Arquitectura TI COLOMBIA
MARCO DE REFERENCIA

vive digital Colombia

G.SIS.02 Guía Técnica de Sistemas de Información - Trazabilidad

Guía Técnica

Versión 1.0

30 de diciembre de 2014

Sistemas de Información

MINTIC

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0	30/12/2014	Emisión

DERECHOS DE AUTOR

AUTORA

María Isabel Mejía Jaramillo
Viceministra de Tecnologías y Sistemas de la Información
Ministerio de Tecnologías de la Información y las Comunicaciones

COLABORADORES

Jorge Fernando Lobo Bejarano
Director de la Dirección de Estándares y Arquitectura de TI
Ministerio de Tecnologías de la Información y las Comunicaciones

Asesores del Ministerio de Tecnologías de la Información y las Comunicaciones
Claudia Milena Rodríguez Álvarez
Lina Marcela Morales

Asesores de la Corporación Colombia Digital
Javier Orlando Torres Páez
Deicy Alexandra Parra Chaux
Diego Antonio Campos Cáceres
Jorge Alberto Villalobos Salcedo
Diana Piedad Gómez Castaño
Javier Alexander Mayorga Melo
Jaime Leonardo Bernal Pulido
Hermes Camilo Cubaque Barrera
Leydi Viviana Cristancho Cruz

Medios Digitales
María Astrid Toscano Villán
Ricardo Rojas Ortíz
Jhon Henry Munevar Jiménez

UT Everis Tecnocom
Alberto Pizarro Carrasco
Gerardo Antonio Moreno
Martha Lucía Parra
Martha Patricia Naranjo Becerra
David Fernando de la Peña Santana
Lucio Augusto Molina Focazzio
Silvia María Fernández Coello
Karin Xiomara Marroquín
Maribel Ariza Rojas
Ramiro Andrés Delvasto
Diego Ordóñez
Édgar Esquiaqui
Ricardo Abad Chacón Ibarra
Juliana Botero Iragorri
Juan Pablo Sequera España

TABLA DE CONTENIDO

PÁG.

LISTA DE IMÁGENES

PÁG.

LISTA DE TABLAS

PÁG.

ABREVIATURAS Y ACRÓNIMOS

Abreviatura / Acrónimo	Descripción
AE	Arquitectura Empresarial
CSV	Registros Separados por Coma (Comma-Separated Values).
IP	Protocolo de Internet (Protocol Internet).
IPSec	Seguridad del Protocolo de Internet (Internet Protocol Security).
JSON	Notación de Objetos JavaScript (JavaScript Object Notation).
NIST	Instituto Nacional de Estándares y Tecnología del Departamento de Comercio de Estados Unidos. (National Institute of Standards and Technology. U.S. Department of Commerce).
SAN	Red de Área de Almacenamiento (Storage Area Network).
SHA	Algoritmo de Seguridad para Cálculo de Hash (Secure Hash Algorithm).
SIEM	Sistemas de Gestión de Eventos e Información de Seguridad (Security Information and Event Management).
SIS-INF	Sistemas de Información.
XML	Lenguaje de Marcas Extensible (Extensible Markup Language).

INTRODUCCIÓN

A partir del análisis de las diferentes fuentes de información, en donde una muestra significativa de entidades del Estado colombiano expresan sus inquietudes respecto a la gestión de las Tecnologías de la Información (TI), se identifica su preocupación por contar con directrices referentes al manejo de los registros de errores, eventos y trazabilidad de sus SIS-INF.

A continuación se presentan los objetivos y el alcance de la presente especificación, así mismo se identifican los lineamientos del Marco de Referencia de Arquitectura Empresarial (AE) para la gestión de TI, que apoya la misma.

OBJETIVOS

- Definir la clasificación de los diferentes tipos de mensajes de error y trazabilidad que deben registrar los SIS-INF, con el fin de facilitar la identificación, selección y priorización de la información necesaria para los procesos de monitoreo, gestión de incidentes e identificación de mejoras.
- Establecer la información mínima básica que debe registrarse para la identificación adecuada de los eventos y excepciones generadas por los SIS-INF de la entidad.
- Identificar mejores prácticas y recomendaciones para realizar una adecuada gestión del registro de eventos.

