

Nuevo enfoque de arquitectura para la interoperabilidad de sistemas de información en la gestión de desastres

Marcelo Zambrano^{1a,1b}, Ana Zambrano², Francisco Pérez³, Edgar Maya⁴, Paúl Rosero⁵, Eduardo Ortiz⁶

omzambrano@utn.edu.ec, ana.zambrano@epn.edu.ec, frapecar@upvnet.upv.es, eamaya@utn.edu.ec, pdrosero@utn.edu.ec, eduardo.ortiz@epn.edu.ec

^{1a,4,5} Universidad Técnica del Norte, 100110, Ibarra, Ecuador.

^{1b} Instituto Tecnológico Superior Rumiñahui, 171103, Sangolquí, Ecuador.

^{2,6} Escuela Politécnica Nacional, 170525, Quito, Ecuador.

³ Universitat Politècnica de València, 46022, Valencia, España.

Pages:69–81

Resumen: Cuando un desastre se suscita en un determinado núcleo social, es indispensable que las organizaciones responsables de gestionarlo, actúen de manera conjunta con el objetivo de alcanzar una respuesta que minimice los daños y pérdidas derivadas de su presencia. Para esto, es necesario que dichas organizaciones intercambien información de forma permanente, con el objetivo de obtener una conciencia situacional común que les permita coordinar sus operaciones y gestionar el incidente de la mejor manera posible. Este artículo describe la arquitectura de una plataforma de interoperabilidad, que les permite a las organizaciones, involucradas en la gestión de un desastre, intercambiar información, de modo transparente, e independiente de los sistemas de información y herramientas informáticas utilizadas por cada una de ellas.

Palabras-clave: bases de datos distribuidas; gestión de desastres; interoperabilidad; redes P2P; sistemas de información.

New architecture approach for the interoperability of information systems in disaster management

Abstract: When a disaster arises in a certain social nucleus, it is essential that the organizations responsible for managing it, act jointly with the objective of reaching a response that minimizes the damages and losses derived from their presence. For this, it is necessary that these organizations exchange information permanently, with the aim to obtain a common situational awareness that allows them to coordinate their operations and manage the incident in the best possible way. This article describes the architecture of an interoperability platform that allows organizations involved in the management of a disaster, to exchange information transparently and independently of the information systems and computer tools used by each of them.

Keywords: distributed databases; disaster management; interoperability; P2P networks; information systems.

1. Introducción

Un desastre puede definirse como un incidente de carácter dañino que pone en riesgo al medio ambiente, la propiedad y/o la vida de las personas. Para gestionarlo, es necesaria la participación de múltiples organizaciones relacionadas con la protección y seguridad pública, las cuales deben orquestar sus operaciones para alcanzar una respuesta que permita mitigar sus efectos destructivos y minimizar las posibles pérdidas ambientales, materiales y humanas (Blanchard, 2008; ACNUR, 2012; FEMA, 2015). Pero esta diversidad de recursos, habilidades y conocimientos, indispensables para alcanzar una respuesta integral que cubra los requerimientos de todos los involucrados (Gobierno, organizaciones de respuesta y ayuda humanitaria, damnificados, etc.), también es el principal obstáculo para que dichas organizaciones trabajen de manera conjunta y orienten sus esfuerzos en una misma dirección, puesto que cada una de ellas posee sus propios objetivos, tecnología, procedimientos, etc. Para solventar este inconveniente, es necesario que dichas organizaciones intercambien información, de forma permanente, obteniendo un conocimiento común de la situación (conciencia situacional) que les permita coordinar sus operaciones y colaborar (Williams, 2010).

