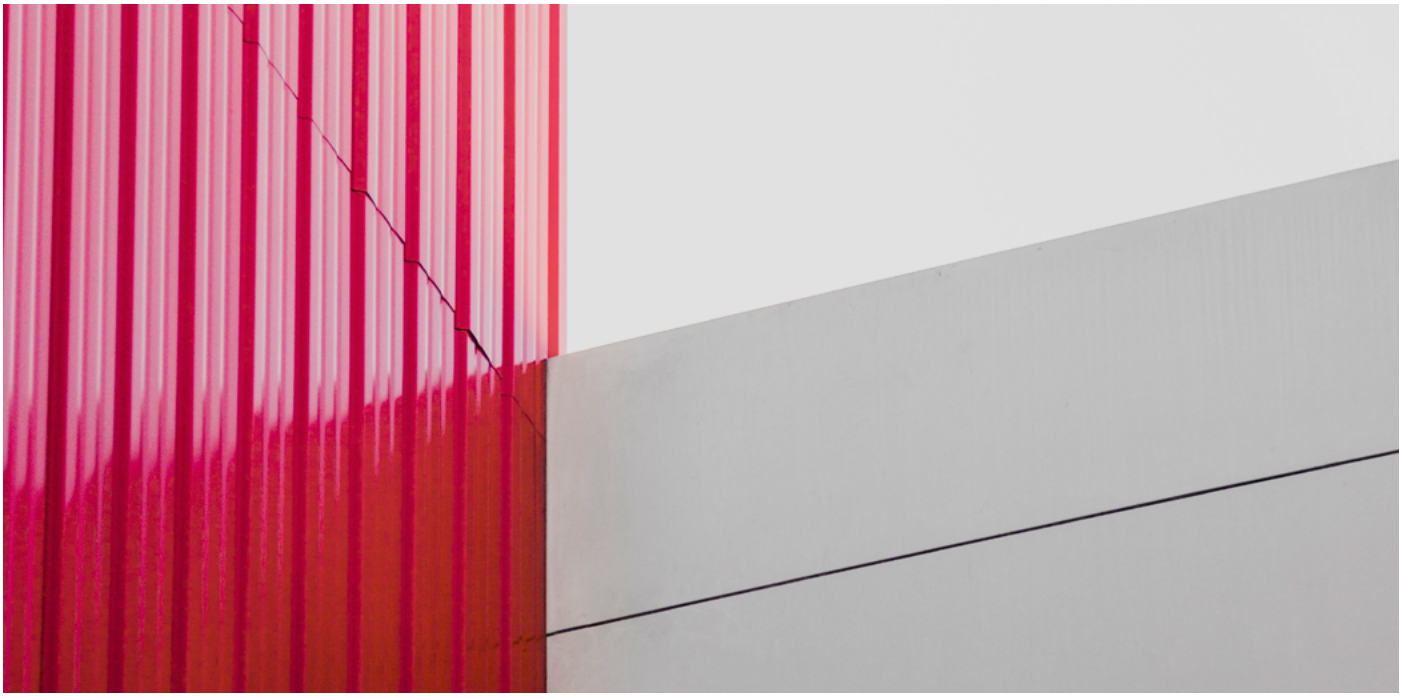
4 - 5 Ver **"What Is a Trigger Event?"**

Hay eventos para todos

Los eventos determinantes son internos o externos. Cuando un empleado deja la organización en malos términos, es razonable pensar en un reclamo judicial; cuando se acerca una auditoría interna de seguridad informática, de cumplimiento regulatorio o de cualquier otra naturaleza, o se perfile una denuncia en un canal de ética, estamos hablando de eventos internos. Los externos corresponden a las demandas judiciales, cartas documentos con reclamos económicos o notificaciones que sin serlas son suficientemente claras. Las redes sociales son parte importante y no se puede a esta altura ignorarlas por principio como canales de conocimiento - sobre todo cuando el cliente las frecuenta.

