Tipo de artículo: Artículo original

Marcos de referencia para gestión de registros de auditoría

Log records management frameworks

Gilberto Enrique González Hidalgo[1]*, https://orcid.org/0000-0001-6399-7635
Henry Raúl González Brito [2], https://orcid.org/0000-0002-3226-9210
Mónica Peña Casanova [3], https://orcid.org/0000-0003-2500-4510

[1] CIGED, Facultad 2, Universidad de las Ciencias Informáticas. Carretera a San Antonio Km 2 ½ Torrens. Boyeros. La Habana. Cuba. gegonzalez@uci.cu
[2] Telemática, Facultad 2, Universidad de las Ciencias Informáticas. Carretera a San Antonio Km 2 ½ Torrens. Boyeros. La Habana. Cuba. henryraul@uci.cu
[3] Facultad 2, Universidad de las Ciencias Informáticas. Carretera a San Antonio Km 2 ½ Torrens. Boyeros. La Habana. Cuba. monica@uci.cu

*** Autor para correspondencia: gegonzalez@uci.cu**

Resumen

La protección de la información es un factor esencial para la sostenibilidad de las organizaciones. En este escenario, cobra gran importancia las acciones encaminadas a garantizar la auditoría de los sistemas con el objetivo de prevenir o detectar violaciones que afecten la integridad, disponibilidad y confidencialidad de los datos. Dentro de los principales problemas que surgen durante la gestión de registros de auditoría, se encuentran que en ocasiones se desconoce cómo y de qué eventos generar registros, así como qué tratamiento darles a los registros generados. Esta investigación tiene como objetivo principal, la elaboración de un procedimiento que contribuya a perfeccionar el proceso de gestión de los registros de auditoría desde el desarrollo de las aplicaciones informáticas, hasta su implantación y explotación, con el objetivo de garantizar la trazabilidad de los sistemas. Para lograrlo, en primer lugar, se analizaron normas, guías y estándares que describen el proceso de gestión de los registros de auditoría. Después de realizado el análisis, se identificaron los principales aspectos que se deben considerar en dicho proceso y se elaboró un procedimiento aplicable a los sistemas de gestión de la información. Dicho procedimiento fue validado mediante la aplicación del método de Redes de Petri, para comprobar su estructura, e implementado en un caso de estudio para comprobar la ejecución de cada una de las actividades identificadas.

Palabras clave: auditoría, gestión de registros de auditoría, pistas de auditoría, auditoría de sistemas.

Abstract

The protection of information is an essential part of the sustainability of organizations. In this scenario, actions aimed at ensuring the auditing of systems with the aim of preventing or detecting violations that affect the integrity, availability and confidentiality of data take on great importance. Among the main problems that arise during the management of audit reports, we find that sometimes it is not known how and from which events records are generated, as well as what treatment is given to the generated records.The main objective of this research is the development of a procedure that contributes to the improvement of the audit record management process from the development of the computer applications to their implementation and operation in order to guarantee the tracking of the systems. To achieve this, firstly, guidelines and standards describing the audit record management process were analyzed. After the analysis, the main aspects to be considered in such process were identified and a procedure applicable to the information management systems was elaborated, which allows the centralized management of the audit records. This procedure was validated by applying the Petri Network method, to check its structure, and implemented in a case study to check the execution of each of the identified activities.

Keywords: *audit trails, logs, log management.*

Recibido: 10/01/2021
Aceptado: 08/11/2020

Introducción

Los registros siempre han sido la manera más utilizada para preservar las actividades realizadas en los sistemas de cómputo y aunque en un inicio, fueron creados con fines de diagnóstico y depuración de los sistemas, han ido evolucionando para registrar eventos e información que es útil para la realización de auditoría y análisis forenses en caso de actividades maliciosas o ataques a los sistemas.

La información generada por eventos en los sistemas informáticos no siempre es suficiente para reconstruir las acciones realizadas sobre ellos, además los usuarios no poseen el conocimiento adecuado para generar los registros que permitan la trazabilidad de las acciones, por lo cual existe el riesgo de tener una violación de seguridad y pase desapercibida. Por este motivo, se debe garantizar durante el desarrollo de las aplicaciones informáticas, una correcta estrategia de trazabilidad y auditoría de la información que permita detectar cualquier tipo de anomalía en las acciones realizadas por las personas que utilizan dichas aplicaciones.

La Universidad de las Ciencias Informáticas, centro docente-productor, como parte del cumplimiento de las políticas de informatización del país, tiene entre sus misiones la de "…, producir aplicaciones y servicios informáticos a partir del vínculo estudio – trabajo como modelo de formación – investigación - producción, sirviendo de soporte a la industria cubana de la Informática." Cuenta con 10 centros que desarrollan actividades de I+D+i y realizan más de 100 proyectos al año (UCI, 2020).

