ieee.es
Instituto Español de Estudios Estratégicos

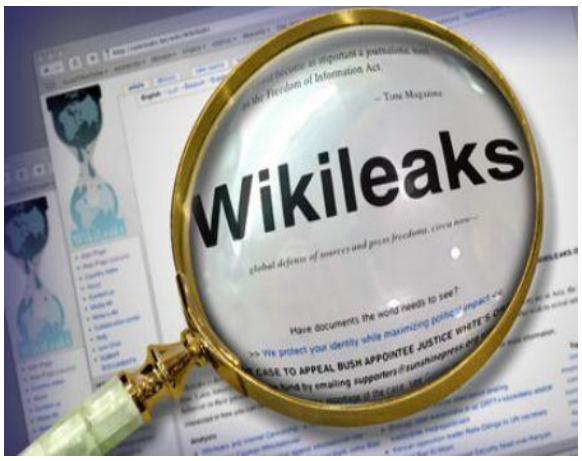
Documento de Opinión 28/2011

"De WikiLeaks a la "Data Loss Prevention": Un angosto desfiladero para la información corporativa"

Jesús Gómez Ruedas
Teniente Coronel ET

(Abril 2011)

Seguramente muy pocos lectores habrán podido escapar al efecto mediático de las noticias relacionadas con el "caso WikiLeaks"[1]. Como todos ustedes saben "www.WikiLeaks.org" es un dominio de internet, perteneciente a la categoría "portal de denuncias", que se ha convertido en claraboya digital, de ámbito mundial, de una organización de carácter internacional, sin ánimo de lucro y cuyos fundadores permanecen en el anonimato; publica informes anónimos y documentos reservados o clasificados, siempre preservando el anonimato de sus fuentes. En poco más de tres años la base de datos que alberga todos esos informes y documentos ha superado el millón de documentos.



Aunque esta organización se postula para el hospedaje de filtraciones que revelen comportamientos que se pudieran calificar de poco éticos por parte de gobiernos, especialmente los de tipo autoritario, de confesiones religiosas y de empresas de todo el mundo, la realidad es que, hasta la fecha, las reseñas más afamadas de WikiLeaks han venido germinando alrededor de la actividad de los Estados Unidos de América en materia de política exterior, muy especialmente en todo lo relacionado con las operaciones militares en Iraq y Afganistán.

WikiLeaks saltó a la fama en los primeros días de abril de 2010 al difundir un vídeo, hasta entonces clasificado, de una operación militar estadounidense en Bagdad contra supuestos insurgentes. De acuerdo a la denuncia de WikiLeaks, en el transcurso de este incidente habrían fallecido dos empleados de la agencia de noticias Reuters.

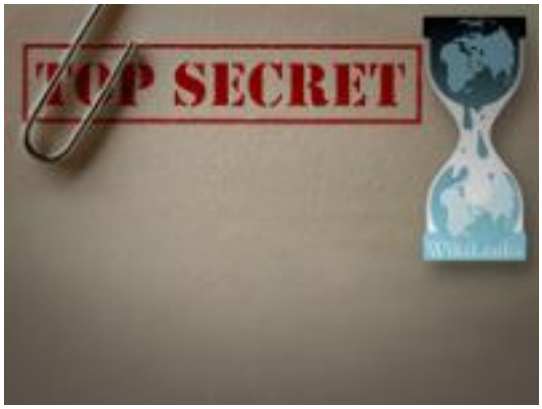
Dos meses después emergía la noticia del arresto del soldado norteamericano Bradley Manning: Según diversos medios de comunicación, este joven analista de inteligencia de las Fuerzas Armadas estadounidenses habría sido el autor de las filtraciones en favor de WikiLeaks. El 6 de julio de 2010 se informaba de los dos cargos contra el soldado Manning, fundamentados en diversas violaciones del Código de Justicia Militar; el primer cargo viene motivado por la presunta *"transmisión de información clasificada a su ordenador personal,*