Cruzando la línea

El conocimiento del evento desencadenante altera cualquier programa de borrado rutinario que se implementara antes del mismo. No es creíble eso de "sólo apreté delete" si es que sabía que esa planilla, ese mensaje, correo electrónico o video, eran parte de la evidencia de un conflicto previsible. Cruzar la línea va a imponer una presunción en contra de la inocencia del cliente en este punto. ¿Cómo juega todo esto con la existencia de un plan o programa de borrado de información rutinario? Esa es otra de las preguntas favoritas de los clientes. Veamos, estos programas están diseñados y/o administrados por el área de IT. Forman parte de la documentación relativa al almacenamiento y control de la información electrónica. Describen las herramientas que se usarán, el modo y tiempos en que se ejecutará. También el protocolo a seguir. Así, si éste indica que el área de tecnología actuará con autonomía y resulta que la orden de borrar o disponer de la información viene de, digamos, Legales, estamos en problemas. Si los plazos de borrado se modifican o acortan luego de un evento desencadenante, aun cuando el protocolo se siga, estamos en problemas. Si la documentación se borró siguiendo un programa regular impartido por la casa central, sin que hubiera sido implementado aún por la sucursal local antes del evento desencadenante, estamos también en problemas. Y por último, no luce bien que usemos una nueva herramienta de borrado, licenciada después del evento desencadenante. Son estas algunas de las situaciones especiales que, sugerimos, sean consideraradas en su totalidad.



A veces si, a veces no

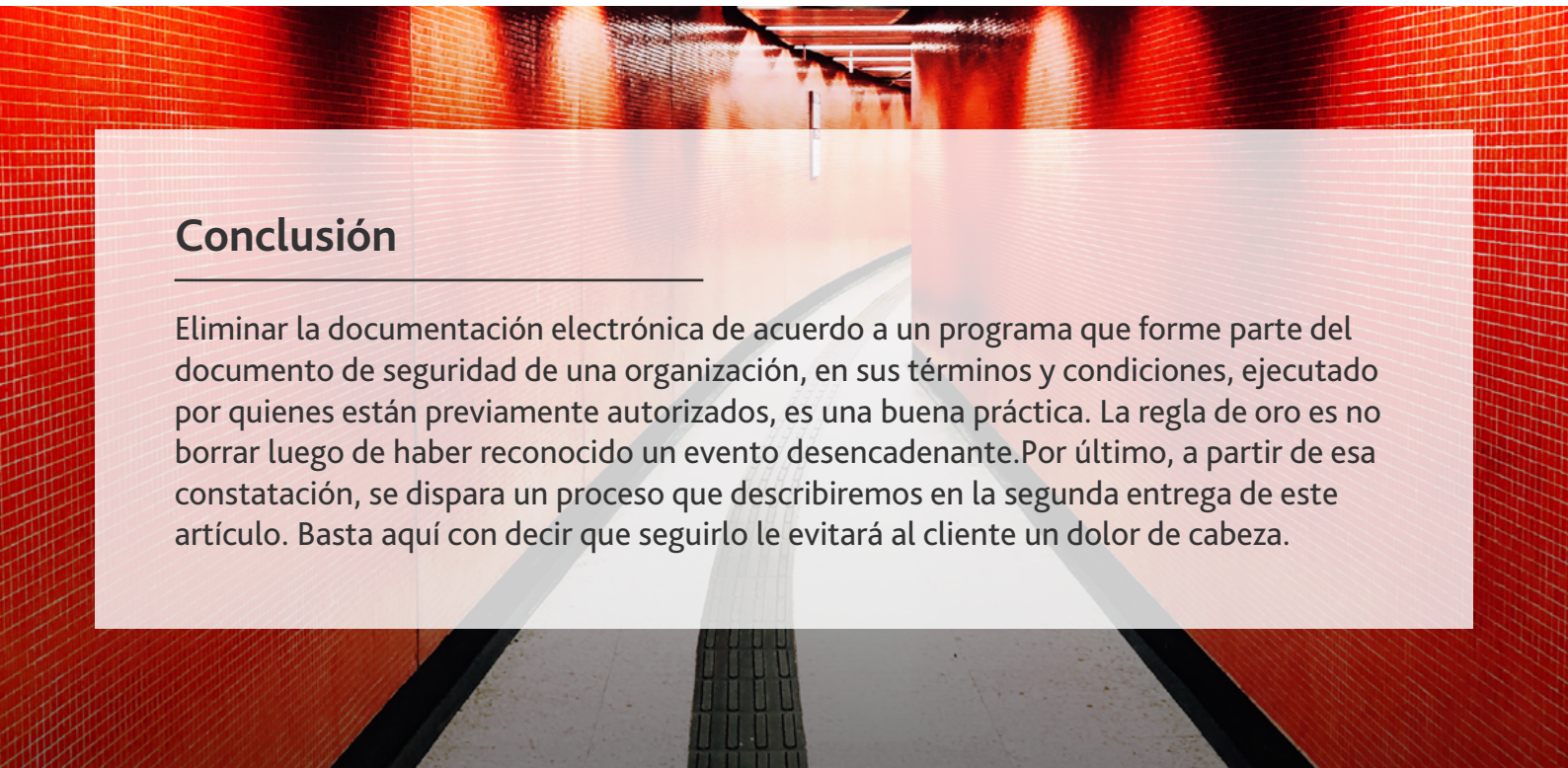
Por ejemplo, se va un gerente. ¿Debo conservar almacenada la información corporativa de su celular, GPS, laptop y demás ordenadores? Si su salida ha sido en buenos términos, consideramos que no sería lo más conveniente. Conservarla sería un riesgo a la protección de la privacidad de la información. ¿Qué ocurre en caso de ataque informático? Aun cuando este tema lo abordaremos en otro artículo (no se libraran de nosotros tan fácilmente) aquí se abre una delicada línea entre lo que hay que eliminar para proteger la información electrónica y los datos de terceros y la necesidad de conservar rastros electrónicos para investigar el ataque. ¿Y si el empleado perdió/le borraron su ordenador? Bueno, corra a borrar - nadie lo objetará.