La capacidad de dos o más sistemas para intercambiar información y utilizarla para alcanzar sus objetivos se conoce como interoperabilidad (IEEE Standard Computer Dictionary, 1991). En escenarios complejos (heterogéneos y multiorganizacionales) como en el caso de la Gestión de Desastres (GD), la interoperabilidad es la clave para la adquisición de una conciencia situacional común y la orquestación de los recursos implicados. Organismos como la Agencia Federal para la Gestión de Emergencias de los Estados Unidos (Federal Emergency Management Agency, s. f.), la Organización Internacional de Normalización con su Comité Técnico para la Protección y Seguridad de la Sociedad (ISO/TC 223, s. f.), La Oficina de las Naciones Unidas para la Reducción del Riesgo de Desastres (United Nations, 2017), entre otras, han publicado diferentes tipos de estándares y recomendaciones, recalcando la importancia de la interoperabilidad en GD. Este artículo presenta una alternativa para la materialización de estas estrategias y recomendaciones. Propone la implementación de una plataforma de interoperabilidad que permita a las organizaciones, involucradas en la GD, integrarse dentro de una infraestructura de comunicaciones compartida, con el objetivo de intercambiar información utilizando sus propios sistemas de información (SI) y herramientas informáticas. El principal aporte de esta investigación se encuentra en su Espacio de Información Compartida (EIC), el cual permite gestionar como una única entidad de almacenamiento toda la información proveniente de los diferentes SI. Se asienta sobre una Base de Datos Distribuida No Relacional (BDD NoSQL) y una red de comunicaciones mallada (P2P), para dotar a la plataforma de la agilidad y resiliencia requerida para operar en entornos críticos y hostiles como en el caso de los desastres.

La validación se realizó mediante pruebas de funcionalidad a un prototipo implementado en base a la arquitectura descrita en este artículo. Las pruebas se realizaron dentro de un escenario simulado para un desastre, en el cual, tres SI registrados en la plataforma (InaSAFE, WebGIS y GESTOP), ubicados en tres localidades diferentes, compartieron

información referente al estado del entorno y las unidades de respuesta supervisadas por cada uno de ellos. La información compartida permitió la obtención de una conciencia situacional común que sirvió como punto de partida para la planificación, toma de decisiones y coordinación de las operaciones de respuesta y recuperación.

Este artículo está dividido en cinco secciones: primero, se realiza una introducción al contexto y metodología utilizada para el desarrollo de la plataforma; segundo, se describe la motivación y los trabajos que sirvieron como referencia de esta investigación; tercero, se detalla la arquitectura, sus funcionalidades y los bloques principales que la conforman; cuarto, se describen las pruebas de funcionalidad y los resultados obtenidos durante las mismas; y finalmente, quinto, se exponen las conclusiones y futuras líneas de investigación relacionadas con este trabajo.

2. Motivación y trabajos relacionados

Uno de los factores más importantes a ser considerados, con respecto a la interoperabilidad, es la forma en que los usuarios acceden a la información disponible. De manera general, los usuarios son renuentes a la utilización de herramientas informáticas externas, ya sea por afinidad con aplicaciones que usan habitualmente o por falta de experticia en aplicaciones que desconocen. La plataforma de interoperabilidad descrita en este artículo tiene como objetivo principal posibilitar que, las organizaciones involucradas en la gestión de un desastre, utilicen sus SI propietarios para compartir y/o adquirir información útil para gestionar el desastre. Para su desarrollo, se ha tomado como referencias principales al Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM) y a las BDD NoSQL.

El JC3IEDM (Figura 1), fue creado por el Programa de Interoperabilidad Multilateral de la OTAN, con el objetivo de apoyar y facilitar el intercambio de información de mando y control en entornos tácticos multinacionales (NATO, 2012). Propone la implementación de una capa de intermedia de comunicaciones (middleware) y un modelo de datos normalizado, para permitir que esos SI heterogéneos intercambien información. Cada SI debe poseer su propia interfaz de comunicaciones, la cual le permite obtener y/o publicar información desde o hacia el modelo de datos definido en la middleware.

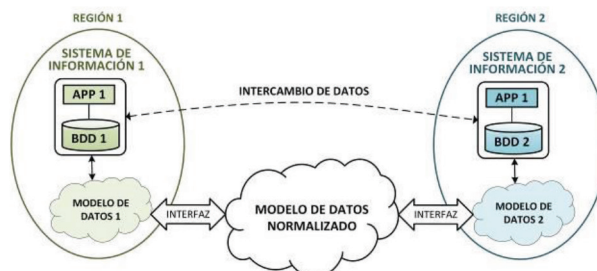


Figura 1 – Esquema general JC3IEDM.