ALCANCE DE LA GUÍA TÉCNICA

- Proponer la estandarización del registro de mensajes de errores, excepciones, eventos de seguridad y trazabilidad, que deben registrar los Sistemas de información (SIS-INF) de las entidades del Estado colombiano.
- Relacionar buenas prácticas y sugerencias para la gestión de la información de eventos y trazabilidad, con el fin de apoyar los procesos de monitoreo, control correctivo e identificación de mejoras dentro de la gestión de los SIS-INF realizada por las entidades.

LINEAMIENTOS DEL MARCO DE REFERENCIA DE AE ASOCIADOS

El siguiente lineamiento del dominio de Sistemas de Información del Marco de Referencia de Arquitectura Empresarial (AE) para la gestión de TI, es apoyado de manera directa por la especificación:

Auditoría y trazabilidad de los Sistemas de Información (LI.SI.23).

DESCRIPCIÓN

Contar con un formato común para el registro de logs de eventos y trazabilidad junto con criterios unificados para la gestión y protección de dichos registros, facilita la consolidación de logs generados por diferentes SIS-INF, así como su posterior análisis y revisión, lo cual permitirá identificar problemas operativos, incidentes de seguridad, entre otros eventos relevantes para la entidad, y recopilar información útil para la resolución de dichos problemas.

Adicionalmente la adecuada gestión de los logs servirá de soporte en procesos de monitoreo, control de calidad, mejora continua, análisis forense, investigaciones internas, etc.; teniendo en cuenta que la normatividad del Estado colombiano a partir de la Ley 87 del 29 Noviembre de 1993 en su artículo 4, define como elemento para el sistema de control interno el "Establecimiento de sistemas modernos de información que faciliten la gestión y el control" en las entidades.

El Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST), define, en su publicación SP-800-92 [5], la gestión de eventos como "el proceso para generar, transmitir, almacenar, analizar y desechar los datos del log de seguridad". Esta definición se puede generalizar a cualquier log generado por un sistema, aplicación o SIS-INF.

En este capítulo se presenta la estructura propuesta para el registro de mensajes, así como aspectos de almacenamiento, seguridad y consideraciones adicionales respecto a la gestión de esta información.

1.1. Estructura para el registro de mensajes

A continuación se describe la estructura propuesta para la estandarización de los mensajes de errores, excepciones, eventos y trazabilidad, que deben registrar los SIS-INF de las entidades.

La estructura sugerida contiene los siguientes campos:

Fecha y hora	IP origen	Entidad origen	SIS-INF	Usuario	Tipo de mensaje	Contenido según el tipo de mensaje

Imagen 1. Estructura para el registro de mensajes

Fuente. Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic.

- Fecha y hora: YYYY-MM-DD HH24: MI:SS
- IP Origen: dirección IP del host en donde se origina el evento o acción que genera el mensaje.
- Entidad origen: cuando el mensaje a registrar se genera a partir del intercambio de información entre dos entidades, se requiere identificar cuál es la entidad consumidora del servicio.
- Usuario: usuario que realizó la operación que genera el mensaje
- SIS-INF: identificador del sistema de información que genera el mensaje
- Tipo de mensaje: código que permite identificar los tipos de mensajes
- Contenido del mensaje: cuerpo del mensaje, relativo a su tipificación

1.2. Tipos de mensajes

Para definir la tipificación de los mensajes, se tiene en cuenta la siguiente clasificación de la información a registrar:

- Eventos propios del funcionamiento del SIS-INF
- Eventos relacionados con la seguridad de la información y el SIS-INF
- Trazabilidad de transacciones y de información funcional del SIS-INF

1.3. Eventos del sistema de información

En la siguiente tabla se describen los tipos de mensaje para registrar los eventos propios del sistema de información, los cuales se generan durante la operación del mismo:

Tipo	Código	Descripción
Errores	<ERROR>	Errores no recuperables del SIS-INF
Excepciones	<EXCEP>	Excepciones del SI, que afectan su rendimiento

		o la disponibilidad de funcionalidades críticas
Advertencias	<WARNING>	Comportamientos atípicos del SIS-INF, cambios en la configuración, etc.
Depuración	<DEBUG>	Información de seguimiento de nuevas funcionalidades, o para evaluar el comportamiento de operaciones críticas del SIS-INF.
Información	<INFO>	Información relacionada a requerimientos no funcionales, como eventos de reinicio, inventario de componentes disponibles, etc.

