# Administrando la confidencialidad de la información

Jeimy J. Cano, Ph.D, CFE

*Algunas consideraciones sobre el saneamiento de medios de almacenamiento.*

La información como activo base de las organizaciones modernas es fuente de ventaja competitiva y generación de nuevas oportunidades de negocio. En este sentido, una adecuada clasificación de la información, asociada con una comprensión de la inseguridad en los procesos de negocio, así como procedimientos concretos para la disposición de los medios de almacenamiento, establecen características y condiciones de sistemas de gestión de seguridad informática que han entendido que la protección de la información va más allá de los elementos tecnológicos y de procedimiento, pues saben que la seguridad no es posible sin el entendimiento de las circunstancias que propone la inseguridad de la información.

La inseguridad de la información es parte inherente de la dinámica de las organizaciones modernas. Un reciente estudio disponible en la página web de attrition.org demuestra que durante 2006 y lo corrido del 2007 (http://attrition.org/dataloss/) la pérdida de datos y exposición de los mismos por la pérdida de portátiles, dispositivos USB y demás formas de almacenamiento portátil ha sido una importante constante. Alrededor de 343 casos documentados (en 2006) de universidades, empresas públicas o privadas nos muestran que a pesar de los múltiples esfuerzos de las organizaciones por mantener su información "segura", la inseguridad aumenta su capacidad de acción.

Frente a este panorama que reta a los profesionales de la seguridad informática, a los proveedores de soluciones de seguridad, a las prácticas de seguridad informática en las organizaciones, se abren diversos cuestionamientos que buscan encontrar soluciones o respuestas a estas cifras de pérdida

y exposición de datos, generalmente calificados como confidenciales.

Los interrogantes podríamos agruparlos desde los aspectos humanos hasta los aspectos tecnológicos, pasando por los metodológicos y de gestión. Si bien la seguridad de la información es una propiedad emergente de un sistema (entendiendo éste como cualquier conjunto de componentes que se arreglan y relacionan entre sí para lograr un propósito común), los profesionales y analistas de seguridad generalmente procuran comprenderla como un fenómeno exclusivamente sistemático, lo que implica una alta concentración en los aspectos tecnológicos, administrativos y humanos cada uno desde su propia dinámica y perspectiva.

Al conjugarse una visión sistemática de la seguridad (aquella que busca identificar la inseguridad de la información), la evolución de las vulnerabilidades en los diferentes mecanismos tecnológicos, la falta de compromiso de las organizaciones con el tema de seguridad y una limitada cultura del cuidado de la información, se establece el escenario ideal para que la inseguridad desarrolle todo su potencial, un escenario donde la función de la seguridad no tiene la variedad requerida para identificar la inseguridad, ni comprenderla.

En este contexto, comprender el trinomio clásico de la seguridad de la información: confidencialidad, integridad y disponibilidad, se hace una labor desafiante y desconcertante, pues cada una de las fallas de seguridad identificadas podría corresponder a múltiples escenarios y variables que superan la capacidad de atención y operación de la función de seguridad.

En consecuencia, administrar la confidencialidad de la información residente en los diferentes medios de almacenamiento estático (discos duros, arreglos de discos, servidores corporativos, etc.) y móvil (USB, CD Roms, portátiles, entre otros) es una labor que demanda más que dispositivos de control de acceso a los medios de almacenamiento, sino adelantar una gestión de seguridad de la información, que exige regular el uso de los mismos, adaptarse a las condiciones cambiantes de la organización, los negocios y la tecnología, y aprender de la inseguridad que es propia al proceso de creación, uso, registro, transporte, recuperación y disposición de la información en la organización.

## Clasificación de la información

Cuando se revisa el tema de seguridad de la información, muchos son los enfoques y propuestas que se adelantan para desarrollar la protección de la información. Revisando las buenas prácticas internacionales en este

tema, encontramos las orientaciones y estrategias sugeridas por la norma ISO27001, la gestión de seguridad de la información dentro del marco de control de COBIT, las guías prácticas del *Nacional Institute of Standards and Technology* – NIST norteamericano, las directivas Europeas sobre seguridad de la información del Instituto de Seguridad Alemán – BSI, entre otras.

Si revisamos cada una de ellas, observamos que detallan diversas estrategias prácticas para aplicar en los procesos de las organizaciones con el fin de aumentar los niveles de protección de la información. De igual forma, todas ellas tienen un común denominador donde insisten a las organizaciones en un proceso básico para abordar un proyecto de seguridad informática: la clasificación de la información.

Clasificar la información es quizá el proceso más crítico y delicado en la gestión de la seguridad de la información. Sin una adecuada clasificación de la información, las decisiones de protección de la información no se asocian claramente con las funciones de negocio y la información crítica que manejan. De igual forma, al no estar clasificada la información el flujo de la misma en los procesos de negocio no se conoce y las medidas de seguridad que se establezcan posiblemente no serán las más adecuadas para la dinámica de la organización.

