ES COPIA AUTENTICADA

ROGER A. SICCHA MARTINEZ
Director General
Oficina General de Administración
MINISTERIO DE ECONOMÍA Y FINANZAS

11 DIC. 2014

REPÚBLICA DEL PERÚ

Resolución Directoral

Lima, 11 de diciembre de 2014 N° 424-2014-EF/43.01

CONSIDERANDO:

Que, de conformidad al literal g) del artículo 64 del Reglamento de Organización y Funciones del Ministerio de Economía y Finanzas, aprobado mediante Decreto Supremo N° 117-2014-EF, se establece que corresponde a la Oficina General de Tecnologías de la Información, administrar la infraestructura tecnológica informática y de comunicación de datos del Ministerio, garantizando su operatividad, disponibilidad y seguridad;

Que, el numeral 5.4 del Manual de Políticas de Gestión de la Tecnologías de la Información del MEF, aprobado mediante Resolución Directoral N° 160-2014-EF/43.01, de fecha 02 de mayo de 2014, establece que la Oficina General de Tecnologías de la Información, debe contemplar la factibilidad de activar registros de auditoría en sistemas operativos, base de datos y sistemas de información que sirvan para la investigación del comportamiento en la utilización o acceso a estos recursos tecnológicos;

Que, mediante Resolución Ministerial N° 223-2013-EF/41, se incorpora en la Directiva N° 004-2012-EF/41.02 "Lineamientos para la elaboración de Directivas en el Ministerio de Economía y Finanzas", aprobada con Resolución Ministerial N° 359-2012-EF/41, el numeral 5.5 concerniente a la aprobación de documentos técnicos normativos que no sean directivas internas, tales como Manuales, Instructivos y otros de similar naturaleza, que emitan o propongan los órganos de administración interna, en materias de sus respectivas competencias para ser aprobados por el Director General de la Oficina General de Administración;

Que, en ese sentido resulta necesario aprobar los "Lineamientos para la Gestión de los Registros de Auditoría en la Infraestructura Tecnológica del MEF";

De conformidad con lo dispuesto en el Reglamento de Organización y Funciones del Ministerio de Economía y Finanzas, aprobado con Decreto Supremo N° 117-2014-EF/43, y en la Resolución Ministerial N° 223-2013-EF/41.

SE RESUELVE:

Artículo 1.- Aprobar los "Lineamientos para la Gestión de los Registros de Auditoría en la Infraestructura Tecnológica del MEF", que en anexo forma parte integrante de la presente resolución.

Artículo 2.- Publicar la presente resolución en el Portal Institucional del Ministerio de Economía y Finanzas (www.mef.gob.pe), en el Intranet del Ministerio de Economía y Finanzas y disponer su difusión a todo el personal del MEF mediante correo electrónico.

Regístrese y comuníquese.

ROGER A. SICCHA MARTÍNEZ
Director General
Oficina General de Administración

MINISTERIO DE ECONOMÍA Y FINANZAS
Oficina General de Tecnologías de la Información

LINEAMIENTOS PARA LA GESTIÓN DE LOS REGISTROS DE AUDITORIA EN LA INFRAESTRUCTURA TÉCNOLÓGICA DEL MEF

1. OBJETO

Establecer los lineamientos para la gestión efectiva de los registros de auditoría de la infraestructura tecnológica del MEF, a fin de detectar eventos relacionados a la seguridad de la información y de la operatividad de los recursos o aplicaciones tecnológicas.

2. BASE LEGAL

2.1. Ley N° 27785 Ley Orgánica del Sistema Nacional de Control.

2.2. Decreto Supremo N° 117-2014-EF, que aprueba el Reglamento de Organización y Funciones del Ministerio de Economía y Finanzas.

2.3. Resolución de Contraloría N° 320-2006-CG, "Normas de Control Interno".

2.4. Resolución Ministerial N° 246-2007-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007EDI.Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2da Edición".

2.5. Resolución Directoral N° 160-2014-EF/43.01, que aprueba el "Manual de Políticas de Gestión de Tecnologías de la Información del Ministerio de Economía y Finanzas".

3. ALCANCE

Las disposiciones contenidas en el presente documento son de aplicación obligatoria por la Oficina de Infraestructura Tecnológica de la Oficina General de Tecnologías de la Información – OGTI.

4. DISPOSICIONES GENERALES

4.1. DEFINICIONES

4.1.1. *Correlación de registros de auditoría*: consiste en la toma de datos de múltiples fuentes y analizarlos en conjunto.

4.1.2. *Eventos*: acciones, transacciones u operaciones auditables que se han ejecutado en un recurso o aplicación informática.