Sin embargo, actualmente no existe un procedimiento para la gestión de los registros de auditoría en los sistemas desarrollados por la UCI, lo que conlleva a que, para cada nuevo proyecto que se realice, se deba dedicar tiempo y recursos humanos en planificar, adoptar y mejorar continuamente el sistema para la gestión de registros de auditoría. Por otra parte, no todas las aplicaciones informáticas desarrolladas realizan el proceso completo de gestión de registros de auditoría, ni cumplen con los procedimientos, estándares o buenas prácticas para la generación, protección, monitoreo, análisis, almacenamiento y período de retención de dichos registros, por lo cual, estos registros de auditoría, no llegan a convertirse en información realmente útil para el análisis de los sistemas que permita la detección temprana de amenazas y facilite las investigaciones relacionadas con incidentes de seguridad.

Las situaciones antes descritas, provocan problemas en el dimensionamiento de las infraestructuras para el desarrollo de las aplicaciones informáticas, así como, problemas en el mantenimiento y mejora de las soluciones para gestionar los registros de auditoría y generan dificultades en el momento de reconstruir eventos y detectar violaciones de seguridad en los sistemas.

Materiales y métodos

El alto costo que ha implicado históricamente la ausencia o errores asociados a la generación de registros de auditoría han provocado que surjan múltiples marcos de referencia con diversidad de estructura, procesos y términos, lo cual afecta la integración, disminución de la complejidad y aplicación pertinente en las organizaciones de dichos marcos. Como punto de partida para abordar la integración de diferentes marcos de referencia para la gestión de los registros de auditoría, se caracterizan algunos de los más usados en este proceso.

NIST

En su publicación especial 800-92, dedica 9 controles específicos a la auditoría y gestión de trazas, mientras que en el caso de la gestión de incidentes de seguridad determina 14 controles (Kent & Souppaya, 2006). Establece que, para la gestión efectiva de los registros de auditoría, se deben registrar todas las peticiones del cliente y respuestas de los servidores, información de los usuarios, información de utilización del sistema y acciones significativas como el proceso de inicio y apagado de las aplicaciones. De igual manera, se deben generar registros de las fallas y cambios en la configuración de los sistemas (Kent & Souppaya, 2006).

Según esta publicación especial (Kent & Souppaya, 2006),se debe:

- Priorizar la gestión de registros de auditoría de manera adecuada en la organización.
- Establecer políticas y procedimientos para la gestión de registros de auditoría.
- Crear y mantener una infraestructura para la gestión de registros de auditoría.
- Proveer entrenamiento a todo el equipo que tenga responsabilidades en la gestión de registros de auditoría.

En su publicación 800-53, proporciona un conjunto de controles de seguridad que puedan satisfacer los requisitos de seguridad de las organizaciones haciendo frente a diversas amenazas que incluyen ciberataques, desastres naturales, fallas estructurales y errores humanos(Ross, 2014). Para facilitar el proceso de selección y adopción de los controles propuestos, estos se encuentran agrupados en 18 grupos que contienen elementos del proceso de gestión de seguridad de la información. El grupo de “Auditoría y Responsabilidad Proactiva”, mediante los controles desde el AU-01 al AU-12, define los aspectos necesarios para cumplir con la gestión de los registros de auditoría.

En los temas referidos a los equipos de desarrollo de aplicaciones, especifica tres controles (SA-15, SA-16 y SA-17) que detallan elementos relacionados con la necesidad de capacitación por parte de los desarrolladores de los mecanismos de seguridad implementados. Estos controles abordan también, los elementos que debe cumplir el diseño de un sistema o componente, los elementos que deben ser documentados y los procesos de apoyo durante el desarrollo de software.

PCI DSS

El Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS) proporciona una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de cuentas y se aplica a todas las entidades que participan en el procesamiento de las tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios (PCI Security Standards Council, 2018).

En su requisito número 10 "Rastreo y monitoreo de los accesos a los recursos de la red y a los datos del titular de la tarjeta", del 10.1 al 10.7, aborda los temas referentes a la supervisión y evaluación de las redes con regularidad y para ello, define como debe realizarse la implementación de los registros de auditoría en todos los componentes del sistema a fin de poder reconstruir eventos, cuando se deben generar registros, que campos deben contener los registros generados y como deben protegerse estos registros. Además, sugiere que se conserve el historial de registros de auditorías durante, al menos, un año, con un mínimo de disponibilidad para análisis de tres meses (PCI Security Standards Council, 2018).

ISO/ IEC 27001:2013

Entre los controles del estándar ISO/IEC 27001, el A.12 "Seguridad en las operaciones", incluye en su epígrafe A.12.4 "Registro y monitoreo", los aspectos referidos a la generación, tratamiento y protección de los registros de auditoría. Para ello indica que los registros de eventos que muestran las actividades del usuario, excepciones, fallas y eventos de seguridad de la información deben ser producidos, guardados y revisados regularmente (Chopra & Chaudhary, 2020).