Por su parte, las bases de datos distribuidas (BDD) aprovechan la estructura multiorganizacional, característica de la GD, para segmentar la carga de trabajo

(almacenamiento y procesamiento de datos) entre todos los nodos que conforman el *cluster*. Las bases de datos no relacionales, llamadas también No only SQL (NoSQL), permiten representar y almacenar cada objeto a ser compartido, con un esquema de datos independiente, solventando las deficiencias de las bases de datos tradicionales (relacionales) en cuanto a la gestión de datos heterogéneos. La Figura 2, muestra un diagrama que resume la propuesta en cuanto a la gestión de datos con BDD NoSQL para esta investigación (Han et al., 2011).

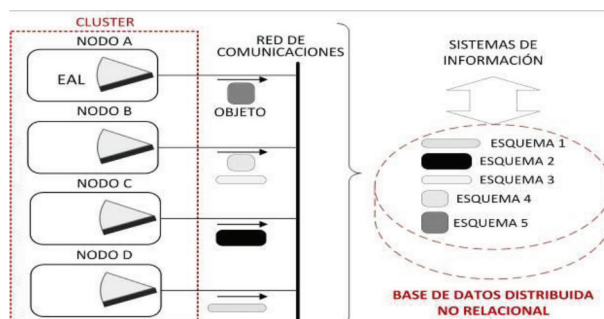


Figura 2 – Esquema para la gestión de datos

3. Arquitectura

La arquitectura ha sido diseñada con el objetivo de otorgar a la plataforma la agilidad y resiliencia requerida para operar y cumplir con las exigencias del entorno de un desastre. Cada organización utilizará sus propios SI para obtener y/o compartir información dentro de la plataforma, y la capa de middleware adaptará la información proveniente desde y hacia ellos al modelo de datos definido en su interior. La comunicación entre los SI y la plataforma, se realiza bajo un modelo de información basado en el estándar Efficient XML Interchange (EXI) (Doi et al., 2012; Jaiswal & Mishra, 2013), y la información que se requiera compartir se almacenará en una BDD NoSQL que da forma al EIC.

Para facilitar su análisis y desarrollo, la arquitectura se ha dividido en tres bloques principales (Figura 3):

1. Sistemas de información: dispositivos, equipos o SI, registrados en la plataforma con el objetivo de aportar y/u obtener información de la misma.
2. Middleware, cumple las funciones de transceptor entre la subred de comunicaciones y los SI.
3. Subred de comunicaciones, es la responsable de proveer la conectividad entre los nodos que conforman la plataforma. Su topología, así como la tecnología utilizada en los enlaces de comunicación, son transparentes para la middleware, lo que facilita su implementación y escalabilidad.

La arquitectura ha sido desarrollada en su totalidad bajo *software* libre, eliminando la dependencia con los fabricantes (mantenimiento, actualizaciones, etc.) y dejando la puerta abierta para su personalización y desarrollo de nuevas funcionalidades. Linux se ha elegido como sistema operativo para los nodos de comunicaciones, Apache Cassandra como Gestor de Base de Datos, Java como lenguaje de programación para el desarrollo

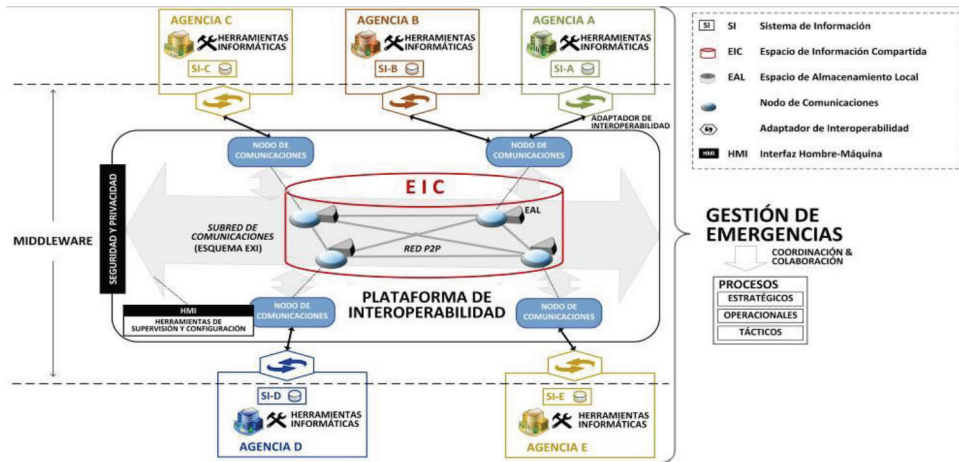


Figura 3 – Arquitectura en tres bloques. Bloque 1: sistemas de información; bloque 2: capa middleware; bloque 3: subred de comunicaciones

de los distintos módulos de *software* y AngularJS como *framework* Javascript para la implementación del *frontend* de la Interfaz Hombre-Máquina (HMI).

