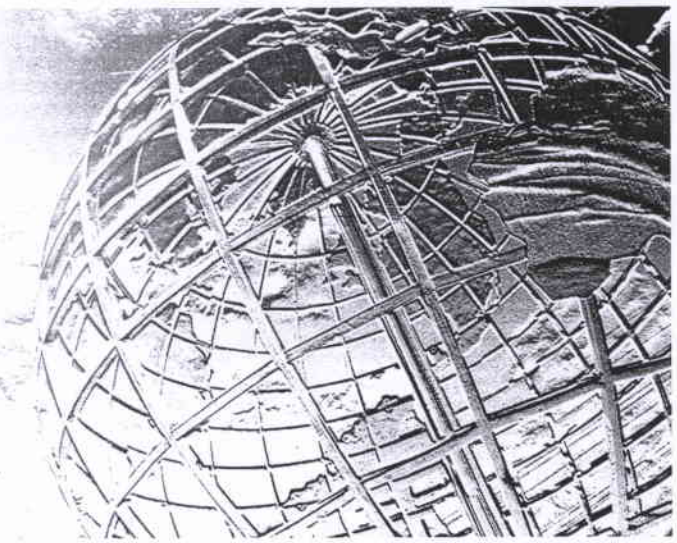
LMI facilita el cumplimiento normativo

Permite recuperar y gestionar la información de manera segura

En momentos de incertidumbre económica, como el que atravesamos en estos momentos, la conformidad legal y todas aquellas decisiones que permitan reducir los riesgos, se convierten en necesidades primordiales. LMI permite conocer toda la información de registros y gestionarla eficazmente para cumplir con las normas.



Nuria Cordón.-

El análisis efectivo de grandes volúmenes de información procedentes de diferentes fuentes supone un gran desafío para cualquier organización: cientos de gigabytes de datos cada día, diversidad de formatos o la presencia de registros falsos dificultan enormemente el análisis. Esta situación se hace más necesaria si se tiene en cuenta que las organizaciones deben cumplir con el marco normativo relacionado con la protección de los datos. En España, la LOPD (Ley Orgánica de Protección de Datos) exige guardar la información de acceso a los datos a cualquier organización, pero es importante tener en cuenta que dicha información no se genera únicamente en los sistemas de seguridad, sino también en ámbitos operacionales. Por ello, es necesario que las empresas puedan recuperar de manera rápida, segura y robusta esa información en el menor tiempo posible. Ante estos retos, LMI *(Log Management & Intelligence)* permite conocer toda la información de registros y gestionarlos de manera eficaz para cumplir con las normas.

> "Hemos avanzado en la gestión de la información, en la recolección de los 'logs', etc.",
>
> R. Gallego, dtor. gral. de security risk management de Entel

En España, la consultora Entel ha llegado a un acuerdo con LogLogic para implantar sus soluciones de seguridad, enmarcadas dentro de LMI. "En momentos de crisis –comenta Ramsés Gallego, director general de security risk management de Entel– la conformidad legal y todo lo que ayude a mitigar riesgos se vuelve sensible".

Cuatro fases

Para ello, esta aproximación a tecnología, como la definen desde Entel, está compuesta por cuatro fases básicas. La primera de ellas tiene que ver con la recolección y la indexación y permite recoger el 100% de los *logs* de cualquier fuente en el momento que se precise. Básicamente, un log es utilizado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.

En la segunda fase entran en juego las alertas, basadas en tecnología de aprendizaje, lo que permite resaltar el cumplimiento y las amenazas en segundos, a través de análisis en tiempo real. El almacenaje es el tercer paso en el que los directores de tecnología pueden decidir almacenar la información de forma segura, automatizada e inmutable. Por último, en la cuarta fase se pueden realizar hasta 13.000 informes personalizados en segundos con plantillas LOPD, SOX, PCI, COBIT, ITIL o ISO.

Según Gorka Sadowski, senior technical advisor de LogLogic EMEA, gracias a la alianza con Entel "ya hay empresas españolas que están implantando esta tecnología y cada vez serán más las que se sumen a esta nueva herramienta". En la actualidad, muchas soluciones de auditoría de seguridad se sitúan bajo la disciplina SIM *(Security Information Manager)* que se encarga de automatizar la gestión de eventos en los sistemas y dispositivos de seguridad y presentarlos en un cuadro de mandos. Sin embargo, de acuerdo con Gallego, con LMI "hemos avanzado en dicha gestión de la información, en la recolección de los *logs*, en el cuadro de mandos, etc., mejorando la inteligencia que se dota a la recogida de datos". "Algunas de estas tecnologías ya existían, pero en la disciplina de *Log Management* están desarrolladas e integradas para proporcionar un servicio inigualable para empresas grandes y medias", apunta Sadowski.

> Gracias a la alianza de Entel y Loglogic, empresas españolas ya están implantando LMI