En gráfico:

Borrado rutinario permitido (Según programa documentado)

Obligación de preservar (Prohibido borrar)

Evento desencadenante



Conclusión

Eliminar la documentación electrónica de acuerdo a un programa que forme parte del documento de seguridad de una organización, en sus términos y condiciones, ejecutado por quienes están previamente autorizados, es una buena práctica. La regla de oro es no borrar luego de haber reconocido un evento desencadenante.Por último, a partir de esa constatación, se dispara un proceso que describiremos en la segunda entrega de este artículo. Basta aquí con decir que seguirlo le evitará al cliente un dolor de cabeza.

Flujo de notificación y preservación de documentación electrónica

Evento desencadenante

↑

Detección por el área responsable (legal / compliance /auditoría)

↑

Notificación formal interna a custodios y TI

↑

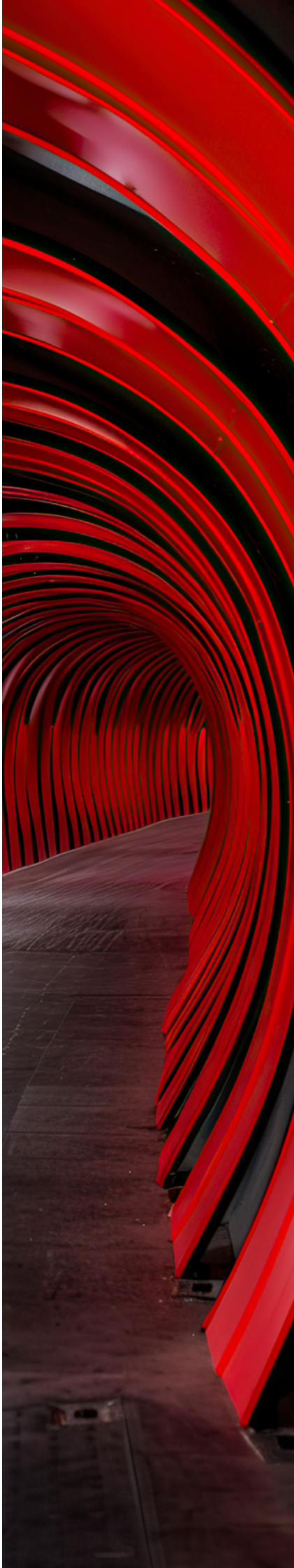
Obligación de preservar documentación electrónica

