

Trazabilidad de las Operaciones Electrónicas. Un Reto para la Gerencia de Tecnologías de Información

By Jeimy J. Cano, Ph.D, CFA, CFE

Introducción

Las organizaciones del siglo XXI están inmersas en una dinámica de relaciones digitales e informáticas que exigen de ellas mejores prácticas y estrategias, para mantener el debido control y registro de las operaciones en el desarrollo de su negocio. Asimismo, en este nuevo entorno, es preciso estar preparado tanto a nivel técnico como administrativo en la práctica de la administración de “inseguridad informática” [CANO 2004], como una forma de procurar un ambiente computacional más seguro, donde el riesgo inherente se mantenga dentro de niveles previstos y aceptables.

Estos elementos sugieren que las empresas deben estar avocadas a reevaluar sus relaciones de negocio corporativas, considerando nuevas formas para efectuar la reconstrucción y rastros de las operaciones electrónicas de sus usuarios y sus socios de negocio. Esta nueva competencia exige de la organización mayor conciencia sobre la evidencia digital inmersa en sus sistemas computacionales y la manera cómo la administra. En consecuencia, no es suficiente mantener un registro de las operaciones, se requieren características adicionales para darle sentido a la reconstrucción de los eventos.

Sincronización, control, integridad de archivos y confiabilidad en la generación de los registros de auditoría son elementos requeridos para darle vida a la trazabilidad o a la capacidad para rastrear, reconstruir o establecer relaciones entre los objetos monitoreados de un sistema. En trazabilidad se hace referencia a un concepto sistémico, en la necesidad de establecer relaciones y observar el todo, y sistemático, en la manera como se alcanza y se materializa el concepto en las aplicaciones corporativas.

En este sentido, este documento plantea una propuesta inicial sobre la trazabilidad de las operaciones en las aplicaciones corporativas. Es un marco de discusión básico para mejorar y desarrollar el concepto a profundidad, fundamentado en características técnicas y administrativas requeridas en arquitecturas de cómputo. El constante avance de la tecnología y los procedimientos internos de las organizaciones, sugieren elementos nuevos que deben ser revisados para enriquecer la temática de la trazabilidad.

Definiendo la Trazabilidad

Establecer qué significa la trazabilidad, implica revisar definiciones y reflexiones que previamente se han establecido alrededor de la auditoría de las tecnologías de información (TI). Si bien el registro de las operaciones electrónicas es un factor

fundamental en los procesos de las organizaciones, la reconstrucción de eventos obedece tanto a la formalidad de los registros de auditoría, como a las características técnicas y administrativas que las organizaciones deben adoptar si quieren contar con estrategias y escenarios para rastrear situaciones particulares. Se entiende por reconstrucción de eventos a la asociación que pueda existir entre las transacciones de una aplicación o sistema, teniendo en consideración sus posibles interfases.

Trazabilidad es la *capacidad* que tiene una organización o sistema para *rastrear, reconstruir o establecer* relaciones entre *objetos monitoreados*, para identificar y analizar situaciones específicas o generales en los mismos.¹ Para aclarar esta definición se procede a profundizar en las palabras señaladas, brindándole un sentido práctico de aplicación que será revisado más adelante en el documento:

- *Capacidad*—Esta palabra sugiere la definición de acciones y estrategias específicas por parte de la organización o sistema que permita, bajo directrices establecidas, desarrollar una actividad específica.
- *Rastrear, reconstruir o establecer*—Este conjunto de verbos hacen referencia a la esencia misma del concepto que especifican. Son las acciones que se buscan efectuar cuando de trazabilidad se habla.
- *Objetos monitoreados*—La trazabilidad sin una adecuada definición de pistas de auditoría no logra alcanzar sus objetivos (*rastrear, reconstruir o establecer*). El monitoreo es un prerrequisito para darle sentido a la trazabilidad como capacidad en un sistema. Es importante aclarar que es posible no tener monitoreo definido formalmente, pero sí, registros propios de los sistemas o procesos que pueden ser útiles para rastrear, reconstruir o establecer relaciones. Asimismo, es fundamental la capacidad de relacionar esa información de auditoría, entre los diversos niveles y componentes de una infraestructura informática. Estas relaciones se establecen siempre y cuando los registros de auditoría generados y la arquitectura de cómputo se adhieran a las características básicas descritas más adelante.