Además, la información de los registros deberá estar protegida contra la manipulación y el acceso no autorizado y las actividades realizadas por los administradores y los operadores del sistema, se almacenarán y los registros se protegerán y revisarán periódicamente. También, los relojes de todos los sistemas de procesamiento de información relevantes dentro de una organización o dominio de seguridad se sincronizarán con una única fuente de tiempo de referencia (Chopra & Chaudhary, 2020).En el caso del control A.16 referido a "Gestión de incidentes de seguridad", se propone que las organizaciones deberán definir y aplicar procedimientos para identificar, recolectar y preservar, información que pueda ser utilizada para esclarecer algún incidente (Chopra & Chaudhary, 2020).

Controles Críticos

Los 20 controles críticos de seguridad se agrupan en tres grupos: Básicos (del uno al seis), Fundacionales (del siete al 16) y Organizativos (del 17 al 20). Dentro de los controles Básicos, el número seis: "Mantenimiento, monitoreo y

análisis de logs de auditoría", describe elementos que se pueden implementar teniendo en cuenta la clasificación de la organización (Center for Internet Security, 2019).

Para organizaciones con recursos y experiencia en ciberseguridad limitados se debe garantizar que todos los sistemas tengan los registros habilitados (Center for Internet Security, 2019). Para organizaciones con recursos y experiencias en ciberseguridad moderados se recomienda además, que se utilicen al menos tres fuentes para sincronizar las fechas, que los registros incluyan información detallada de los eventos, que exista espacio suficiente para almacenar los registros, que los registros sean agregados a una infraestructura central y que se revisen para detectar anomalías utilizando un SIEM o una herramienta de análisis de logs (Center for Internet Security, 2019). Para las organizaciones maduras, con recursos y experiencia en ciberseguridad significativos. Además de los elementos anteriores, plantea que se debe mejorar regularmente los sistemas SIEM para identificar mejor los eventos (Center for Internet Security, 2019).

OWASP

Según (Stock et al., 2017), el registro y monitoreo insuficiente en las aplicaciones figura como una de las diez principales vulnerabilidades reconocidas por *OWASP* en las aplicaciones. Por esta razón, se describen algunos aspectos para determinar cuándo una aplicación es vulnerable y prevenir esta deficiencia (Stock et al., 2017).Para ello propone registrar todos los errores de inicio de sesión, de control de acceso y de validación de entradas para identificar cuentas sospechosas y conservarlos por tiempo suficiente para un posterior análisis. Además, de acuerdo a esta publicación, todas las transacciones importantes deben generar una traza de auditoría con controles de integridad que permitan detectar su modificación o borrado (Stock et al., 2017).

La Guía de Registros, identifica los principales problemas en la gestión de trazas, así como las funciones principales y los elementos necesarios para planear una infraestructura que soporte dicha gestión. En cuanto a los eventos que deben generar registros, sugiere que se deben registrar las peticiones del cliente y respuestas de los servidores, uso de la información (tipo de transacción y tamaño, tráfico generado) y acciones operativas significativas como el inicio y apagado de la aplicación, fallas de la aplicación y cambios importantes en la configuración de la aplicación (OWASP, n.d.). Además, agrupa las funciones de una infraestructura para la gestión de logs en tres grupos General, Almacenamiento y Análisis y plantea los elementos que se deben considerar para planear una infraestructura para la gestión de registros de auditoría (OWASP, n.d.).

HITRUST-CSF

El Health Information Trust Alliance (HITRUST) Common Security Framework (CSF), consiste en controles de seguridad diseñados para guiar a las entidades en la implementación de medidas para cumplir con la regulación

(Health Information Privacy) HIPAA. En los controles asociados a la "Gestión de Comunicaciones y Operaciones", el objetivo 9.10, "Monitoreo", contiene las especificaciones que se deben cumplir en cada nivel para la generación, monitoreo y protección de los registros (All, 2019).

El nivel uno es aplicable a todos los sistemas y orienta que los registros de auditoría deben incluir un identificador de usuario, la acción realizada, la fecha de la acción realizada y un identificador de los datos. También especifica que el período de retención de los registros en este nivel es definido por la organización (All, 2019).

El nivel dos, se aplica para los sistemas que generen de 6 750 a 85 000 transacciones por día y que el número de usuarios sea de 500 a 5 500. Este nivel detalla que se deben registrar, además, todos los intentos de autenticación (válidos o no válidos), los intentos de acceso a los datos (válidos o no válidos), cambios en la configuración del sistema, uso de privilegios, creación de objetos a nivel de sistema, cambios en el estado de la protección del sistema y otros aspectos relacionados con las redes.

Marco regulatorio en Cuba

En la Resolución 126, dentro de las medidas de control para comprobar la seguridad en un sistema informático que se describen, se encuentra la gestión de las trazas de los servicios y sistemas informáticos (MINCOM, 2019a). E cuanto a la Resolución 128, en los aspectos referidos a la gestión de incidentes y violaciones de seguridad de las TIC, se plantea como uno de sus requisitos, que se debe garantizar la recolección y preservación de las trazas de auditoría y que la metodología para la gestión de la seguridad informática, incluye, como parte de los componentes que forman parte de las políticas de seguridad, la definición de las responsabilidades de los usuarios, especialistas y directivos, sus derechos y obligaciones con respecto a la gestión de las trazas de auditoría y otros aspectos (MINCOM, 2019b).