4.1.3. *Incidente de seguridad*: cualquier hecho que podría afectar la confidencialidad, integridad y disponibilidad de la información registrada en los recursos informáticos del MEF.

4.1.4. *Registros de auditoría:* información o pista de auditoria de eventos secuenciales producidos por los recursos o aplicaciones tecnológicas, que permite rastrear, analizar y determinar la causa raíz de lo reportado; estando éstos registros contenidos en archivos protegidos contra escritura.

4.1.5. *Servidor:* un servidor es una computadora que maneja peticiones de data, email, almacenamiento, servicios de redes y transferencia de archivos de otras computadoras (clientes).

4.2. El proceso de la Gestión de los Registros de Auditoría en la Infraestructura Tecnológica comprende las fases de generación, almacenamiento,

monitoreo, análisis y evaluación de los registros de auditoría producidos por los eventos de la infraestructura tecnológica del MEF.

4.3. La OGTI debe contar con la infraestructura tecnológica necesaria y en óptimas condiciones para dar soporte a los procedimientos de almacenamiento, análisis y evaluación de los registros de auditoría, con el fin de identificar los recursos informáticos con fallas, de bajo rendimiento o inseguros.

4.4. Los procesos que gestiona los registros de auditoría de la infraestructura tecnológica del MEF, deben estar debidamente documentados.

5. DISPOSICIONES ESPECÍFICAS

5.1. La Oficina General de Tecnologías de la Información, es el órgano encargado de la Gestión de los Registros de Auditoría en la Infraestructura Tecnológica del MEF, debiendo para ello conducir y cumplir las siguientes disposiciones:

a) Evaluar y definir las características de los registros de auditoría de la infraestructura tecnológica del MEF.

b) Registrar los eventos efectuados por la tecnología informática en las pistas de auditoría establecidas y garantizar que se almacenen con el detalle requerido y por el tiempo de retención establecido.

c) Supervisar y proteger los registros de auditoría generados por los eventos de seguridad de la información, de los recursos tecnológicos, sistemas de información y de las aplicaciones informáticas.

d) Detectar actividades no autorizadas o de uso incorrecto de los recursos y aplicaciones informáticas (incidentes relacionados a intentos para eludir mecanismos de seguridad, violaciones de políticas, actividades fraudulentas o similares).

e) De ser el caso, establecer los mecanismos de enmienda en la infraestructura tecnológica, como producto de las acciones de detección, análisis y evaluación de los registros de auditoría de la infraestructura tecnológica del MEF.

5.2. Para mantener el óptimo funcionamiento de la infraestructura tecnológica que da soporte a la Gestión de los Registros de Auditoría de la Infraestructura Tecnológica del MEF, la OGTI establece los roles y responsabilidades del personal para administrar, operar y mantener la infraestructura tecnológica, alineándose de ese modo a lo dispuesto en las normas técnicas de la seguridad de la información.

5.3. DE LA GENERACIÓN DE LOS REGISTROS DE AUDITORÍA

5.3.1. La OGTI determina la infraestructura tecnológica sobre la que se gestionarán los registros de auditoría, priorizando a la infraestructura tecnológica de soporte a los servicios de tecnología y sistemas de información contenidos en el Plan de Continuidad de Negocio del MEF a cargo de la Dirección de

MINISTERIO DE ECONOMÍA Y FINANZAS
Oficina de Gobierno de Tecnologías

Gestión de Riesgos de la Dirección General de Endeudamiento y Tesoro Público.

5.3.2. La OGTI establece las fuentes de datos para los registros de auditoría a gestionar, tales como:

a) Sistemas Operativos de servidores.

b) Dispositivos o herramientas de redes y seguridad (firewall, anti spam, etc.), para detectar actividades maliciosas, proteger los sistemas y datos, y apoyar los esfuerzos de respuesta a incidentes.

c) Los servicios informáticos implementados, como el correo electrónico, base de datos, directorio activo, servidor de archivos, etc.

d) Las aplicaciones o sistemas de información implementadas en la red del MEF.

Las fuentes de datos a capturar deben contener información sobre:

- Eventos referidos a la operatividad del sistema.
- Eventos de seguridad, como intentos exitosos y fallidos de autenticación, cambios en las configuraciones, etc.

5.3.3. Los registros de auditoría deben contemplar, como mínimo, la siguiente estructura de datos:

a) Fecha y hora; cuando ocurrió el evento que debe estar sincronizado en toda la infraestructura tecnológica que la produce.
b) Tipo de evento; clasificación que establece la OGTI de acuerdo a las fuentes de datos y a la actividad que realiza el recurso informático.
c) Resultado de la acción: siendo ésta de éxito o error. En este último caso, indicar el detalle o código de error asociado.
d) Trazabilidad del evento: información que contiene las direcciones de la red, protocolos, nombre de máquina o terminal de origen y/o destino asociado.
e) Identificación del sistema: Indicar el nombre del sistema, aplicación y/o módulo que generó el evento.
f) Identificación de usuario que generó el evento.
g) Componentes de sistemas o recursos tecnológicos afectados o relacionados.