La capa middleware representa la columna vertebral de esta arquitectura y es la responsable de permitir el intercambio de información entre los SI. Está subdividida en cuatro bloques: adaptadores de interoperabilidad, nodos de comunicaciones, EIC, y la HMI.

3.1. Adaptadores de interoperabilidad

Son los responsables de acoplar la información proveniente de los SI al formato EXI definido en la subred de comunicaciones y viceversa.

Debido a la diversidad y heterogeneidad en los protocolos y formatos de datos utilizados por los diferentes SI, cada uno de ellos necesitará su propio adaptador de interoperabilidad y existirán tantos adaptadores como SI se integren a la plataforma.

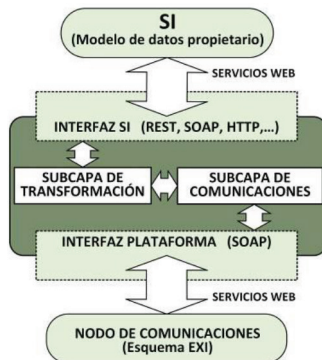


Figura 4 – Adaptador de interoperabilidad

Cada adaptador posee una interfaz hacia el SI y otra hacia el nodo de comunicaciones, permitiendo el flujo de información entre ellos a través de servicios web. Las peticiones/respuestas desde y hacia los SI, se realizan por medio de cualquier tipo de servicio web que haya sido definido en el SI en cuestión (SOAP, REST, HTTP, etc.), mientras que las peticiones/respuestas desde y hacia los nodos de comunicaciones, de acuerdo al diseño de la plataforma y siguiendo los principios de estandarización propuestos, se realizan únicamente por SOAP.

Entre las interfaces de comunicación, existen dos subcapas: transformación y comunicaciones, que permiten llevar a cabo la conversión de los formatos de datos de manera bidireccional. La Figura 4 muestra un diagrama de bloques genérico de un adaptador de interoperabilidad.

3.2. Nodos de comunicaciones

Son la puerta de entrada a la plataforma. Entre sus funciones principales están las de permitir el registro de los SI, almacenar la fracción de la base de datos que le corresponda, y notificar a los SI y otros nodos de cualquier cambio realizado en la información del EIC.

La Figura 5 muestra un diagrama de bloques que resume la arquitectura interna de un nodo de comunicaciones. Se pueden identificar cuatro elementos principales: una capa de usuario, encargada de poner al alcance de los SI los servicios para la configuración de los parámetros operacionales de la plataforma (registro de SI, suscripción a las notificaciones, direccionamiento, etc.) y la interacción con el EIC (lectura, escritura, eliminación y actualización de datos); una capa de operaciones, responsable de los procesos de gestión y funcionales al interior del nodo, como por ejemplo, seguridad, privacidad, comunicación entre nodos, gestión de datos, etc.; dos grupos de servicios transversales, encargados de la supervisión y seguridad de los procesos internos además de los accesos al nodo; y por último, un Espacio de Almacenamiento Local (EAL), en el cual almacena la fracción del EIC que tiene asignado, así como una copia del registro de usuarios y sistemas.