[1] Wiki: Un wiki o una wiki (del hawaiano wiki, «rápido») es un sitio web cuyas páginas pueden ser editadas por múltiples voluntarios a través del navegador web. Los usuarios pueden crear, modificar o borrar un mismo texto que comparten. Los textos o «páginas wiki» tienen títulos únicos.

así como la instalación de software no autorizado en un sistema de información clasificado"; el segundo cargo responde a la supuesta *"distribución a fuentes no autorizadas de información concerniente a la defensa nacional, la divulgación de información clasificada relativa a la defensa nacional, existiendo fundamentos para considerar tales hechos lesivos para los Estados Unidos, y, finalmente, la modificación no autorizada de los privilegios de acceso al sistema informático para obtener información clasificada de este país".*

1. WIKILEAKS NO ES MÁS QUE UN SÍNTOMA

Pero no trata este artículo de analizar el fenómeno WikiLeaks, ni de valorar la conducta o el proceder de su popular responsable, el australiano Julian Assange. Más allá del caso particular, WikiLeaks constituye una muestra ejemplar de las amenazas y las vulnerabilidades que diariamente afrontan organizaciones públicas y privadas, de todo el mundo. **La esencia de este mediático asunto es que las medidas de protección de la información han fallado**.



Alarmas como la que ha encendido WikiLeaks se disparan cada día en cualquier rincón del mundo desarrollado donde la información constituye un activo de interés para sus instituciones. Por ejemplo, en el año 2009 el fabricante de productos de Seguridad *Symantec* y el "*Ponemon Institute LLC"* americano publicaban los resultados del estudio: "Riesgo de fuga de datos durante procesos de reducción de personal"; éstas eran algunas de las conclusiones de dicho informe:

- El 59% de los antiguos empleados reconocieron haber robado información confidencial de la compañía para la que habían estado trabajando anteriormente.
- El 61% de aquellos que admitieron haber sustraído información, manifestaron una opinión desfavorable acerca de su antiguo empleador.
- Como medios de extracción de la información corporativa, el 53% de los encuestados reconoció haber descargado datos en un CD[2] o un DVD[3], el 42% por medio de una unidad USB[4] y el 38% mediante el envío de correos electrónicos a sus cuentas personales.
- Finalmente, 24 de los 1000 encuestados, que habían sido despedidos a lo largo de 2008, continuaban teniendo acceso a los sistemas de información de sus antiguas compañías en enero de 2009.

Más próximo en el tiempo, en diciembre de 2010, la agencia espacial NASA[5] revelaba que dentro de su programa de reciclado de equipamiento informático había vendido 10 ordenadores sin haber eliminado previamente los datos, catalogados como información sensible, almacenados en los mismos. Datos relativos al programa del transbordador espacial y a las aplicaciones y controles internos de la intranet de la propia NASA estuvieron a punto de pasar a los circuitos comerciales de equipamiento hardware de segunda mano. La Agencia

[2] CD: Disco Compacto (Compact Disc)
[3] DVD: Disco Versátil Digital (Digital Versatile Disc)
[4] Memoria USB (Universal Serial Bus): Dispositivo de almacenamiento masivo que utiliza memoria de la denominada "tecnología flash" para guardar información.
[5] NASA: Agencia Nacional del Espacio y la Aeronáutica (National Aeronautics and Space Administration)

achacaba el fallo de seguridad a una cadena de errores humanos y a la falta de coordinación interna en un organismo de tan grandes dimensiones. Al parecer, algunos centros de la NASA, antes de la venta de un ordenador, retiraban los discos duros para proceder a su inutilización, mientras que otros centros utilizaban un software no corporativo para limpieza de datos, al tiempo que tampoco empleaban procedimientos de verificación del borrado de los datos: ¡Todo un reclamo para aquellos gobiernos u organizaciones tradicionalmente hostiles al gigante americano!