Tabla 1. Eventos del sistema de información

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic).

La información contenida en el cuerpo del mensaje de los eventos del SIS-INF, debe contemplar:

- Identificación del componente o del paquete de *software*
- Funcionalidad u operación que se está ejecutando
- Posible causa del error y demás información para realizar el correspondiente análisis

1.4. Eventos de seguridad de la Información

El estándar ISO/IEC 27002:2013 *Information Technology – Security Techniques – Code of Practice for Information Security Controls* [4], en su numeral 12.4 hace referencia a que "Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información". En dicho numeral se mencionan los campos del log que se deben considerar, donde sea pertinente. La estructura propuesta en la sección 2.1 del presente documento, tiene en cuenta las directrices del estándar mencionado.

A continuación se presentan los tipos de mensajes propuestos para registrar los eventos de seguridad que son generados por los SIS-INF de la entidad, estos eventos dependen de los controles de seguridad de la información que se encuentren implementados en los SIS-INF mencionados.

Dentro de estos eventos de seguridad no se contemplan los mensajes de trazabilidad generados por componentes de *software* específico que implementen controles de seguridad determinados, pues es posible que estos componentes cuenten con una estructura para el registro de mensajes de log ya definida.

Tipo	Código	Descripción
Errores	<ERROR>	Errores no recuperables del SIS-INF
Excepciones	<EXCEP>	Excepciones del SI, que afectan su rendimiento o la disponibilidad de funcionalidades críticas.
Advertencias	<WARNING>	Comportamientos atípicos del SIS-INF, cambios en la configuración, etc.
Depuración	<DEBUG>	Información de seguimiento de nuevas funcionalidades, o para evaluar el comportamiento de operaciones críticas del SIS-INF.
Información	<INFO>	Información relacionada a requerimientos no funcionales, como eventos de reinicio, inventario de componentes disponibles, etc.

Tabla 2. Eventos de seguridad de la información

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic).

La información contenida en el cuerpo del mensaje de los eventos de seguridad, debe contemplar:

- Identificación del tipo de información y componente del SIS-INF involucrado en el evento de seguridad a registrar
- Descripción del evento de seguridad que se presenta

- Información que el SIS-INF pueda recopilar para realizar el correspondiente análisis

1.5. Trazabilidad de transacciones e información funcional

En la siguiente tabla se presentan los mensajes e información de trazabilidad que el SIS-INF debe registrar, y que servirá de insumo para los controles de auditoría y seguimiento de las operaciones críticas de los procesos de negocio de la entidad:

Tipo	Código	Descripción
Consulta	<CONS>	Acción de consulta de información a través del SIS-INF.
Creación	<INS>	Acción de registro de datos y/o información a través del SIS-INF.
Modificación	<MOD>	Acción de modificación de los datos y/o información a través del SIS-INF.
Eliminación	<DEL>	Acción de eliminación de datos y/o información a través del SIS-INF.
Seguimiento	<TRACE>	Información asociada al seguimiento de una operación o transacción determinada.

Tabla 3. Trazabilidad de transacciones e información funcional

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic).

La información contenida en el cuerpo de los mensajes de trazabilidad, debe contemplar:

- Identificación del tipo de información o componente del SIS-INF al que se le está realizando el seguimiento.
- Identificación de la información que se modifica o elimina, acorde al tipo de mensaje.
- Detalle de la información relativa a las operaciones y funcionalidades críticas a las que se requiere hacer seguimiento.
- Información adicional a criterio y necesidades de la entidad.

1.6. Almacenamiento

El registro de eventos puede realizarse en archivos y en tablas de bases de datos, para lo cual se pueden tener en cuenta los siguientes formatos de almacenamiento:

- Lenguaje de Marcas Extensible – XML (*Extensible Markup Language*) [8]: es un lenguaje de etiquetado extensible que permite definir etiquetas personalizadas para describir y organizar datos; XML es un estándar internacional y es ampliamente utilizado en el intercambio de información.