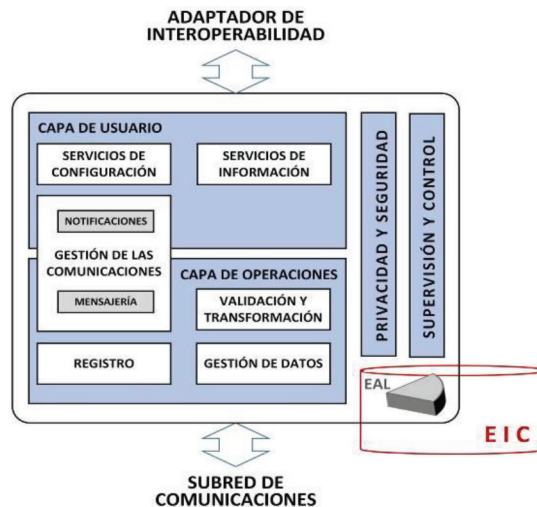


Figura 5 – Nodo de comunicaciones

Las comunicaciones con los otros nodos y con los SI enlazados a la plataforma a través de él, se realizan por medio de datagramas en formato EXI, que informan de cualquier cambio en la información y/o el estado de la plataforma. Estos datagramas, antes de ser almacenados, deben ser validados y transformados al formato definido en el EIC por medio del módulo de validación y transformación.

Pueden desplegarse tantos nodos, como sean requeridos, y cada nodo puede servir a más de un SI, dependiendo del alcance de la plataforma, la capacidad de procesamiento del nodo y los requerimientos propios de cada SI en cuanto a recursos, seguridad, disponibilidad y/o confiabilidad.

3.3. Espacio de Información Compartida

El EIC es el núcleo de la arquitectura. Utiliza una BDD NoSQL y una red virtual P2P, para gestionar la información proveniente de los SI como un único espacio de almacenamiento lógico. Posee un modelo de datos independiente a los utilizados por los SI integrados a la plataforma, y cada objeto almacenado es definido con una clave única basada en un modelo clave-valor, bajo su propio esquema de datos. El EIC aprovecha el carácter distribuido de la arquitectura, para permitir la asignación y distribución dinámica del procesamiento y almacenamiento de los datos. Una de sus principales ventajas, es la independencia de los objetos, que hace que la ubicación física y el esquema de los datos, sean transparentes para los SI.

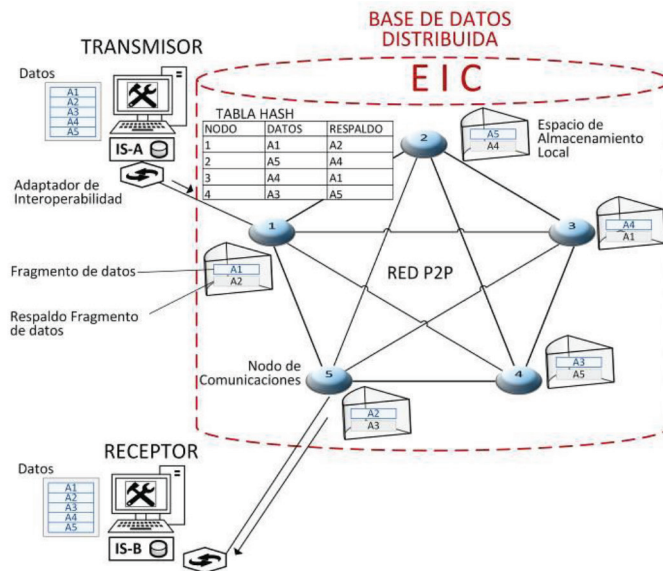


Figura 6 – Espacio de Información Compartida

En cuanto a la gestión de datos y la implementación del EIC, se aprovecha el carácter distribuido y el algoritmo P2P de Apache Cassandra (DataStax, 2016). Tanto la carga de trabajo como la redundancia son parametrizables y deben ser configuradas de acuerdo a la

confiabilidad, disponibilidad y escalabilidad requerida. La red interna P2P presenta una topología lógica no jerárquica en anillo que permite la respuesta simultánea de múltiples nodos a múltiples peticiones (escalabilidad horizontal). Las consultas, actualizaciones, borrados e inserciones de información, se realizan por medio del lenguaje propietario Cassandra Query Language (CQL), y la librería Kundera brinda soporte para el API de Persistencia de Java (JPA) (Apache Software Foundation, 2017). La Figura 6 muestra un diagrama de bloques que resume la arquitectura interna del EIC.

3.4. Seguridad e interfaz hombre-máquina

La accesibilidad y privacidad de la plataforma se gestiona a través de la HMI, la cual, permite la creación y asignación de perfiles y permisos a través del módulo de “privacidad y seguridad”. De la misma manera, permite la generación de auditorías y el mantenimiento de la plataforma por medio del módulo de “supervisión y control”. Cada nodo posee una réplica del registro de usuarios y sistemas, garantizando siempre y en cualquier circunstancia, la accesibilidad y seguridad de la plataforma. Respecto a la seguridad de las comunicaciones, se gestiona en base a los protocolos de seguridad como HTTPS y TLS.