5.3.4. Los sistemas de información desarrollados por la OGTI que vienen ejecutándose y no han incorporado registros de auditoría en su desarrollo, deben ser evaluados y de ser necesario, adecuarlos paulatinamente para incorporar esta funcionalidad con el objeto de que se cumplan las normas establecidas de seguridad de la información.

MINISTERIO DE ECONOMÍA Y FINANZAS
Oficina de Gobierno de Tecnologías

5.4. DE LA INFRAESTRUCTURA TECNOLÓGICA PARA LA GESTIÓN DE LOS REGISTROS DE AUDITORÍA

5.4.1. La OGTI establece la infraestructura tecnológica a emplearse para la gestión de los registros de auditoría, de acuerdo a criterios, tales como, espacio de almacenamiento, capacidad de procesamiento y tiempo adicional de procesamiento que se requiere para el uso de esta funcionalidad.

5.4.2. La OGTI debe asegurar que la infraestructura tecnológica donde se procesan y almacenan los registros de auditoría estén debidamente protegidos contra la manipulación y accesos no autorizados.

5.4.3. La OGTI identifica, determina e implementa el recurso software a ser empleado para gestionar los registros de auditoría en la infraestructura tecnológica del MEF.

5.5. DE LA OPERATIVIDAD EN LA GESTIÓN DE LOS REGISTROS DE AUDITORÍA

5.5.1. La OGTI configura las fuentes de datos que intervienen en la gestión de los registros de auditoría, asegurando que estén sincronizadas con una fuente de hora precisa, lo cual permite la correlación de eventos de los registros de auditoría.

5.5.2. La OGTI debe implementar procedimientos para el monitoreo de los registros de auditoría implementados para verificar el correcto funcionamiento de los servicios y la conformidad en el cumplimiento de las políticas de seguridad de información establecidas.

5.5.3. La OGTI define el método y el procedimiento del almacenamiento de los registros de auditoría, basado en la infraestructura tecnológica implementada para la gestión de los registros de auditoría y al tiempo de almacenaje de los registros según las disposiciones que se establezcan para este fin.

5.5.4. El personal de la OGTI dispuesto para la operatividad de la gestión de los registros de auditoría, monitorea el funcionamiento correcto de la infraestructura con la que se gestionan los registros de auditoria, realizando acciones correctivas si estas presentan problemas en su funcionamiento. Ante cualquier falla o problema presentado se informa al Director de la Oficina de Tecnología de la Información de la OGTI, para que gestione la adquisición del mantenimiento correctivo de los recursos afectados.

5.5.5. El análisis de los registros de auditoría se realiza ante eventos que afecten los servicios o ante situaciones de comportamientos anómalos, siendo los objetivos principales:

a) Detectar los aspectos negativos que hayan afectado a los sistemas: errores, inconsistencias o hechos que comprometan la seguridad.

MINISTERIO DE ECONOMÍA Y FINANZAS · REPÚBLICA DEL PERÚ · Oficina de Gobierno de Tecnologías

b) Identificar el origen de las fallas operacionales o de seguridad, evaluar su criticidad y dictar las medidas pertinentes tanto para solucionar los eventos que tuvieron lugar, como para recomendar las acciones necesarias para evitar o controlar posibles hechos similares en el futuro.

c) Predecir el comportamiento de los sistemas y/o recursos bajo ciertos parámetros, por ejemplo su rendimiento ante una gran cantidad de operaciones ejecutadas concurrentemente.

6. RESPONSABILIDADES

6.1. La OGTI a través de la Oficina de Infraestructura Tecnológica es la responsable de difundir, implementar y cumplir con lo dispuesto en el presente documento.

6.2. La Oficina de Sistemas de Información de la OGTI es responsable de evaluar la necesidad de que los sistemas de información que se implementen, cuenten con registros de auditoría.

7. DISPOSICIONES COMPLEMENTARIAS

7.1. La OGTI incorpora en su presupuesto anual los costos de implementación, mantenimiento y actualización de la infraestructura tecnológica y también del recurso humano necesario para mantener el proceso de Gestión de los Registros de Auditoría de la Infraestructura Tecnológica del MEF.

7.2. La OGTI proporciona información y asistencia técnica respecto a los datos contenidos en los registros de auditoria de la infraestructura tecnológica del Ministerio, como apoyo a las acciones de auditoría, análisis forense y gestión de incidentes de seguridad de la información.