  A continuación se presentan un ejemplo de la notación XML:

```
<?xml version="1.0" encoding="UTF-8"?>
<MENSAJE fechahora="2014-08-20 14:00:00">
    ...
    <Usuario>FMartinez</Usuario>
    <TipoMensaje>ERROR</TipoMensaje>
    ...
</MENSAJE>
```

Imagen 2. Ejemplo de notación XML

Fuente. Ministerio de Tecnologías de la Información y las Comunicaciones.

La Universidad de Eindhoven en Noruega, ha definido el XES – Extensible Stream Standard [1], un metalenguaje para registrar eventos y mensajes de trazabilidad basado en lenguaje XML.

El lenguaje XML es extensible y permite la definición de la estructura de los datos, así como su validación, es fácil de procesar, validar y analizar sintácticamente, su estructura permite separar el contenido del formato de presentación; sin embargo una de las posibles desventajas que puede presentar el uso de XML para el registro de los mensajes de errores y trazabilidad, es que puede llegar a ocupar un espacio de almacenamiento considerable.

- Notación de Objetos JavaScript – JSON (JavaScript Object Notation) [7]: es un formato de texto ligero para el intercambio y registro de datos, basado en

subconjunto de los objetos de Javascript; está constituido por dos estructuras: Una colección de pares "nombre:valor", y una lista ordenada de valores.

A continuación se presenta un ejemplo de la notación JSON:

```
{
….
"Usuario": "FMartinez",
"TipoMensaje":"ERROR"
…
}
```

Imagen 3. Ejemplo de notación JSON

Fuente. Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic).

JSON es simple de generar e interpretar y puede ser leído por cualquier lenguaje de programación; es sencillo construir un analizador sintáctico de JSON, esta notación se ha constituido como una alternativa al uso de XML.

- Archivos con registros separados por coma - CSV (Comma-Separated Values) [9]: es un formato de texto sencillo para representar datos en forma de tabla; cada registro corresponde a una línea, las líneas se separan entre sí a través de retorno de carro, en cada línea los campos se separan por comas.

A continuación se presenta un ejemplo del formato CSV:

```
FechaHora,Usuario,TipoMensaje
"2014-08-20 14:00:00","FMartinez","ERROR"
"2014-08-20 14:00:00","FMartinez","ERROR"
```

Imagen 4. Ejemplo de formato CSV

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic).

El formato CSV es sencillo de generar e interpretar automáticamente, y no ocupa espacio significativo comparado con otro tipo de formatos, sin embargo no es extensible y no permite definir formatos ni validaciones.

- Archivos de texto plano: Es común encontrar productos y aplicaciones del mercado que registran sus mensajes de errores y depuración en archivos de texto plano.

A continuación se presenta un ejemplo de un archivo de log en texto plano.

```
2008-06-0515:39:14,891 ERROR [com.example.logging] - Usuario
FMartinez..
```

Imagen 5. Ejemplo de un archivo de log en texto plano

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic).

Si bien es cierto existen en el mercado componentes ya desarrollados para registrar los mensajes de errores y trazabilidad en archivos de texto plano, que facilitan la labor de registro; estos archivos pueden representar dificultades para el análisis de la información registrada, ya que no disponen de mecanismos que aseguren la estructura y el formato del mensaje.

Se deben definir políticas de rotación de archivos de logs, referentes al cierre del archivo actual y apertura de uno nuevo, teniendo en cuenta criterios como tamaño y/o frecuencia (cada hora, cada día, cada semana, etc.). Esta rotación permitirá mantener un tamaño manejable de los archivos históricos facilitando la revisión y el análisis.

Así mismo es importante establecer donde se almacenarán los archivos de log históricos, el tiempo de retención y si algunos de los mismos deben preservarse por almacenar información que tenga especial interés para procesos de control interno y/o auditoría.

Acorde con lo anterior, los archivos de mensajes de errores y trazabilidad se almacenan en los servidores o dispositivos, teniendo en cuenta las siguientes condiciones:

- No almacenado: algunos registros de eventos son habilitados durante el proceso de instalación del servidor, dispositivo o SIS-INF. Por lo tanto, es importante, para los administradores técnicos, asegurar y depurar los servicios de auditorías que se encuentran activos en cada uno de los sistemas.