Proponiendo Niveles de Trazabilidad

Es importante aclarar que la trazabilidad exige algunas características básicas en la arquitectura para lograr “rastrear, reconstruir o establecer,” como lo son (adaptado de CANO 2002):²

- Sincronización
- Control y aseguramiento de registros de monitoreo

- Confiabilidad de la generación de registros de monitoreo
- Basado en estas características presentadas, es primeramente necesario establecer una clasificación básica para la trazabilidad en las aplicaciones corporativas de acuerdo con nivel de importancia y criticidad en el cumplimiento de su misión (Ver **tabla 1**).

Tabla 1 —Propuesta de Niveles de Trazabilidad

Nivel de Trazabilidad	Característica requerida			
	Definición de Pistas de Auditoría	Confiabilidad en la Generación de Monitoreo	Control y Aseguramiento de los Registros de Monitoreo	Sincronización de la Arquitectura de Cómputo
ALTA	X	X	X	X
MEDIA	X	X	X	
BAJA	X	X		

El nivel de *trazabilidad alta* está asociado con la necesidad que tiene la organización de crear, almacenar y recuperar información confiable que sea reconocida como evidencia digital válida en cualquier proceso judicial que se adelante alrededor de las aplicaciones que requieran este nivel. Contar con este nivel de trazabilidad exige por parte de la organización mantener un conjunto de prácticas organizacionales alrededor de la definición y control de registros de auditoría como base fundamental para fortalecer los esquemas probatorios a futuro, los cuales deben estar fundados en las directrices de seguridad de la información de la organización.

El nivel de *trazabilidad media* está relacionado con el requisito de las organizaciones por mantener evidencia de las acciones realizadas por usuarios o procesos en el uso de los sistemas de información y las posibles relaciones entre ellos. Si bien esta información se puede requerir para procesos de investigación interna de las empresas, hay que considerar que la sincronización no es un requisito formal de la misma. Es decir, no está asociada la generación de registros de auditoría a un sistema centralizado de tiempo que verifique la hora y fecha de su creación. Se confía en el manejo del tiempo interno para los dispositivos de hardware o software. Los registros generados con nivel de trazabilidad media obedecen a políticas y formalidades establecidas por la organización.

El aplicar un nivel de *trazabilidad baja* es una decisión que toma una organización conciente de que los registros de los eventos en los sistemas no requieren mayores exigencias más allá del debido registro de las acciones de los usuarios para efectos de estadísticas y proyecciones de uso. Los registros generados o relaciones establecidas bajo este nivel no pueden ser considerados evidencia confiable de hechos acontecidos.

Es importante anotar que el nivel de detalle que alcance la investigación, está asociado con el nivel de granularidad definido para las pistas de auditoría del sistema investigado. Es decir, mientras el diseño de las pistas de auditoría no responda una definición formal de lo que se requiere registrar para revisión posterior, los resultados de la investigación podrían resultar menos detallados o inclusive inconclusos.

Trazabilidad en Aplicaciones Corporativas

Basado en estas premisas iniciales, se establece entonces una explicación de los niveles de trazabilidad para las aplicaciones corporativas, construyendo la propuesta (ver **tabla 2**) en un

Tabla 2—Propuesta de Trazabilidad en Aplicaciones Corporativas

	Misión Crítica	Apoyo Actividades Administrativas	Departamentales o Desarrollos Locales
ALTA	X		
MEDIA		X	
BAJA			X

campo de aplicación práctica para las organizaciones.

Las aplicaciones de misión crítica son aquellas que soportan los procesos esenciales del negocio. Usualmente son componentes de software de procesamiento intensivo que además generan registros de seguridad, de control y estadísticos. Estos cumplen con el encargo de generar valor agregado, mayor eficiencia y efectividad en el desarrollo de las actividades más importantes de la empresa. Los usuarios y clientes generalmente tienen interacción con estas aplicaciones que crean transacciones u operaciones que deben ser registradas, almacenadas y recuperadas según sea la solicitud de éstos y las políticas de la organización. En este sentido, la manera como se genera la información y se conserva, son elementos claves para fundamentar el discurso probatorio en caso de requerirse ante una diligencia judicial.

Por otra parte las aplicaciones de apoyo administrativo y las departamentales, si bien, son importantes para las áreas dueñas de los procesos, sus registros de auditoría y la capacidad para relacionar los eventos allí registrados, responden a directrices propias de la organización en tanto no afecten los procedimientos y normas establecidos.

Con esto en mente y buscando establecer un marco de evaluación base para revisar y validar la trazabilidad en las aplicaciones corporativas, se plantea como siguiente paso una estrategia práctica de evaluación aplicando los conceptos previos en aspectos técnicos y administrativos. Para ello se revisarán características propias de los sistemas operacionales, bases de datos y las aplicaciones.