En consecuencia de lo anterior, al no estar clasificada la información, sumado al desconocimiento de los individuos del papel o rol (usuario, propietario o custodio) que juegan con la misma, aparece un escenario donde las fallas de seguridad desbordan las consideraciones tecnológicas instaladas y los procedimientos de operación previstos. En este momento, la gestión de incidentes de seguridad debe entrar en acción para avanzar en una contención y control del mismo, como una estrategia para disminuir el impacto de la vulnerabilidad identificada.

Revisando las prácticas de algunas organizaciones, encontramos que poseen importantes configuraciones en las infraestructuras de seguridad, procedimientos formales de operación y esfuerzos valiosos en la concientización de los usuarios, pero limitados ejercicios permanentes de clasificación (o desclasificación) de la información, los cuales hacen que en el modelo de seguridad implantado, la inseguridad adquiera matices que pueden desencadenar situaciones desconocidas o inesperadas.

En este aparte no se pretende detallar una clasificación específica para la información, pues existen múltiples recursos en el web y en la literatura que abarcan y especifican estrategias para hacerlo; sencillamente es un llamado de atención para las organizaciones que buscan fortalecer sus sistemas de

gestión de seguridad informática, no sólo en las inversiones naturales de tecnologías, sino en el activo base y razón de ser de la seguridad informática, la información.

## Medios de almacenamiento y mecanismos de seguridad informática

Con la información clasificada establecer los mecanismos de seguridad informática se vuelve una tarea menos dispendiosa, pues al tener establecidos qué activos de información tienen mayor sensibilidad para los diferentes procesos y por tanto, para la organización, se detalla con mayor claridad las exigencias requeridas para su protección.

Si lo anterior es correcto, los individuos de la organización notarán que no es lo mismo estar en un área crítica de negocio, que en un área de apoyo. Las condiciones de operación y las exigencias propias de flujo de información allí, enviarán un mensaje claro y preciso a los participantes, que se interrogarán sobre lo que sucede en el mismo. En este sentido, los profesionales y operadores que intervienen en tal proceso sabrán que usar la información y producir información en éste, requiere cuidados y protección especial que el proceso mismo le demanda.

La aparición de estrategias como el cifrado de los datos, los controles de acceso fuerte (autenticación fuerte), las exigencias de horario y limitaciones para ingreso de medios de almacenamiento móviles como agendas digitales, Ipods, mp3, mp4, USB, entre otros, serán mensajes directos para los involucrados en dicho proceso. Tener acceso a información sensible para el negocio de la compañía equivale a ser parte del personal clasificado y a los activos corazón de la empresa.

Una visión complementaria a la ya expuesta está relacionada con los medios donde se almacena este tipo de información clasificada como sensible. La función de seguridad, la función de tecnología y el área de archivo, en conjunto con el área jurídica, deberán afinar criterios de acción que permitan a la organización, custodiar y recuperar la información ahora y en el futuro. Las directrices que se establezcan, deberán articular lo mejor de las características de portabilidad informática, las mejores prácticas de conservación de los archivos físicos, la mejor funcionalidad de los mecanismos de seguridad y una flexible y adecuada regulación jurídica para limitar futuros impactos ante fallas que incidan en la información sensible de la organización, incluyendo la información de sus clientes.

La evolución de los medios de almacenamiento establece un reto constante

para las organizaciones y su información. Lo que hoy podemos comprender a través de los medios magnéticos y ópticos, será un reto y controversia al valorar estrategias holográficas y cuánticas. Las tecnologías de almacenamiento y los sistemas de archivo que la soportan son variables críticas para la conservación y recuperación de la información en el futuro, pero también, elementos necesarios para adelantar la disposición (saneamiento) final de los medios y su información.

## Saneamiento de medios de almacenamiento

Sanear un medio implica reconocer la importancia del mismo, la valoración de la información allí residente y los tiempos previstos de conservación de los datos. Sanear un medio, exige de la organización la madurez suficiente para integrar en los procesos de negocio, la disciplina formal de la clasificación de la información de las áreas de negocio y la capacidad para decidir que hacer con la misma en el tiempo. Sanear la información, es comprender que la función de tecnologías de información, es ser el custodio y soporte estratégico de los procesos de negocio y como tal, convertirse en una aliada para promover un adecuado registro, recuperación y permanencia en el tiempo de la información de la organización. (GARFINKEL, S. y SHELAT, A. 2003)