Las regulaciones o guías analizadas hasta ahora, describen los aspectos relevantes que se deben tener en cuenta para cumplir con los objetivos de la gestión de registros de auditoría, incluyendo, los elementos que debe contener cada registro para garantizar la trazabilidad de los eventos. Además de estas, existen otras que describen el tratamiento que se le debe dar a la información recolectada y el tipo de información que no debe recolectarse.

El GDPR, redactado por la Unión Europea y puesto en práctica a partir del año 2018, está enfocado en la protección de los datos de las personas. En la sección de "Principios relacionados con el procesamiento de datos personales" se describe que la información personal de los usuarios debe ser (Otto, 2018):

- Procesada legalmente, de manera transparente en relación con el interesado.
- Recolectada con fines específicos y legítimos y no puede ser adicionalmente manejada de manera incompatible con dichos fines.
- Limitada en relación con los fines para los cuales se recolecta.

- Almacenada solo por el tiempo necesario para el cual fue recolectada.
- Procesados de forma tal que su que se garantice su protección contra acceso no autorizado.

Esta guía, redactada por *OWASP*, describe la información que debe ser excluida de los registros generados (OSWAP, 2019). Entre esta información se encuentran cadenas de conexión, código fuente de las aplicaciones, contraseñas de usuarios o equipos, información bancaria, *tokens* de acceso, información personal del usuario o cualquier tipo de información sin el consentimiento previo del usuario.

Resultados y discusión

El análisis de los principales marcos de referencia asociados a la gestión de registros de auditoría arroja que se pueden agrupar en dependencia de la función o capa que afecten dentro de una infraestructura de gestión de registros de auditoría. Asociado a los elementos de Generación y Almacenamiento, se pueden identificar que existen múltiples orígenes de registros, además, al generar registros, pueden existir inconsistencia en el contenido, en la fecha de creación y en el formato de dichos registros (Kent & Souppaya, 2006).

Por otra parte, la información que contienen los registros, de los sistemas y la red, es sensible, por lo cual es necesario que se garantice la integridad y confidencialidad de los mismos. La falta de protección de los registros puede causar que se modifiquen o eliminen, lo cual puede permitir que una actividad maliciosa pase desapercibida (Kent & Souppaya, 2006).

En el caso del Análisis, constituye un reto ya que, el nivel de minuciosidad que requiere, ha provocado que se lleve a cabo como resultado de la ocurrencia de incidentes de seguridad. Las herramientas de analítica en tiempo real no abarcan toda la heterogeneidad de las infraestructuras a considerar en las organizaciones. Este tratamiento reactivo puede provocar pérdidas a las organizaciones. (Kent & Souppaya, 2006).

En el análisis realizado, no se evidenció consenso respecto a las pautas de registro para sistemas comerciales y de código abierto como parte del proceso de desarrollo de software. En estas soluciones, los registros generados se basan solamente en función de la experiencia del dominio de los desarrolladores. Además, a medida que el código de registro, se mezcla con el código fuente, es muy difícil mantener y actualizar el código de registro junto con el código de función para sistemas en constante evolución (Chen, 2019).

Proceso de planeación de la gestión de registros

Con respecto a la fase de planeación, como parte de la gestión de registros de auditoría, se evidenció que, para lograr el éxito de las organizaciones en la gestión de registros de auditoría, es importante que se tengan en cuenta un conjunto de elementos que impactan en el resultado final. Durante el proceso de planeación de la gestión de registros se deben considerar los siguientes elementos (Kent & Souppaya, 2006):

1. Definición de roles y responsabilidades de los individuos que se esperan, estén involucrados de la gestión de registros.
2. Establecimientos de políticas que incluyan las etapas de generación, transmisión, almacenamiento y monitoreo de registros.
3. Aseguramiento de la factibilidad para las organizaciones de las políticas establecidas.
4. Diseño de una infraestructura para la gestión de registros.

Consideraciones para diseño de infraestructura de la gestión de registros de auditoría

Los marcos de referencia consultados coinciden en que la gestión de registros de auditoría incluye las siguientes capas: Generación, Procesamiento ,Almacenamiento y Monitoreo de registros (Anton, 2013) (Kent & Souppaya, 2006). Como parte del diseño de la infraestructura, una de los primeros puntos que se deben establecer, durante la fase inicial del proyecto, son los roles y las responsabilidades de cada una de las personas involucradas en la gestión de registros. En empresas de desarrollo pequeñas puede ocurrir que el desarrollador de software sea también el arquitecto de la solución y a la vez, la persona encargada de brindar el soporte a la aplicación. Un entorno como este, puede traer problemas teniendo en cuenta la necesidad de separación de las responsabilidades (Anton, 2013).