3.5. Gestión de las comunicaciones y datos

Las comunicaciones entre nodos, así como a las comunicaciones entre un nodo y los SI integrados a través de él se realizan en base al estándar EXI, creado por el World Wide Web Consortium (W3C). El EXI está pensado para optimizar el rendimiento y uso de recursos en redes que operan en entornos con capacidades limitadas, como en el caso de los desastres (baja capacidad de procesamiento y almacenamiento, ancho de banda limitado, congestión, pérdida de paquetes, etc.) (Doi et al., 2012; Jaiswal & Mishra, 2013). Gestiona la información por medio de un esquema XML que explota la naturaleza estructurada del formato para optimizar la transmisión y procesamiento de datos. El esquema EXI definido en la plataforma es distribuido a través de toda la subred de comunicaciones, de tal manera que cada nodo sea capaz de comprimir/descomprimir los objetos de datos recibidos y/o enviados. Tanto la publicación como los requerimientos de información (datos y metadatos) siguen el mecanismo EXI implementado. Cada vez que un SI comparte información, esta se valida, transformada y almacenada en el EIC, para que sea accesible a través de cualquiera de los nodos del Clúster.

Los SI deben especificar las temáticas de los cuales van ser proveedores, y las temáticas a las cuales quieren suscribirse como consumidores. Cada vez que se comparte una nueva información en el EIC, el nodo local notifica a los SI registrados sobre él y suscritos a la temática en cuestión, de la actualización de información por medio de su servicio de “notificaciones”. Si un SI considera de interés la información, es capaz de recuperarla desde el EIC, para transformarla a su modelo de datos propietario y ponerla a disposición de sus usuarios. De manera similar, el nodo local comparte la actualización con los otros nodos de la plataforma a través del servicio de “mensajería”, para que estos, a su vez, notifiquen a los SI registrados sobre ellos, de la nueva información disponible.

Para que un nuevo nodo pueda integrarse a la plataforma, el primer paso a realizar es su registro sobre la misma. Una vez autorizado su acceso, el nodo pasa a formar parte del EIC, iniciando las comunicaciones con los otros nodos a través de la subred. Cada

nodo dispone de un EAL, donde almacena la porción de datos que le corresponde, de acuerdo a una tabla HASH, creada por el algoritmo P2P de Cassandra (Apache Software Foundation, 2017; Padhy, Patra & Satapathy, 2011). La disponibilidad de los datos y resiliencia de la plataforma se garantiza en base a la creación de múltiples copias en diferentes nodos (redundancia), las cuales dependen de un factor de replicación (número de réplicas de la información en nodos diferentes) que puede ser configurado de forma discrecional.

4. Validación y resultados

La funcionalidad de la plataforma se validó por medio de pruebas a un prototipo implementado en base a la arquitectura descrita en este artículo. Las pruebas se desarrollaron dentro de un escenario simulado para un desastre, que inicia con el colapso de la central hidroeléctrica de Bolarque (Cuenca-España), ocasionando una inundación que afecta la central nuclear José Cabrera (Guadalajara-España), con un posible escape radiológico de por medio. Se implementaron tres nodos de comunicaciones en tres localidades diferentes (Madrid, Cuenca y Valencia), y a través de ellos, se integraron a la plataforma tres Sistemas de Información Geográfica (GIS) como se muestra en la Figura 7.



Figura 7 – Escenario de pruebas

Nodo	Hardware	Software Nodo	Software SI
1 Madrid	Intel Core i7 2.8 RAM 16GB Disco 2TB Red Ethernet		Ubuntu 15.10 WebGIS (DESTRIERO, 2017) Adapt. de Interoperabilidad 1
2 Cuenca	Intel Core i7 2.9 RAM 8GB Disco 1TB Red Ethernet	CentOS 7.0 Open VPN Apache Cassandra 3.2	Ubuntu 15.10 InaSAFE (InaSAFE, 2017) Adapt. de Interoperabilidad 2
3 Valencia	Intel Core i7 3.3 RAM 16GB Disco 1TB Red Ethernet		Windows 8.1 GESTOP (TR'Sistemas, 2017) Adapt. de Interoperabilidad 3

Tabla 1 – Hardware y software infraestructura de pruebas

Gracias a la segmentación y distribución de la carga de trabajo, los GIS y sus respectivos adaptadores de interoperabilidad, pudieron ser implementados sobre HOST con características estándar de *hardware* y *software*, como se observa en la Tabla 1.