Cuando no existe claridad sobre qué se puede sanear, o mejor aún, sobre cuáles medios destruir, aparece el síndrome de "guárdelo para siempre", que lo que implica son altos costos de almacenamiento físico, materialización de las obsolescencia tecnológica y sobre manera, un mensaje de la organización para sus clientes, de que no ha sido capaz de administrar la seguridad de sus datos de acuerdo con los cambios y exigencias del medio. Así mismo, se abre la posibilidad de pérdidas y exposiciones de información por fallas en los procedimientos y operación de los mecanismos de seguridad previstos. (GARFINKEL, S. y SHELAT, A. 2003, GEIGER, M., FAITH CRANOR, L. 2006, GUTMANN, P. 1996)

De acuerdo con las guías del NIST, consignadas en su documento NIST 800-88 (KISSEL, R., SCHOLL, M., SKOLOCHENKO, S. y LI 2006) y otras directrices en este sentido (US DoE - National Industrial Security ProgramOperatingManual-NISPOM. NISPOM 5520.22-M 2006, National Institutes of Health Sanitization guide 2007, ISO/IEC 17799:2005 Sección 10.7, US DoE Cybersecurity Program Media clearing, purging and destruction guidance 2007), el saneamiento de datos se puede comprender a la luz de un cuadro de decisiones basado en la clasificación de la información y si ésta, dejará o no la organización. Si bien, las condiciones y acciones sugeridas por este instituto establecen

una buena práctica organizacional, es preciso revisarla y adaptarla a las necesidades de cada empresa y sus negocios, pues aplicarla sin este criterio, podría demandar inversiones importantes para las corporaciones y sus áreas de tecnologías.

El NIST establece tres acciones específicas para sanear los medios: distorsionar, purgar y destruir, que dependen de las variables previamente mencionadas y detalladas en la figura anterior.

Distorsionar, implica modificar la información lógica residente en el medio de almacenamiento y materializada en los documentos residentes en el sistema de archivos. La estrategia generalmente utilizada para distorsionar es la sobre escritura del medio, tantas veces como sea necesario para limitar la extracción de la información por parte de un tercero a través de programas especializados para estudiar los sistemas de archivo. (KISSEL, R., SCHOLL, M., SKOLOCHENKO, S. y LI 2006, GUTMANN, P. 1996)

Purgar, busca modificar físicamente el medio de almacenamiento, procurando destruir la estructura física (magnética u óptica) inicial del medio con el fin de evitar cualquier acción de recuperación de la información residente en el dispositivo. Esta estrategia generalmente viene acompañada de un dispositivo de hardware (desmagnetizadores) que afecte

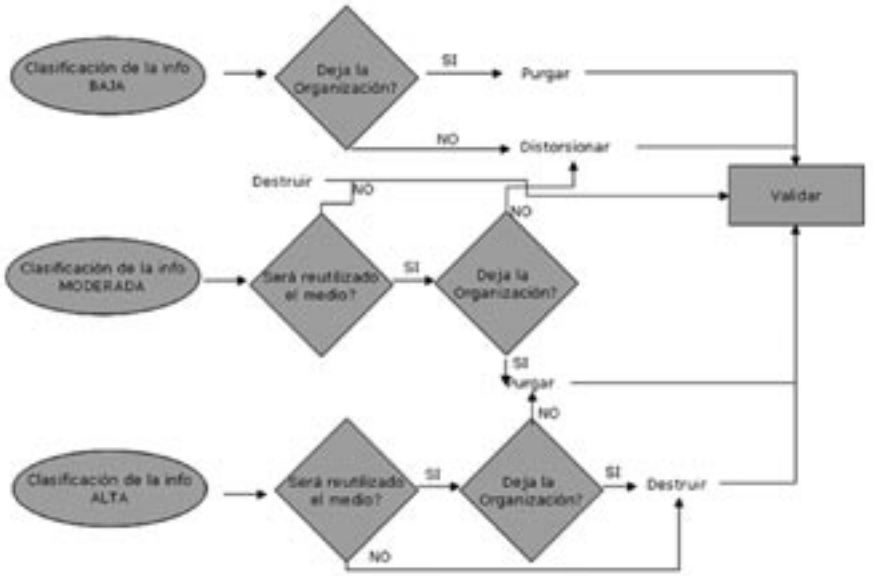


*Figura 1. Saneamiento de Medios (Traducción libre de: NIST 800-88 Guidelines for media sanitization)*

directamente el medio y desaparezca cualquier formato o registro de información en el mismo. (idem)

Destruir, acción que no requiere mayores detalles, busca desaparecer el medio donde se encuentra la información. La destrucción del mismo debe seguir un análisis formal del área de tecnología, de la función de seguridad y del área de negocio para que la información allí guardada se haya transferido, transformado o registrado en nuevos medios más modernos con las características inicialmente establecidas por los dueños o propietarios de la información. (idem)

## Reflexiones finales

La confidencialidad de la información es una característica requerida para las organizaciones modernas, donde no satisfacerla adecuadamente, implica posibles fallas que pueden poner en riesgo los negocios de la misma. Por tanto, comprender la inseguridad de la información, más que detectarla, exige una reflexión profunda de la organización para avanzar en una gestión de seguridad de la información orientada por un discurso de modelaje sistémico y sistemático.