Si se buscan referentes en otros ámbitos de las corporaciones del mundo desarrollado, se puede constatar que, en los últimos años, como consecuencia de los variados escándalos, generalmente financieros, suscitados por episodios de fraudes multimillonarios, el marco legal y regulatorio que rige el entorno de las comunidades afectadas ha venido promoviendo mecanismos orientados a garantizar la medición, la contabilidad, el control, la monitorización, el almacenamiento de registros… de cualquier tipo de activo corporativo, especialmente si tiene dimensiones monetarias. En cambio, cuando se habla del activo "información corporativa" esa actitud proactiva y esa necesidad de control se tornan más laxas. Incluso resulta fácil asimilar que, por ejemplo, la publicación del balance trimestral de Disney constituya materia reservada y manejada como secreto empresarial hasta los últimos segundos del día D-1, de modo que nadie obtenga rédito alguno del conocimiento prematuro de esa información; pero, en cambio, si esa información se relaciona con una organización pública, no son pocos los defensores del derecho a la publicidad de todas las actuaciones de las Administraciones Públicas. Esta percepción podría tener alguna de sus raíces en los usos y costumbres de las generaciones más jóvenes y en su percepción del rol de la tecnología como un elemento connatural y dinámico de su entorno de vida.

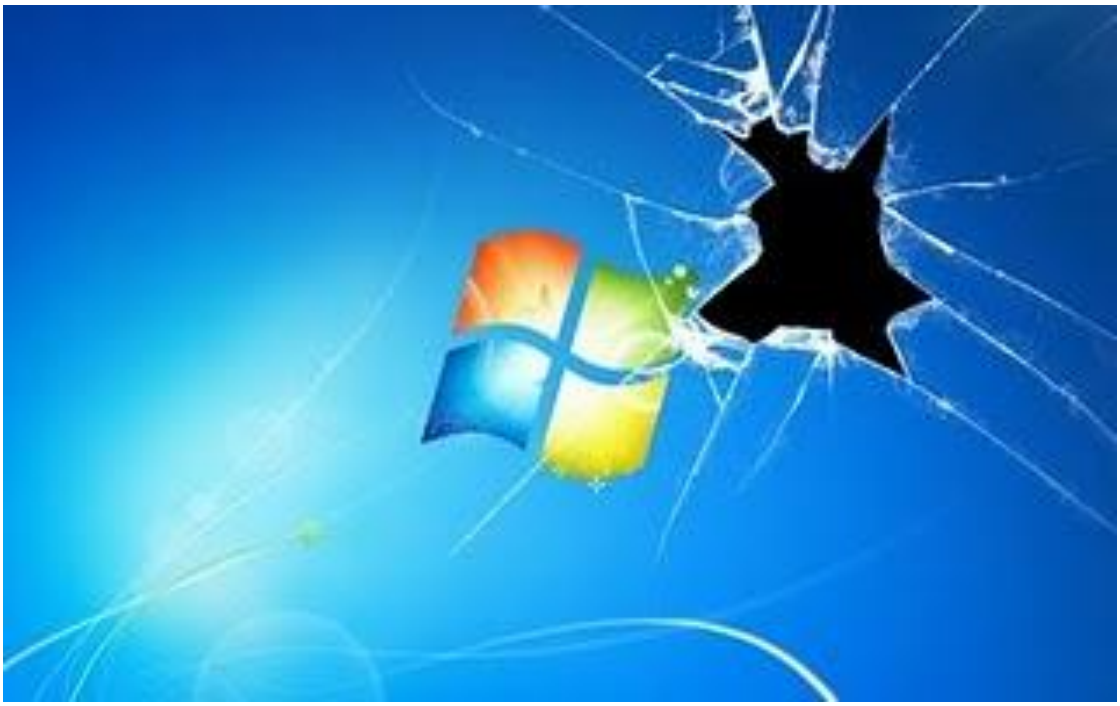
2. LA NUEVA SOCIEDAD DIGITAL

El escritor americano Marc Prensky acuñó en el año 2004 el término "nativos digitales" para referirse a las nuevas generaciones que no han conocido otro entorno que aquel en el que internet, los teléfonos móviles y, en general, los dispositivos informáticos han venido siendo elementos consustanciales. El propio sesgo dinámico y comercial de la sociedad occidental ha constituido el caldo de cultivo para todo tipo de cambios en los modos de comunicación, en las reglas de mercado, en la publicidad o en los negocios que pudieran satisfacer a estas jóvenes generaciones de "nativos digitales": Por ejemplo, Internet ya no es una mera herramienta de búsqueda de información, sino que, progresivamente, se ha venido convirtiendo en un lugar de encuentro donde compartir e intercambiar información, ya sea de carácter personal, profesional o socio-cultural. La naturaleza transnacional y global de las modernas autopistas de la información convierte en una quimera la capacidad de una única nación para gestionar de forma autónoma, sin la colaboración de otras, sus incidentes de seguridad de la información. El individuo pasa de un rol pasivo a uno mucho más activo de generador de contenidos. En consecuencia, se refuerza la interacción social y la web 2.0 se transforma en una herramienta de "inteligencia colectiva".