La visión que se puede tener de un sistema es limitada por la información que se recolecta de dicho sistema y por el tiempo que es conservada (Anton, 2013). Por esta razón, las organizaciones deben ser capaces de desarrollar políticas que definan los requisitos obligatorios y las recomendaciones sugeridas para varios aspectos de la gestión de registros, incluidos los tipos de eventos que deben registrar cada componente, las datos (campos) que se deben registrar de cada tipo de evento y la frecuencia con que cada tipo de evento debe generar registros (Kent & Souppaya, 2006).

En los equipos de desarrollo de software, los arquitectos y desarrolladores, deben ser capaces de generar registros sobre la actividad de los usuarios sobre el sistema ya que el registro de la infraestructura desde dispositivos de red y sistemas operativos no será suficiente para detectar e investigar amenazas a nivel de aplicación. Los equipos de seguridad deben de guiar a los desarrolladores y arquitectos en el proceso de generación de registro para garantizar que sean útiles y efectivos en las fases posteriores (Anton, 2013).

Actualmente, no existe un recurso centralizado para guiar a los desarrolladores de software en la implementación de mecanismos de registro de actividad del usuario que permitan capturar, de forma consistente los eventos necesarios para realizar un análisis forense de dicha actividad.

Durante la generación de los registros, se debe tener en cuenta que, si bien es cierto que muchos estándares, buenas prácticas y normas, proponen que se deben registrar todas las peticiones del usuario y las respuestas del servidor, no

se debe confundir con registrar todos los detalles de estas peticiones ya que los registros de auditoría no deben contener más información que la necesaria (Eds & Steffen, 2018).

Existen un grupo de valores que no deben formar parte de los registros generados con fines de auditoría, por ejemplo, contraseñas, números de seguridad social, cumpleaños, números de teléfono, nombre completo, números de tarjetas bancarias, información genética o biométrica de la persona (Anton, 2013)(OSWAP, 2019). Los datos de las personas almacenados en los registros, deben contener la información mínima que permita identificarla en el sistema.

Un elemento importante durante la gestión de los registros de auditoría, es conocer su clasificación, lo cual permite generar un tratamiento específico de acuerdo al tipo de registro generado. Aunque el proceso de clasificación ocurre posterior a la generación, es importante conocer de antemano los posibles criterios que permiten clasificar los registros de auditoría. La clasificación puede realizarse ateniendo a múltiples criterios como fuente de origen, contenido, prioridad o función.

Uno de los aspectos más importantes para generar información útil de las aplicaciones para detectar o resolver un incidente de seguridad, es identificar los eventos que deben generar dicha información. Producir una cantidad excesiva de registros puede impactar significativamente en los propios sistemas y en la infraestructura. Según el análisis realizado a partir de las distintas normas, guías buenas prácticas y controles, se presentan en la **Tabla 3**, un grupo de eventos relevantes de acuerdo a su presencia en los documentos analizados.

Tabla 3 Grupo de eventos relevantes según normas, guías, buenas prácticas o controles

Eventos relevantes	Normas, guías, buenas prácticas o controles
Peticiones de clientes y respuestas del servidor.	PCI DSS; SP-800-92;OWASP Logging Guide; ISO/IEC 27001
Actividades con las cuentas de los usuarios.	ISO/IEC 27001;HITRUST CSF;OWASP Logging Guide; PCI DSS; SP-800-92
Acciones operacionales significativas.	HITRUST CSF; ISO/IEC 27001;OWASP Logging Guide; SP-800-92;
Acciones con privilegio de administración.	PCI DSS; ISO/IEC 27001;HITRUST CSF;
Creación, modificación y eliminación de los objetos a nivel de sistema.	PCI DSS; HITRUST CSF; ISO/IEC 27001

Además de estos grupos de eventos relevantes presentados, se propone que se registre información de los intentos de acceso a información no autorizada y errores en la entrada de datos en la interfaz de usuario, los cuales pueden ser indicios de un intento de ataque al sistema.

Las organizaciones deben tomar en consideración que se debe limitar la información de auditoría solo a la información que es necesaria para requisitos de auditoría específicos. Esto contribuye a un mejor desempeño ya que no se incluyen datos que pudieran dificultar la localización de información de interés para resolver o detectar un

problema(Ross, 2014). Además, disminuye el riesgo de presentar dificultades en el almacenamiento y mejora la eficiencia del procesamiento realizado para el análisis de los registros.

Cada registro generado debe responder a cuándo, donde, quién y qué operación se realizó sobre el sistema. Generar información que responda a estas preguntas aumenta la posibilidad de identificar anomalías o correlaciones entre diferentes registros de dispositivos(Breier & Branišová, 2017). En la **Tabla 4** se relacionan los campos de eventos que responden a estas preguntas con los estándares, guías o controles que lo proponen.