Evaluando la Trazabilidad de las Aplicaciones Corporativas

Con los conceptos básicos establecidos, se procede entonces a detallar los niveles de revisión y evaluación de la trazabilidad de las aplicaciones corporativas, buscando puntualizar la implementación y operación de las características requeridas para los niveles definidos: alta, media y baja.

Para avanzar en esta tarea, se proponen preguntas y pruebas fundamentales que permitan validar el cumplimiento o no de las características presentadas previamente. Para ello se presenta un formato (ver **tabla 3**) de revisión y validación de los niveles de trazabilidad propuestos. Es decir, se detalla a continuación una estrategia de evaluación para los niveles de trazabilidad: alta, media y baja.

Tabla 3—Formato de Evaluación de Trazabilidad de Aplicaciones Corporativas

FORMATO DE EVALUACIÓN DE TRAZABILIDAD DE APLICACIONES CORPORATIVAS			
Nombre del evaluador:			
Nombre de la aplicación a evaluar:			
Sistema operacional del servidor:			
Base de datos y su versión:			
Fecha:			
		¿Hay evidencia?	Observaciones
Sistema Operacional	Documentación de la fecha de instalación		
	Documentación de últimos parches instalados		
	Registros de auditoría de control de acceso de los usuarios		
	Control de integridad y acceso a los archivos principales del sistema de archivos (evaluar el caso para Unix y Windows)		
	Listado de procesos activos y autorizados en la máquina		
	Sincronización de fecha y hora del sistema		
Base de Datos	Sincronización de fecha y hora del sistema de BD		
	Documentación de últimos parches instalados en la BD		
	Registros de auditoría de control de acceso de los usuarios BD		
	Documentación de la definición de pistas de auditoría		
	Documentación de las pruebas realizadas sobre la confiabilidad de las pistas definidas		
	Control de integridad y acceso a los archivos del log definidos en la BD		
Aplicación	Documento de especificación de control de acceso a la aplicación		
	Documento de pruebas del registro de control de acceso a la aplicación		
	Control de integridad y acceso a los archivos del log definidos en la aplicación		
	Sincronización de fecha y hora del sistema		
	Documento de control de cambios en los archivos fuentes de la aplicación		

Convenciones

En la columna *¿Hay evidencia?* los valores permitidos son:

- **SI**—Corresponde a que existe y se aplica sistemáticamente la actividad o elemento en evaluación
- **PARCIAL**—Corresponde a que existe y no se aplica sistemáticamente la actividad o elemento en evaluación

- **NO**—Corresponde a que NO existe la actividad o el elemento en evaluación

Análisis de la Tabla

Luego de completar la tabla, se podrá clasificar el sistema según los resultados siguientes:

- **Trazabilidad alta**—Las respuestas deben ser SI en todos los aspectos de evaluación.
- **Trazabilidad media**—Existe al menos un PARCIAL en alguno los elementos a evaluar tanto en sistema operacional, base de datos y aplicaciones.
- **Trazabilidad baja**—Existe al menos un NO en algunos de los elementos de evaluación. Esta calificación se presenta así dado que esto puede impactar cualquiera de los elementos a evaluar en el sistema operacional, base de datos y aplicaciones.

Limitaciones de la Propuesta

Definir y evaluar la trazabilidad de las operaciones en las aplicaciones corporativas exige tanto de la organización como del evaluador un nivel de experiencia y madurez en el campo del debido registro, auditoría y control. Sólo así se podrá establecer un diagnóstico base de la situación de una organización frente a su trazabilidad.

La propuesta desarrollada en este documento es un primer paso en el refinamiento del concepto de trazabilidad, lo cual requiere una constante revisión y análisis de las variables que exhibe la tecnología y su aplicación en las organizaciones. Por lo tanto, es probable que el formato de evaluación requiera en un futuro de una actualización para hacer más exhaustiva la caracterización de las condiciones requeridas a nivel de sistema operacional, la base de datos y la aplicación.

La formulación de los niveles de trazabilidad sugeridos en este documento es una orientación basada en la experiencia del manejo de pistas de auditoría en las organizaciones. Consecuentemente sugiere una estrategia práctica de análisis, sin exigir condiciones ideales de formalidad que no se puedan cumplir. Es probable que para algunos las características definidas para los niveles de trazabilidad alta sean exigentes y que requieran importantes ajustes a nivel técnico y organizacional, pero efectivamente las autoridades de justicia pueden demandar altos niveles de certeza para validar la evidencia. Esto implica mejorar en los aspectos mencionados previamente.