En consecuencia de lo anterior, los medios de almacenamiento y la clasificación de la información son factores claves de éxito para avanzar en un adecuado manejo de la seguridad de la información. Si bien, las medidas tecnológicas de seguridad por sí mismas no proveen el nivel de protección requerido, la información requiere de una visión que integre la problemática del área de negocio, las consideraciones del área de tecnología y los elementos jurídicos que la regulan.

El saneamiento de medios de almacenamiento se convierte en un procedimiento interno (previsto por la norma ISO 27001 Sección 10.7) de las organizaciones que procura fortalecer y verificar que la información se mantiene dentro de los linderos de la corporación (ZETTERSTROM, H. 2002), limitando cualquier fuga que pudiese darse cuando los medios que la contienen abandonan la misma. Es claro, que este procedimiento está articulado en el factor humano y por tanto, establece un reto de confiabilidad y protección que exige de la función de seguridad, reconocer y aprender de la inseguridad propia de esta situación.

No clasificar la información, ni considerar una estrategia de saneamiento de medios, es abrir la puerta a una mayor complejidad en la administración de la seguridad de la información, es promover la generación inesperada de eventos que exijan más allá de su capacidad al equipo de atención de incidentes, es desbordar la capacidad

de aprendizaje de los profesionales a cargo de la seguridad de la información.

Cuando logramos comprender que la seguridad de la información es una propiedad emergente de un sistema, el trinomio básico de la seguridad se hace más comprensible, se establece una ruta de conocimiento y aprendizaje, que sin mayores consideraciones técnicas permite a todos los individuos de la organización entender las decisiones sobre la seguridad. Si esto es así, tendremos nuevos aliados y mayor información sobre la inseguridad, esa que es estrategia de aprendizaje, fuente para desaprender y arma para comprender.

## Referencias


*[1] KISSEL, R., SCHOLL, M., SKOLOCHENKO, S. y LI (2006) Guidelines for media sanitization. NIST Special Publication 800-88. Septiembre. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf*

*[2] GARFINKEL, S. y SHELAT, A. (2003) Remembrance of Data Passed: A Study of Disk Sanitization Practices, IEEE Security & Privacy, vol. 1, no. 1, 2003, pp. 17–27.*

*[3] GUTMANN, P. (1996) Secure Deletion of Data from Magnetic and Solid-State Memory. San Jose: Sixth USENIX Security Symposium Proceedings. Disponible en: www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html*

*[4] GEIGER, M., FAITH CRANOR, L. (2006) Scrubbing Stubborn Data: An Evaluation of Counter-Forensic Privacy Tools. IEEE Security and Privacy, vol. 4, No. 5, pp. 16-25, Sept/Oct.*

*[5] US DoE Cybersecurity Program (2007) Media clearing, purging and destruction guidance. Disponible en: http://cio.energy.gov/documents/CS-11_Clearing_and_Media_Sanitization_Guidance.pdf.*

*[6] US DoE (2006) National Industrial Security Program Operating Manual-NISPOM. NISPOM 5520.22- M. Disponible en: http://www.dss.mil/files/pdf/nispom2006-5220.pdf*

*[7] ISO/IEC 17799:2005 (2005) Code of Practice for Information Security Management, Control 10.7.2 (Disposal of Media).*

*[8] National Institutes of Health (2007) NIH Sanitization guide. Draft document. Disponible en: http://irm.cit.nih.gov/security/SanitizationGuide-1-16-07.doc*

*[9] ZETTERSTROM, H. (2002) Deleting sensitive information. Why hitting delete isn't enough. Reading Room SANS Institute. Sección Privacy. Disponible en: http://www.sans.org/reading_room/whitepapers/privacy/691.php*



***Jeimy J. Cano, Ph.D, CFE.*** *Miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI), Facultad de Derecho, Universidad de los Andes. Colombia. Miembro Investigador de ALFA-REDI (Red Latinoamericana de Especialistas en Derecho Informático). Ingeniero de Sistemas y Computación, Universidad de los Andes. Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Ph.D in Business Administration, Newport University. Profesional certificado en Computer Forensic Analysis (CFA) del World Institute for Security Enhacement, USA. Profesional certificado como Certified Fraud Examiner (CFE) por la Association of Certified Fraud Examiners. Coordinador Lista de Seguridad – SEGURINFO (ACIS).*