Tabla 4 Campos de eventos según estándares, controles y guías

Responde a	Campos	SP 800 53	PCI DSS	CISCSC	HITRUST CSF
Cuándo	Fecha/Hora del evento	X	X	X	X
Dónde	Recurso afectado	X	X	X	X
	Identificador de la aplicación/ dirección destino	X	-	X	-
Quién	Identificador de usuario	X	X	X	X
	Dirección IP/ Origen	X	X	X	X
Qué	Tipo del evento	-	X	-	X
	Descripción del evento	X	-	X	-
	Indicador de éxito o fallo	X	X	-	-

Al definir los eventos de interés y los atributos que debe contener cada registro, se garantiza que exista una trazabilidad de las acciones realizadas sobre el sistema. Una vez que los registros son generados, necesitan ser enviados a otro componente de la infraestructura para ser analizados y procesados. Para esto es imprescindible definir una estrategia de transporte que permita enviar los registros de forma segura desde los servidores donde son generados hasta los servidores donde serán procesados.

Las aplicaciones y sistemas utilizan diversas maneras para registrar y organizar sus registros. Sin embargo, para evitar que los desarrolladores de software tengan que diseñar sus propios sistemas de registro, se introdujeron algunos formatos de registro estándar. A continuación, se describen algunos de ellos:

Syslog

De acuerdo a la definición de este protocolo, el mensaje está formado por tres partes (GmbH, 2009); La cabecera (*header*), que representa la información del archivo de registros, por ejemplo, prioridad del registro, versión del protocolo, marca de tiempo, nombre del servidor, nombre de la aplicación, id del proceso e id del mensaje; los datos estructurados (*structure-data*), que puede contener información específica asociada al propio protocolo o a la

aplicación que genera el mensaje; y el mensaje (*message*) que contiene información sin formato establecido del evento que generó el registro.

Fluentd

Es un recopilador de datos de código abierto ampliamente utilizado. Su arquitectura, estructura los datos en formato *JSON* y proporciona la flexibilidad para procesar datos que podrían recopilar, filtrar, almacenar en búfer y enviar a otros destinos o fuentes (Kandan et al., 2017).

Advanced Message Queueing Protocol (AMQP)

El protocolo *AMQP*, es un estándar utilizado para la comunicación entre aplicaciones u organizaciones que ofrece seguridad a través de la autenticación y cifrado mediante *SASL* o *TLS* (*AMQP Protocol*, 2020). Se centra fundamentalmente en los entornos orientados a mensajes y puede considerarse como un protocolo de *middleware* orientado a mensajes. Funciona a través de un mecanismo de publicación/suscripción utilizando el protocolo *TCP* y la principal ventaja de este protocolo, es que permite almacenar los mensajes y enviarlos posteriormente, lo que proporciona confiabilidad incluso cuando hay interrupciones en la red (Mathkar et al., 2020).

No todos los registros generados por los sistemas deben ser procesados y almacenados por la infraestructura de gestión de registros. Solo se enviarán a la infraestructura de gestión de registros, las entradas que se consideren de interés. Generalmente, si los registros se almacenan en los servidores de infraestructura, se recomienda almacenarlos también a nivel del sistema (MinTIC, 2019).

Una vez transferidos los registros desde los sistemas hacia la infraestructura, se deben definir acciones para analizarlos y almacenarlos. El análisis de los registros de auditoría es el conjunto de acciones que se realizan para categorizar, normalizar y correlacionar los registros. Por otra parte, el almacenamiento detalla los elementos necesarios para preservar los registros, entre ellos, formato, tiempo de retención y protección de los registros generados.

La información generada, puede ser diferente dependiendo del sistema que genera la entrada de registro, pero no sólo en el formato, sino también en la cantidad. Resolver esta situación conlleva que sea necesario realizar un proceso de normalización y categorización de los registros para convertirlos en un formato estándar que pueda ser procesado por la infraestructura (Forsberg, 2018). Teniendo en cuenta la importancia de los registros, asociadas a la capacidad de mostrar las operaciones realizadas sobre un determinado entorno, y a ser empleados para esclarecer incidentes de seguridad informática, es importante proteger su integridad, disponibilidad y su confidencialidad.

Disponer de un único formato para los ficheros de registros facilita el proceso de análisis y revisión. En esta capa, es importante que el origen de los registros sea confiable, es decir que solo los eventos generados por los sistemas o

dispositivos autorizados, sean almacenados en un archivo de registro (Accorsi, 2013). Existen varios formatos disponibles para conservar los registros generados. Estos se pueden agrupar en registros basados en texto y binarios (Anton, 2013). Los registros basados en texto son los más utilizado debido al bajo costo que implica que los sistemas generen este tipo de registros y la existencia de frameworks en los distintos lenguajes de programación que facilitan la generación de registros en este formato.

