

Investigaciones forenses en tiempo real

Las actividades de negocio cada vez se llevan a cabo con mayor **descentralización** y con mayor peso del **teletrabajo**. Sin embargo, las necesidades de activar una **investigación con todas las garantías y con validez forense** siguen siendo críticas para una defensa efectiva. Mediante nuestros sistemas de **investigación remota**, detectamos acciones sospechosas, preservamos las evidencias y actuamos de forma inmediata.

Vivimos una época de profundos cambios y transformaciones, tanto en lo relativo a la operativa de las organizaciones, como a los nuevos modelos de acceso a los recursos corporativos por parte de los empleados. Este nuevo paradigma ofrecerá grandes oportunidades para las empresas, pero a su vez genera importantes riesgos asociados a la distribución geográfica de los equipos y el acceso a información confidencial.

Para mantener un control efectivo sobre los activos de una compañía, asegurando una apropiada cobertura ante obligaciones regulatorias, es necesario evaluar si el enfoque actual es suficiente a la hora de gestionar estos desafíos.

Un **planteamiento proactivo** ante dichas amenazas permite a las organizaciones tomar decisiones estratégicas y tácticas, y adelantarse a cualquier acción legal que pudiera surgir. En definitiva, identificar hechos potencialmente problemáticos antes de que generen una crisis interna, supone una clara ventaja a la hora de investigar los mismos. Este enfoque permite proteger mejor a las organizaciones, a sus empleados y sus clientes, reduciendo costes innecesarios y asegurando un apropiado cumplimiento de las obligaciones de control y supervisión.

Principales retos

Falta de información sobre lo que está pasando en el día a día de una organización, línea de negocio o departamento: ¿Quién está accediendo a información confidencial?, ¿Cuándo?, ¿Con qué fin?, etc.

Supervisión insuficiente sobre posibles incumplimientos de políticas internas, accesos a sistemas o actividades irregulares por parte de empleados.

Medidas de control ineficaces en la situación actual, basadas en protocolos de prevención desactualizados y un enfoque reactivo.

Nuestro enfoque

Monitorización continua de la actividad relativa al teclado, aplicativos y archivos para identificar conductas irregulares.

Respuesta en tiempo real, aislando dispositivos y bloqueando acciones para evitar daños irreparables a la compañía.

Defensa legal efectiva, gracias a la preservación forense automática de las evidencias, garantizando una defensa más robusta.

Obtención de información granular, asegurando un proceso de toma de decisiones efectivo, realista y flexible.



Principales casos de uso



Monitorización de acceso a información confidencial

Alertas de empleados accediendo, en remoto o fuera del horario laboral, a los sistemas de la entidad con información confidencial. Posibilidad de analizar la frecuencia de accesos a cierta información y las horas a las que se producen de cara a impedir conductas irregulares e investigar cualquier actividad inusual.



Uso inapropiado de la información de clientes

Alertas sobre almacenamiento de información confidencial fuera de los sistemas autorizados; detección de incumplimientos de la política de protección de datos; entendimiento profundo de los hábitos generales de los usuarios que ayuden a definir políticas internas y a fomentar metodologías de trabajo adecuadas.



Uso no autorizado de dispositivos de almacenamiento externo

Monitorización de los dispositivos externos utilizados por los empleados en sus equipos, al objeto de supervisar e impedir la salida de datos sensibles de la organización.



Investigaciones internas

Vigilancia localizada en áreas funcionales de alto riesgo con preservación automática de evidencias antes de su posible destrucción, a raíz de la generación de las alertas de conductas irregulares definidas previamente o de denuncias internas recibidas; actuación proactiva ante posibles requerimientos regulatorios o judiciales.



Análisis del tráfico de correo entrante y saliente

Estableciendo reglas es posible diseñar detectores de contenido que identifiquen información sensible, así como dominios o terceros potencialmente sospechosos.



Mitigación del riesgo con terceras partes

Relación inusual o directamente prohibida con agentes comerciales o con compañías de la competencia podrá ser detectada antes de que constituya un riesgo de pérdida de negocio, o de sanción por relaciones que pudieran derivar en acciones contrarias al derecho de la competencia.



Propiedad Intelectual

Controles para mitigar el riesgo de copia de propiedad intelectual de la entidad, como pueden ser algoritmos o códigos propios. Generación y preservación de capturas de pantalla evidenciando los hechos.



eDiscovery

Ampliación de una investigación mediante búsquedas en otras fuentes de información relevantes para conseguir un mayor entendimiento de los hechos investigados; pudiendo presentar los hallazgos de las mismas en un informe pericial forense a aportar ante un eventual procedimiento judicial.



Nuevos riesgos derivados del teletrabajo

Un entorno con menor vigilancia física puede derivar en impresión de documentación confidencial, toma de capturas de pantalla de datos de clientes, uso indebido de servicios corporativos, así como otros indicios o evidencias de actividades irregulares.

Enfoque proactivo de investigaciones



Jorge Lledías

Socio

jlledias@deloitte.es

+34 91 514 52 00



Iván Ruiz

Director

iruizperez@deloitte.es

+34 91 443 23 02



Beatriz de la Higuera

Senior Manager - Discovery

bdelahiguera@deloitte.es

+34 91 822 93 46

Deloitte hace referencia, individual o conjuntamente, a Deloitte Touche Tohmatsu Limited ("DTTL") (private company limited by guarantee, de acuerdo con la legislación del Reino Unido), y a su red de firmas miembro y sus entidades asociadas. DTTL y cada una de sus firmas miembro son entidades con personalidad jurídica propia e independiente. DTTL (también denominada "Deloitte Global") no presta servicios a clientes. Consulte la página <http://www.deloitte.com/about> si desea obtener una descripción detallada de DTTL y sus firmas miembro.

Deloitte presta servicios de auditoría, consultoría, legal, asesoramiento financiero, gestión del riesgo, tributación y otros servicios relacionados, a clientes públicos y privados en un amplio número de sectores. Con una red de firmas miembro interconectadas a escala global que se extiende por más de 150 países y territorios, Deloitte aporta las mejores capacidades y un servicio de máxima calidad a sus clientes, ofreciéndoles la ayuda que necesitan para abordar los complejos desafíos a los que se enfrentan. Los más de 244.000 profesionales de Deloitte han asumido el compromiso de crear un verdadero impacto.

Esta publicación contiene exclusivamente información de carácter general, y ni Deloitte Touche Tohmatsu Limited, ni sus firmas miembro o entidades asociadas (conjuntamente, la "Red Deloitte"), pretenden, por medio de esta publicación, prestar un servicio o asesoramiento profesional. Antes de tomar cualquier decisión o adoptar cualquier medida que pueda afectar a su situación financiera o a su negocio, debe consultar con un asesor profesional cualificado. Ninguna entidad de la Red Deloitte será responsable de las pérdidas sufridas por cualquier persona que actúe basándose en esta publicación.