Definitivamente, las Tecnologías de la Información han desencadenado una nueva "revolución industrial" con repercusiones en todos los ámbitos de la realidad humana: la prensa digital le gana terreno a la tradicional prensa escrita; el sujeto se torna más participativo y ofrece una mayor sensibilidad individual por todo lo que ocurre en "su mundo"; los canales y los formatos de información son variados (blog, SMS[6], chat, telefonía móvil, mensajería instantánea, contenidos multimedia, …) y, frecuentemente, muestran una idiosincrasia más atraída por la inmediatez que por el análisis profundo y sosegado; muchos representantes de esta nueva sociedad sienten algún nivel de rechazo hacia modelos de negocio no alineados con este modelo de conducta; todo ello, en definitiva, dibuja un escenario con importantes dosis de consumismo, incertidumbre legal y oportunismo.

En consecuencia, las organizaciones, ya sean públicas o privadas, deben asimilar este profundo cambio socio-cultural, revisar sus pautas de actuación y modular sus mensajes para inculcar en los miembros de esta nueva sociedad los beneficios de un manejo adecuado, razonable y responsable de la información, así como la necesidad de protegerla; deberán, para ello, ofrecer algún tipo de garantía de su buen hacer en tal responsabilidad, de modo que, a semejanza de lo que se hace en otras áreas de responsabilidad corporativa, los controles internos que se desplieguen para el manejo de la información sirvan para prevenir, mitigar o corregir la eventual aparición de abusos o de cualquier tipo de actuación irregular.

Para responder a este desafío, la **innovación** se ha convertido en elemento clave para el progreso de las naciones y, por tanto, sus organizaciones, públicas o privadas, deben posicionarse en esta nueva Economía del Conocimiento. Ubicar al ciudadano como epicentro de la actuación de las administraciones públicas no debería confundirse con la disminución de la importancia crítica de la información de esas organizaciones, ni, por supuesto, con una pretendida transparencia absoluta de la misma.



[6] SMS: Servicio de Mensajes Cortos (Short Message Service)

3. LA GESTIÓN DE LA INFORMACIÓN RESERVADA

Parece evidente que los tradicionales mecanismos y procedimientos de gestión de la información especialmente protegida deben ser revisados para, sacando partido de sus principios y bondades intrínsecas, adaptarse a la nueva realidad socio-cultural y a los nuevos riesgos. Atrás deben quedar obsoletos modelos de gestión basados en estructuras rígidas.