Los elementos conceptuales tratados en este documento, requieren de más reflexión y análisis, para modelar mejor las características de rastreo y relaciones requeridas para reconstruir las acciones de los usuarios. Por tanto, las estrategias y propuestas presentadas buscan ser un pretexto académico base para futuro análisis relativo al tema.

Reflexiones Finales

La trazabilidad de las operaciones en las aplicaciones corporativas es un reto actual de la gerencia de TI dado que la evidencia de las operaciones y el soporte legal de las mismas ahora se encuentra en medios electrónicos. Esto demanda la capacidad para demostrar la certeza de la operación y los

procedimientos y actividades asociadas que permitan sortear la evaluación y revisión de la administración de justicia, en caso de ser requerida.

La evidencia digital cobra hoy por hoy mayor importancia que en el pasado y las organizaciones que están o se lanzan a un escenario de negocios, bien sean electrónicos o no, deben procurar establecer actividades o procesos base que les permitan afrontar una reclamación sobre actividades en sus sistemas con el debido cuidado, diligencia y previsibilidad. Con ello se deben disminuir los costos derivados de investigaciones forenses en informática para demostrar o verificar las prácticas de seguridad y control vigentes en la organización.

En este sentido, la trazabilidad de las operaciones en las aplicaciones es un tema que debe ser parte de la agenda de los gerentes de TI, como un aspecto importante de negocios y como una manera de probar de manera legal el debido registro de las operaciones de sus empresas. Por lo tanto, la trazabilidad debe pasar de un contexto eminentemente histórico y técnico a ser una directriz organizacional y práctica regular de las empresas.

Referencias

¹ Definición adaptada de: *IEEE Standard Computer Dictionary: A compilation of IEEE Standard Computer Glossaries*. New York, 1990

² Sincronización—Esta característica requiere que la arquitectura presente unos mecanismos de tiempo centralizado que sean utilizados por las máquinas que soportan las aplicaciones.

Control y aseguramiento de registros de monitoreo—Esta característica exige que los registros de monitoreo estén configurados de tal manera que se conozca dónde se generan, quién tiene acceso a ellos y si ocurren cambios, queden documentados con fecha, hora y responsable. Esto permitiría además el uso de esta información como sustento legal en caso de requerirse.

Confiabilidad de la generación de registros de monitoreo—Este elemento hace referencia a la efectividad y eficiencia de las características del registro de eventos (logs de auditoría) en los sistemas de información. Es decir, verificar que el registro de los eventos realizados está conforme con la definición de monitoreo establecida para el sistema de información.

Bibliografía

Cano, J.; "RE.D.AR. Preparación Forense de Redes. Un Modelo de Análisis," Conferencia Magistral. Primer Congreso Iberoamericano de Seguridad Informática, celebrado en febrero de 2002 en Morelia, México. Disponible en www.criptored.upm.es/guiateoria/gt_m142e.htm

Cano, J.; "Inseguridad Informática: Un Concepto Dual en Seguridad Informática," *Revista de Ingeniería*. Universidad de los Andes, Facultad de Ingeniería. Mayo 2004, ISSN:0121-4993.

Casey, E; *Digital Evidence and Computer Crime*, Academic Press, 2000

Casey, E; *Handbook of Computer Crime Investigation*, Academic Press, 2001

Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones, *Internet Comercio Electrónico & Telecomunicaciones*, Legis—Universidad de los Andes, 2002

Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones, *Derecho de Internet & Telecomunicaciones*, Legis—Universidad de los Andes, 2003

Mandia, K.; Proise, C.; Pepe, M.; *Incident Response and Computer Forensics*, 2nd Edition, McGraw Hill, 2003

Riofrio, J.; *La Prueba Electrónica*, Editorial Temis, 2005

Weber R.; *Information Systems Control and Audit*, Prentice Hall, 1999

Jeimy J. Cano, Ph.D, CFA, CFE

es ingeniero de sistemas y computación, Universidad de los Andes. Cuenta con una maestría en ingeniería de sistemas y computación de la Universidad de los Andes. Es doctor en filosofía en administración de negocios, de la Newport University. Es conferencista, profesor universitario e investigador independiente en seguridad informática a nivel nacional e internacional. Y es coordinador general de la lista de seguridad SEGURINFO. Cano puede ser contactado en: jjcano@yahoo.com.

Information Systems Control Journal is published by the Information Systems Audit and Control Association Inc. Membership in the association, a voluntary organization of persons interested in information systems (IS) auditing, control and security, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of the Information Systems Audit and Control Association and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *Information Systems Control Journal* does not attest to the originality of authors' content.

© Copyright 2005 by Information Systems Audit and Control Association Inc. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by the Information Systems Audit and Control Association Inc., for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

www.isaca.org