A medida que un archivo de registro envejece, se vuelve menos relevante para los informes diarios y las tareas de revisión de registros, pero sigue siendo crítico para cumplir con el período de retención establecido y realizar análisis forense (Anton, 2013). Por este motivo, independientemente del formato de registro que se seleccione, se deberán comprimir las entradas antiguas para ahorrar espacio en disco. Los sistemas continuarán generando registros, el espacio de almacenamiento en dicho entorno disminuirá y será más difícil procesar los registros por su gran tamaño. Realizar la rotación de los ficheros, va a permitir mantener solo los registros más relevantes en el momento y almacenando los demás para conservarlos por el tiempo definido para cada sistema para realizar una mejor revisión de la información ya que el tamaño de los registros para analizar, es menor.

Existen varios esquemas de rotación de ficheros que pueden emplearse, basado en tiempo (cada hora, diariamente, semanalmente), basado en tamaño (MinTIC, 2019), o la combinación de ambos esquemas anteriores (Kent & Souppaya, 2006).

Entre las herramientas que se pueden emplear para la rotación de los ficheros, se encuentra *logrotate*, una utilidad presente en sistemas operativos Linux que ayuda a gestionar la rotación de los registros mediante la configuración de distintos parámetros (Both, 2020). Otra forma de ejecutarla es mediante tareas programadas en las cuales se pueden asociar *scripts* con las instrucciones necesarias para realizar la rotación de los ficheros.

El período de retención de los registros generados por las aplicaciones informáticas, es esencial para las investigaciones forenses y auditoría, así como para cumplir con normativas y regulaciones vigentes (Mirilla, 2019).

La cantidad de gigabytes necesaria para conservar los registros depende de los *RPS* generados, el tiempo durante el cual son generado en días y el $tamaño\ del\ registro$ .El cálculo se realiza mediante la **Ecuación 1** (paloaltonetworks, 2020):

$$GBs = \frac{[(RPS * 86400) * días] * tamaño\ del\ registro}{1000000000} \quad 1$$

En cuanto al valor de RPS se puede calcular mediante la Ecuación 2 (Rubier, 2015):

$$RPS = \frac{No.registros\ del\ sistema}{Tiempo\ de\ generación(segundos)} \quad 2$$

En la **Ecuación 2**, el $tiempo\ de\ generación$ representa el período, en segundos, durante el cual se generaron los registros y $no.registros\ del\ sistema$, hace referencia a la cantidad de registros generados en el tiempo definido. El espacio de almacenamiento puede reducirse si se comprimen los ficheros, en dicho caso, se debe tener en cuenta también la tasa de compresión.

La generación, procesamiento y almacenamiento de los registros no cumple ningún objetivo, si estos no son monitoreados. El proceso de monitoreo, cubre los aspectos relacionados con la interpretación de los eventos registrados y qué acciones se deben tomar como resultado de ese análisis. Para realizar el análisis de los datos relacionados con los registros operativos y los registros de seguridad, es muy conveniente emplear un *SIEM* (Center for Internet Security, 2019). En (Vazao et al., 2019)se analizan *OSSIM*, *ELK Stack*, *Splunk Free* y *Graylog* y se determina que en el caso de *OSSIM* y *Splunk Free*, no presentan mucha documentación, debido a que se priorizan sus versiones de pago. Por otra parte, *ELK Stack* y *Graylog* poseen más documentación, pero reconoce que también se requiere de investigaciones para resolver los problemas que puedan surgir durante su explotación.

Conclusiones

Una característica presente en el análisis de las regulaciones analizadas consiste en que todos los eventos de los sistemas deben generar registros de auditoría, además se deben conservar y analizar con el objetivo de detectar amenazas, ataques o resolver cualquier problema descubierto. Como práctica común en los artículos analizados, la gestión de los registros de auditoría se realiza de forma centralizada evitando que sea necesario consultar varios servidores para obtener la información necesaria para ejecutarlo y facilitando la reutilización de elementos dentro de la infraestructura de gestión de trazas como, por ejemplo, procedimientos para rotación, normalización y monitoreo de los registros.

Se pudo constatar que no existen muchos libros asociados a esta materia, sin embargo, si se pueden encontrar varios estándares que guían este proceso y un gran número de investigaciones teóricas y prácticas en dicha área; Los estudios analizados que reflejan la generación de información útil durante el desarrollo de un software, estaban mayormente orientados a información con fines de detección de errores en el código fuente. Por este motivo, se fundamenta la necesidad de realizar este tipo de estudio, enfocado en plantear una solución, que permita la generación, procesamiento, almacenamiento y monitoreo de los registros de auditoría con propósitos de seguridad y auditoría, y que pueda ser reutilizada por varias aplicaciones.

A partir del estudio de las regulaciones y artículos analizados, se pudieron identificar las etapas para la gestión de registros de auditoría, así como los principales elementos y acciones a considerar en cada etapa. En cuanto a la

planeación de los registros, durante la etapa de desarrollo de las soluciones, se identificaron un conjunto de roles que deben estar involucrados, los grupos de eventos que deben generar registros y los campos de eventos que deben contener cada registro generado.