Evidentemente, el primer proceso del ciclo de gestión es el irrenunciable análisis de riesgo. De su estudio se determinan en cada caso las necesidades de proteger la confidencialidad, la integridad y la disponibilidad de la información. Ello permite huir de posiciones excesivamente proteccionistas que derivan en una costosa e ineficiente sobreclasificación de la información corporativa así como, en el otro extremo, de posturas seducidas por criterios de generalización y de uniformidad. Por ejemplo, probablemente, no merezcan el mismo nivel de protección los contenidos del Boletín Oficial del Ministerio de Defensa o del Ministerio del Interior relativos a sus activos humanos que sus equivalentes del Ministerio de Fomento. Los riesgos parecen diferentes, luego el tratamiento de la información podrá ser diferente.

Tras el anterior proceso, el siguiente, y transcendental, implica la categorización del nivel de la información de acuerdo a la Política de Seguridad de la Información de la organización. Esta crucial tarea, tradicionalmente asociada a los entornos militares, constituye el principal hándicap para muchas entidades, generalmente como consecuencia de la ausencia de una tradición y una cultura de clasificación de la información, así como debido a la complejidad asociada al lanzamiento de una iniciativa de estas características en organizaciones cuyas bases de datos y repositorios ya guardan importantes volúmenes de información precedente; información que también deberá ser objeto de revisión y de integración en el correspondiente ciclo de gestión de documentos e informes a clasificar, desclasificar, difundir, destruir, etc.

Pero resulta igualmente innegable que sin estrictos controles de confianza para garantizar, hasta cierto punto, que las personas que manejan la información no la emplearán de forma hostil contra su propia organización, la seguridad de la información es una quimera. Sin necesidad de mayor análisis, un par de datos atestiguan esta evidencia: La tradicional vinculación entre el hombre y el eslabón más débil de la cadena de la seguridad de la información y los indicadores que refleja, como una muestra de lo anterior, el reseñado informe de *Symantec* y el "*Ponemon Institute LLC"* americano.

El ciclo continúa con la definición e implantación de unas medidas técnicas y organizativas que deben estar alineadas con la Política de Seguridad de la Información de la organización, sin olvidar las imprescindibles actividades de formación y de concienciación de todos los usuarios y destinatarios de dicha política. Finalmente, antes del reinicio del ciclo, es la hora de la tecnología. ¿Cómo deben coadyuvar las Tecnologías de la Información? Deben ser el instrumento para la detección de información incorrectamente clasificada e impedir las fugas de información.

4. LAS TECNOLOGÍAS DE LA INFORMACIÓN (TI), CERRADURAS DE LAS FUGAS DE INFORMACIÓN (DLP[7], DRM[8], IRM[9], …)

A la hora de valorar la aportación de las TI al reto de la protección de la información corporativa, el propio "caso WikiLeaks" ofrece algunos indicios que ayudan a bosquejar los escenarios habituales de fuga de información:

Para empezar, hay que evitar que todos los usuarios de un sistema de información tengan los mismos privilegios sobre dicha información. Si el analista Manning podía extraer información de la red SIPRNET (Secret Internet Protocol Router Network) en las mismas condiciones que el Secretario de Estado de Defensa, cabe inferir que algo no se había planificado, diseñado o implantado adecuadamente. Es decir, las responsabilidades inherentes a los diferentes usuarios y roles deben tener su reflejo en los privilegios de acceso al sistema de información. Naturalmente, no resulta sencillo articular y armonizar dentro de un sistema de información los diferentes intereses y las variadas necesidades de sus usuarios operativos. Pero si es importante la necesaria granularidad en el acceso a la información por parte de usuarios con diferentes responsabilidades, más importancia adquiere la ausencia de un mecanismo de detección de la extracción sin autorización de informes y documentos.