- Local: todos los servidores cuya capacidad de almacenamiento permita almacenar los archivos de eventos en su estructura de directorios, deben realizarlo de manera local garantizando su disponibilidad y su integridad. La ubicación de los archivos creados por las entradas de registros debe quedar en un File System o directorio diferente a los archivos del sistema. Es obligatorio para los servidores o dispositivos que tienen servicios clasificados como críticos, almacenar localmente estos archivos. Adicionalmente, para garantizar la disponibilidad de los archivos, estos directorios deben incluirse en el plan de copias de respaldo y recuperación del sistema.
- Central: para aquellos servidores que dentro de su capacidad de almacenamiento local no soportan el volumen de información a registrar y para los servidores que se definan que serán monitoreados por herramientas especializadas, es necesario transmitir los archivos de registro de mensajes de errores y trazabilidad, a otro servidor o al servidor de almacenamiento (Storage Area Network - SAN) que defina la Unidad Digital.

Para los SIS-INF considerados como críticos, los registros de trazabilidad deben almacenarse de forma centralizada y de manera local, con el fin de garantizar la integridad y disponibilidad en caso de una investigación.

Para las actividades anteriores se pueden tener en cuenta las recomendaciones del NIST.

1.7. Seguridad

A continuación se describen controles de seguridad y la mejor práctica a tener en cuenta en el manejo de los registros de eventos y trazabilidad, acorde a lo establecido por el Instituto Nacional de Estándares y Tecnología del Departamento de Comercio de Estados Unidos. (National Institute of Standards and Technology. U.S. Department of Commerce – NIST):

Dimensión	Controles	Mejor práctica
Integridad de la información	Calcular "*message digest*"1 del archivo o registro de base de datos, y almacenarlo de manera segura, garantizando así que las modificaciones sobre dicha información pueden ser detectadas.	Para el cálculo del "*message digest*" se hace uso de algoritmos como: ▪ Código de autenticación de mensajes basado en Hash (Hash-based Message Authentication Code - HMAC) ▪ SHA256 ▪ Firma Digital ▪ *Encripción Pretty Good Privacy* (PGP)
Confidencialidad de la información2	Evitar el acceso no autorizado a los logs, a través de la implementación de controles de acceso, el uso de algoritmos de encriptación y el aseguramiento del canal a través del cual se transmiten los logs. Evitar registrar información que tenga el carácter de confidencial en los logs.	Algoritmos de encriptación: ▪ Triple Data Encryption Standard - 3DES. ▪ *Advanced Encription* Standard – AES con tamaños de clave entre 128 y 256 bits, para criptografía simétrica. ▪ Algoritmo para encriptación de llave pública Rivest, Shamir y Adleman - RSA. ▪ Algoritmo para intercambio de claves Diffie-Hellman, con tamaños de clave entre 1024 bits y 2048 bits, para criptografía asimétrica. Protocolos para aseguramiento del canal: ▪ Seguridad de la capa de transporte (Transport Layer Security – TLS) [12]: protocolo que provee privacidad y seguridad en la comunicación entre dos aplicaciones. ▪ IPSec [13]: conjunto de protocolos que provee seguridad a las comunicaciones sobre la capa de red IP (Protocolo de Internet –

[1] Ver significado de *Message Digest* en la sección de Definiciones.

Dimensión	Controles	Mejor práctica
		Internet Protocol).
Disponibilidad de la información.	Asegurar el buen funcionamiento y disponibilidad de los componentes de *software* del SIS-INF que tienen por responsabilidad el registro de los logs, controlando la manipulación y el fallo seguro de los mismos cuando se presenten errores que interrumpan el registro de los eventos.	Guía para la implementación de controles de seguridad informática en aplicaciones. Proyecto Abierto de Seguridad en Aplicaciones Web (Open Web Application Security Project - OWASP). [10].

Tabla 4 Mejores prácticas de seguridad

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic).

1.8. Consideraciones adicionales

Para dar soporte a los procesos de gestión y monitoreo, es importante contar con herramientas que de manera automática permitan consolidar, filtrar, consultar y analizar la información registrada en los logs, como es el caso de los Sistemas de Gestión de eventos e Información de Seguridad (SIEM) de la misma manera se deben establecer responsables que definan políticas de retención, desecho y preservación de los mismos.