Conflictos de intereses

Los autores de la presente investigación declaran que no poseen conflictos de intereses.

Contribución de los autores

Gilberto Enrique González Hidalgo: Ideas, Conceptualización, Investigación, Análisis formal, Redacción

Henry Raúl González Brito: Conceptualización, Redacción – revisión y edición, Análisis formal

Mónica Peña Casanova: Conceptualización, Redacción – revisión y edición, Análisis formal, Supervisión

Referencias

Accorsi, R. (2013). A secure log architecture to support remote auditing. *Mathematical and Computer Modelling*, *57*(7–8), 1578–1591. https://doi.org/10.1016/j.mcm.2012.06.035

All, T. (2019). *HITRUST- 9.3.1*. *November*.

AMQP Protocol. (2020). https://www.amqp.org

Anton, C. (2013). *Logging and Log Management*.

Both, D. (2020). *Using and Administering Linux* (Vol. 2). Apress. Https://doi.org/10.1007/978-1-4842-5485-1

Breier, J., & Branišová, J. (2017). A Dynamic Rule Creation Based Anomaly Detection Method for Identifying Security Breaches in Log Records. *Wireless Personal Communications*, *94*(3), 497–511. https://doi.org/10.1007/s11277-015-3128-1

Center for Internet Security. (2019). CIS Controls. *Center for Internet Security*, *7.1*. Https://www.cisecurity.org/

Chen, B. (2019). Improving the Software Logging Practices in devops. *2019 IEEE/ACM 41st International Conference on Software Engineering: Companion Proceedings (ICSE-Companion)*, 194–197. https://doi.org/10.1109/ICSE-Companion.2019.00080

Chopra, A., & Chaudhary, M. (2020). Implementing an Information Security Management System. In *Implementing an Information Security Management System*. https://doi.org/10.1007/978-1-4842-5413-4

Eds, R. K., & Steffen, B. (2018). *Correct Audit Logging: Theory and Practice.*

Forsberg, J. (2018). *Implementation of Centralized Log Management Solution for Ensuring Privacy of Individuals as Required by EU Regulation*. *March*.

Gmbh, A. (2009). *The Syslog Protocol*. https://tools.ietf.org/html/rfc5424

Kandan, R., Khalid, M. F., Ismail, B. I., Goortani, E. M., Mydin, M. N. M., & Hoe, O. H. (2017). CLOF: A proposed containerized log management orchestration framework. *2017 IEEE Conference on Open Systems (ICOS)*, *2018-Janua*, 13–16. https://doi.org/10.1109/ICOS.2017.8280266

Kent, K., & Souppaya, M. (2006). *Guide to Computer Security Log Management*.

Mathkar, S., Vernekar, N., & Jotkar, G. (2020). *Comparative Study of iot Protocols and Classification of Cloud Platforms*. *9*(6), 77–81.

MINCOM. (2019a). *Resolución 126*. *2*.

MINCOM. (2019b). *Resolución 128*. *2*.

Mintic. (2019). *Guía Técnica de Sistemas de Información - Trazabilidad*. 1–28. https://www.mintic.gov.co/arquitecturati/630/articles-9263_recurso_pdf.pdf

Mirilla, D. (2019). *Slow Incident Response in Cyber Security: The Impact of Task Disengagement in Security Operations Centers*. *September*. https://www.researchgate.net/publication/335692568

OSWAP. (2019). *Logging Cheat Sheet*. https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html

Otto, M. (2018). General Data Protection Regulation – GDPR. In *International and European Labour Law* (Vol. 2014, Issue March 2014, pp. 958–981). https://doi.org/10.5771/9783845266190-974

OWASP. (n.d.). *OWASP Logging Guide*. Retrieved October 20, 2020, from https://owasp.org/www-pdf-archive/OWASP_Logging_Guide.pdf

Paloaltonetworks. (2020). *Sizing Storage for the Logging Service*. https://knowledgebase.paloaltonetworks.com/kcsarticledetail?Id=ka10g000000clvmca0

PCI Security Standards Council. (2018). *PCI-DSS - Requirements and Security Assessment Procedures*. *3.2.1*, 1–139.

Ross, R. S. (2014). Assessing Security and Privacy Controls in Federal Information Systems and Organizations: In *NIST SP-800-53 Ar*. https://doi.org/10.6028/NIST.SP.800-53Ar4

Rubier, J. P. (2015). *Marco de trabajo para la gestión centralizada de trazas de seguridad utilizando herramientas de código abierto*. *151*, 919–928.

Stock, A. Van der, Glas, B., Smithline, N., & Gigler, T. (2017). *Owasp Top 10*. Https://owasp.org

UCI. (2020). *UCI*. http://www.uci.cu/investigacion-y-desarrollo/centros-de-desarrollo

Vazao, A., Santos, L., Piedade, M. B., & Rabadao, C. (2019). SIEM Open Source Solutions: A Comparative Study. *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, *2019-June*, 1–5. https://doi.org/10.23919/CISTI.2019.8760980