No son estos los únicos paisajes de pérdida de información. En una sociedad abarrotada de dispositivos de tratamiento de información cada día más reducidos y potentes, el robo o la pérdida de dichos dispositivos portátiles suponen una importante amenaza, especialmente cuando, en un entorno corporativo, dichos dispositivos no están gestionados por la organización. Igualmente complejo resulta el control de los dispositivos externos de almacenamiento de reducido tamaño y amplia capacidad, como las memorias USB y los discos digitales de variados formatos. Análogamente relevante se presenta la fuga de información a través de los medios de comunicación normalizados en la institución, como puedan ser el correo electrónico, la mensajería interpersonal o la navegación web. No termina aquí la variada casuística, puesto que también conviene recordar los casos de cesión de información a favor de colaboradores externos de la organización en un contexto de falta de control sobre el uso que hacen de ella. Aún así, siempre quedarán lagunas imposibles de cubrir tanto por medios técnicos como procedimentales: el copiado manual de datos, las fotografías del contenido del monitor o, incluso, la información que las personas retienen en su memoria y que podrían utilizar en contra de los intereses corporativos; para estos supuestos solo los mecanismos de valoración de la confiabilidad de los empleados pueden ofrecer cierto nivel de garantía.

Frente a todos estos potenciales escenarios de fuga de información que se dibujan en el marco de organizaciones con multiplicidad de sedes, cuyos empleados requieren de acceso a la

[7] DLP: Prevención de Fugas de Información (Data Loss Prevention).
[8] DRM: Gestión de Derechos Digitales (Digital Rights Management).
[9] IRM: Gestión de Derechos de la Información (Information Rights Management).

información desde el exterior de dichas sedes y con necesidades de compartir información con entidades colaboradoras, las TI ofrecen diversas respuestas de carácter complementario:

- Existen soluciones, basadas en técnicas criptográficas, que permiten el cifrado de la información, ya sea de los propios documentos o ficheros, como del soporte físico de almacenamiento del dispositivo (su disco duro). Siglas como EPP (EndPoint Protection), MDP (Mobile Data Protection) o EDRM (Enterprise Digital Rights Management) se asocian a estas técnicas.
- Otras, en cambio, se orientan a la inspección y el análisis del contexto de la información, poniendo la lupa tanto en los propios metadatos[10], en los archivos, en las bases de datos o en el tráfico de red. Ésta es la aproximación de las herramientas DLP (Data Loss Prevention), DAM (Database Activity Monitoring) o FD (Fraud Detection).

En definitiva, en lo que se refiere a toda aquella información que no sea de difusión pública y que, por tanto, requiera de algún grado de protección, todas estas soluciones tecnológicas deben constituir instrumentos para **evolucionar de un paradigma de seguridad fundamentada en el aislamiento y la fortificación a** uno nuevo que complementa ese enfoque con el valor añadido de **la Seguridad por Contenidos**, acorde con las prácticas actuales de trabajo, en el que cada actor interesado en el manejo de información debe estar dotado de unas autorizaciones específicas para el acceso a la misma.

En cada caso, las tecnologías aplicables dependerán del entorno de tratamiento de la información: los documentos estructurados o preformateados por un sistema de información concreto precisarán de diferentes técnicas a los documentos no estructurados procedentes, por ejemplo, de herramientas ofimáticas. Los diferentes soportes del ciclo de almacenamiento de la información también condicionarán extraordinariamente las soluciones a emplear: no se protege igual la información almacenada exclusivamente en una base de datos centralizada a nivel corporativo que aquella otra que pasa por diferentes estados desde la agenda personal del empleado hasta consolidarse en los sistemas TI centrales de la organización.

Así, a la hora de proteger documentos no estructurados, las **soluciones EDRM (Enterprise Digital Rights Management)** ofrecerán un buen nivel de protección. Estas tecnologías están orientadas a la protección de aquella información que precisa abandonar las dependencias de la organización. Por lo tanto, su campo de acción son los correos electrónicos y, en general, documentos ofimáticos. Posibilitan mantener el control sobre quien accede al documento e, incluso, a qué partes del mismo; definir qué acciones son permitidas (copiar, pegar, editar, imprimir, …); señalar cuando se puede acceder a la información; establecer un control de acceso basado en usuarios o grupos de usuarios; monitorizar las acciones que se realicen sobre el fichero; o, también, bloquear el acceso a la información en cualquier momento, conforme a la política implantada. Para todo ello se utilizan "marcas de agua"[11] que permiten registrar tanto al originador de la información como a los sucesivos participantes en la cadena de distribución.