La calidad de la información registrada en los logs como los resultados de los análisis correspondientes, van a ser fundamentales para la gestión de incidentes, identificación de controles correctivos y posibles mejoras, y para dar soporte a procesos de auditoría y control interno en las entidades del Estado.

La entidad debe seleccionar cuidadosamente las transacciones a las que necesita hacerle seguimiento, las operaciones a auditar (consulta, creación, modificación, eliminación) y la cantidad de información funcional que requiere registrar, con el fin de evitar que esta tarea afecte el desempeño de los SIS-INF y que la información registrada ocupe demasiado espacio de almacenamiento.

GLOSARIO

Dirección IP: Identificador de host dentro de una red de comunicaciones que utiliza el *Internet Protocol*.

Evento: Acción que se genera durante la operación de un sistema de información.

Hash: Funciones que permiten calcular firmas digitales a través de las cuales se puede identificar de manera única un conjunto de datos.

Host: Computador o dispositivo móvil conectado a una red a través de la cual intercambia información.

Log: Registro de un evento ocurrido durante la operación de un sistema de información.

***Message Digest*:** Firma digital que identifica de manera única un conjunto de datos y que tiene la propiedad de cambiar si al menos un bit de los datos sobre los cuales se calculó, es modificado.

Registro: Representa la evidencia de actividades desempeñadas o resultados alcanzados, los cuales sirven como base para verificar que los SIS-INF de la entidad se están desempeñando según lo esperado [6].

SHA-256: Algoritmo que implementa un conjunto de funciones hash para el cálculo de *message digest*, creado por el Instituto Nacional de Estándares y Tecnología del Departamento de Comercio de Estados Unidos. (National Institute of Standards and Technology. U.S. Department of Commerce - NIST).

REFERENCIAS

[1] Eindhoven University of Technology .XES. (2014). Extensible Event Stream Standard. [Online]. Disponible en: http://www.xes-standard.org/_media/xes/xesstandarddefinition-2.0.pdf. [Último acceso: mayo 19 de 2014].

2] ISACA. COBIT-5. A Business Framework for the Governance and Management of Enterprise IT Procesos Catalizadores. Dominio Entrega, Servicio y Soporte. 2012.

[3] International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 27002:2013. Information Technology -- Security techniques -- Code of practices for information security controls. Section 12: Operations Management. 12.4 Logging and monitoring.

[4] República de Colombia. Gobierno Nacional. Ley 87 del 29 Noviembre de 1993. Por la cual se establecen normas para el ejercicio del control Interno en las entidades y organismos del Estado y se dictan otras disposiciones. [Online]. Disponible en: http://www.mininterior.gov.co/sites/default/files/ley_87_de_1993.pdf. [Último acceso: mayo 19 de 2014].

[5] U.S. Department of Commerce. National Institute of Standards of Technology. Special Publication 800-92. Guide to Computer Security Log Management. 2006. [Online]. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf [Último acceso: mayo 18 de 2014].

[6] U.S. Department of Commerce. National Institute of Standards of Technology. Special Publication. Glossary of Key Information Security Terms. NISTIR 7298. Revision 2. 2013. [Online]. Disponible en: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf. [Último acceso: julio 18 de 2014].

[7] ECMA-International. Estándar ECMA-404. "The JSON Data Interchange Format". Octubre 2013. [Online]. Disponible en: http://www.ecma-

international.org/publications/files/ECMA-ST/ECMA-404.pdf. [Último acceso: julio 18 de 2014].

[8] World Wide Web Consortium (W3C). Extensible Markup Language (XML). [Online]. Disponible en: http://www.w3.org/XML. [Último acceso: julio 18 de 2014].

[9] The Internet Engineering Task Force (IETF®). Common Format and MIME Type for Comma-Separated Values (CSV) Files. 2005. [Online]. Disponible en: http://tools.ietf.org/html/rfc4180. [Último acceso: julio 18 de 2014].

[10] Open Web Application Security Project – OWASP. OWASP Developer Guide 2.0.1. 2013. [Online]. Disponible en: https://github.com/OWASP/DevGuide/tree/dc5a2977a4797d9b98486417a5527b9f15d8a251/DevGuide2.0.1. [Último acceso: 27 de junio de 2014]