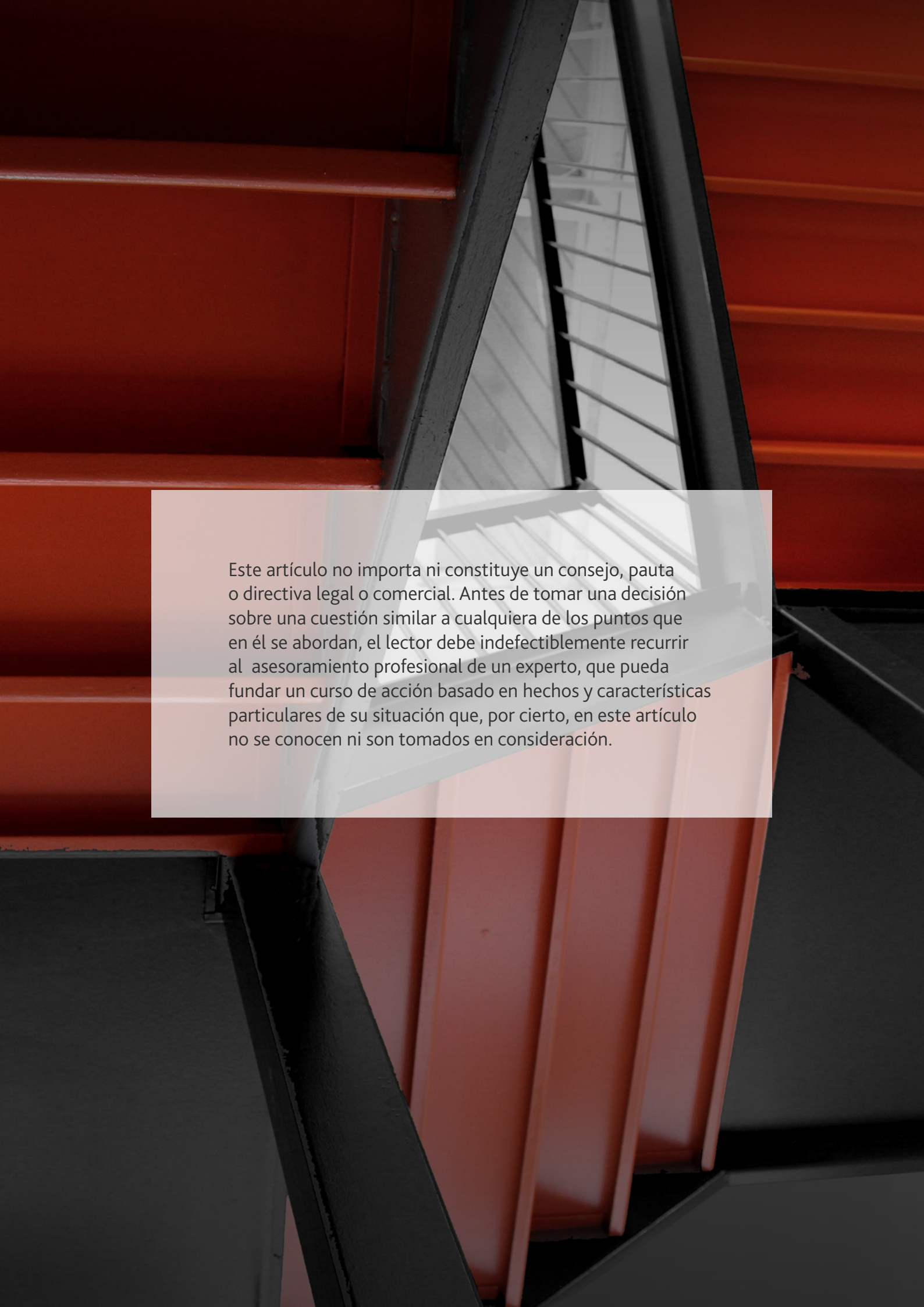
↑

Monitoreo y control del cumplimiento

↑

Cierre / levantamiento de la oblicación





Este artículo no importa ni constituye un consejo, pauta o directiva legal o comercial. Antes de tomar una decisión sobre una cuestión similar a cualquiera de los puntos que en él se abordan, el lector debe indefectiblemente recurrir al asesoramiento profesional de un experto, que pueda fundar un curso de acción basado en hechos y características particulares de su situación que, por cierto, en este artículo no se conocen ni son tomados en consideración.