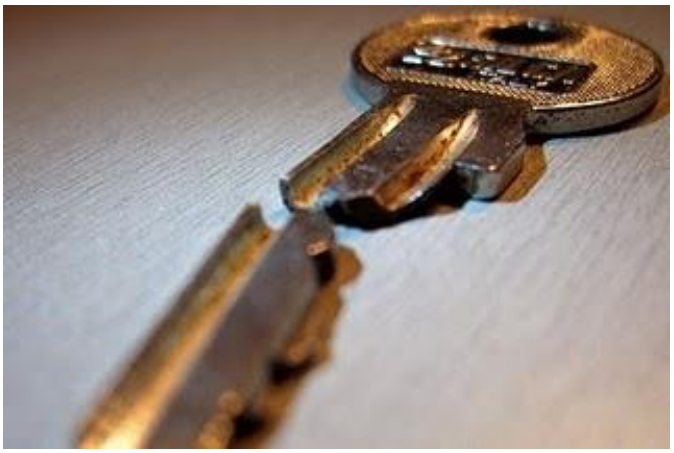
[10] Metadatos: Son datos sobre los datos. Al describir a otros datos, ayudan a clarificar o encontrar datos. El metadato puede ser tener formato texto, voz o imagen.

[11] Marca de agua digital: Técnica de ocultación de información que consiste en insertar un mensaje, oculto o visible, en el interior de un documento digital. Su objetivo principal es poner de manifiesto el uso ilícito del documento por parte de un usuario no autorizado.

Otra aproximación y otras funcionalidades, complementarias de las EDRM, ofrecen las **tecnologías DLP (Data Loss Prevention),** orientadas a la monitorización de fugas y, en particular, a través de documentos no estructurados o preformateados. Su ámbito se establece en los medios y canales de comunicación controlados por la organización, tanto si la información está en uso (mediante agentes de servidores y de estaciones de usuario), en movimiento (gracias a sensores en la red corporativa) o depositada (agentes en sistemas de almacenamiento). Entre sus características se cuentan la inspección y descubrimiento de información sensible en base a diversos atributos relativos al emisor de la información, contenedor de destino, horarios, palabras clave, expresiones regulares o huellas digitales[12] insertas en los ficheros; la capacidad de búsquedas de coincidencias exactas o de realización de análisis estadísticos; pueden monitorizar diversos tipos de protocolos de comunicación (navegación web, correo electrónico, descargas FTP[13],…); disponen de la posibilidad de bloquear o poner en cuarentena aquella información que levante algún indicio de sospecha; cuentan con aplicaciones gráficas para tareas de gestión centralizada.

La estrategia defensiva de este nuevo paradigma de la Seguridad por Contenidos se complementa con **herramientas MDP (Mobile Data Protection)**, para el cifrado de cualquier soporte físico de almacenamiento corporativo, ya sean servidores o estaciones de trabajo, y mitigar así el eventual robo de dispositivos; tras el inicio de la sesión, los usuarios operan sus terminales de forma transparente, manejando todos sus datos cifrados.

Otro elemento fundamental son las **soluciones DAM (Database Activity Monitoring)**, una tecnología específica de seguridad para bases de datos que permite analizar y monitorizar la actividad que se produce en cada servidor de bases de datos, operando autónomamente respecto al Sistema Gestor de la Base de Datos y alertando sobre comportamientos malintencionados, en tiempo real y de forma permanente. Este tipo de herramientas viene siendo utilizadas por empresas de todo el mundo que se hallan sometidas a diversos marcos de control de tipo sectorial: la *Payment Card Industry Data Security Standard* (PCI DSS), del ámbito de las tarjetas de pago; la norteamericana *Health Insurance Portability and Accountability Act* (HIPAA), para Seguros de Salud; o las *Sarbanes-Oxley Act* (SOX) para las empresas que cotizan en bolsa, también en Estados Unidos de América.



[12] Huella digital: Técnica utilizada para introducir en un archivo digital una marca que contiene información sobre los derechos de autor y sobre los usuarios que pueden utilizar ese archivo.
[13] FTP: Protocolo de Transferencia de Ficheros (File Transfer Protocol).

Finalmente, las **técnicas FD (Fraud Detection)** responden a una necesidad de muchas corporaciones, especialmente en los ámbitos financieros, de seguros o de operadores de comunicaciones, que vienen sufriendo cada año pérdidas millonarias. Las técnicas estadísticas y la minería de datos[14] ayudan a anticipar y detectar el fraude, permitiendo la adopción inmediata de medidas. Mediante el uso de sofisticadas herramientas se analizan miles de transacciones que permiten detectar patrones habituales de comportamiento y, en consecuencia, descubrir las transacciones fraudulentas que se apartan de dichos patrones. Estas mismas técnicas son las que se usan para la detección de anomalías e intrusiones en el marco de la gestión de la información corporativa.

Naturalmente, todas estas tecnologías requieren de detallados planes de implantación que deben ir acompañados de meditadas políticas de seguridad alineadas con la misión de la organización y la trascendencia de su información.

5. LECCIONES IDENTIFICADAS

Las corporaciones, públicas o privadas, de forma coherente con su naturaleza y objetivos, deben revisar sus modelos de negocio y **adaptarlos a la nueva realidad estructurada por estas flamantes Sociedad y Economía del Conocimiento**; ello les llevará al conocimiento y percepción de los riesgos inherentes a las mismas y, en consecuencia, a protegerse de ellos. Corolario de todo ello es que **la innovación se ha convertido en elemento clave** para el progreso de las organizaciones y de las naciones.

Tales vientos de innovación deben tener su reflejo en la actualización de los mecanismos de protección de la información corporativa. No resulta aceptable poner en peligro la existencia de la propia organización, o la integridad de sus miembros, por mor de vetustos e ineficaces modelos de gestión de la información reservada. **Las Tecnologías de la Información** ofrecen hoy día un amplio abanico de capacidades para **proveer unos altos niveles de garantía de protección de la información corporativa**. Lógicamente, antes del despliegue de las soluciones tecnológicas, cualquier organización, incluido un Ministerio o un Departamento de Defensa, debe **revisar, simplificar y consolidar su modelo de negocio para la gestión de la información**, alineando e integrando las visiones y necesidades particulares de tipo operativo de cualquier organismo interno; si las políticas de seguridad no se aplican de manera uniforme por todas las entidades internas (como parece que sucedió en la red SIPRNET norteamericana), la fuga de información será un evento seguro y solo restará conocer las consecuencias de la misma. La aplicación de las TI a la protección de la información corporativa implica un requisito fundamental: **La seguridad debe ser transparente para el usuario y para la información reservada**.

Jesús Gómez Ruedas [15]
Teniente Coronel del Ejército de Tierra
Diplomado en Informática Militar
Subdirección General de Tecnologías de la Información y Comunicaciones

[14] Minería de datos: Es la práctica de buscar y explorar en grandes almacenes de datos, dando por resultado el descubrimiento de patrones significativos y reglas. Para hacer esto, la minería de datos utiliza técnicas estadísticas, de automatización de conocimientos y de reconocimiento de patrones.

[15] Las ideas contenidas en los Documentos de Opinión son de responsabilidad de sus autores, sin que reflejen, necesariamente, el pensamiento del IEEE o del Ministerio de Defensa.