En cuanto a la seguridad y conectividad de la plataforma, se utilizaron conexiones SSL con certificados y claves RSA (Rivest, Shamir y Adleman) generados con la herramienta Open-VPN y distribuidos en cada uno de los nodos. Cada GIS compartió, a través de la plataforma, información referente a la identificación y posicionamiento de las unidades de respuesta bajo su supervisión. Esta información permitió crear una conciencia situacional común de todos los recursos desplegados sobre el campo de pruebas, la misma que fue utilizada por el personal táctico y estratégico para planificar y coordinar las operaciones de respuesta y recuperación para la emergencia.

La Figura 8 muestra en segundo plano, la interfaz gráfica (GUI) de cada uno de los GIS utilizados en las pruebas; y como plano principal, la GUI del GIS conectado al nodo 1, mostrando un agregado de todas las unidades sobre el campo de operaciones.

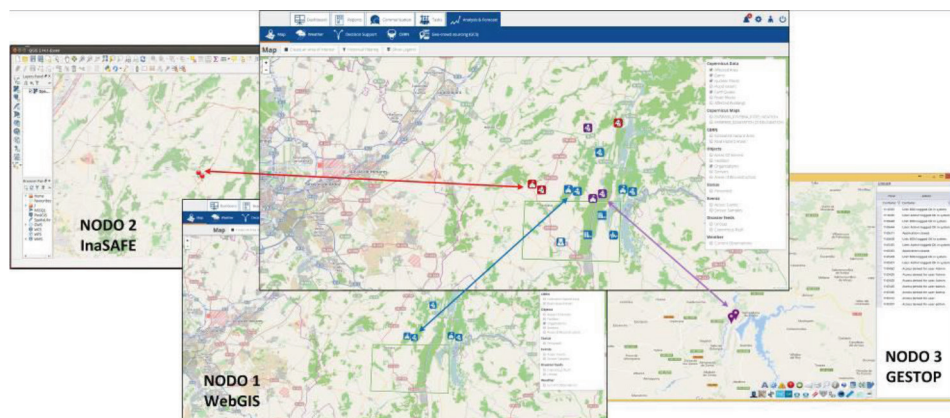


Figura 8 – Unidades de respuesta desplegadas sobre el entorno de pruebas

Durante las pruebas, se contó con la colaboración de personal de Bomberos y Defensa Civil de la Comunidad de Madrid, los cuales tuvieron acceso a la información y reportes generados por los SI integrados a la plataforma. Posterior a esto, se realizó una encuesta al personal táctico y estratégico que colaboró en el simulacro, con el fin de tabular su percepción respecto a las funcionalidades y ayudas que la plataforma ofrece. Los resultados se muestran en la Tabla 2.

El 100% de los encuestados estuvieron de acuerdo, en mayor o menor grado, con la usabilidad de la plataforma. Un 93% usaría la plataforma ya sea para entrenamiento o en un entorno real y cree que su organización se vería beneficiada con las funcionalidades entregadas. Así también, un 87% de los encuestados recomendaría el uso de esta plataforma y coincide con el planteamiento propuesto.

Pregunta	(1)	(2)	(3)	(4)	(5)
<i>Considero que el intercambio de información entre las organizaciones involucradas en la gestión de emergencias es prioritario</i>	10	4	1		
<i>La plataforma promueve la interoperabilidad entre las organizaciones involucradas en la gestión de emergencias</i>	4	11			
<i>La plataforma de interoperabilidad ofrece soporte para la obtención de una conciencia situacional común</i>	2	9	4		
<i>El uso de la plataforma de interoperabilidad puede ayudar a mejorar la coordinación y colaboración</i>	4	10	1		
<i>Recomendaría el desarrollo de adaptadores para otros sistemas de información</i>	2	11		1	1
<i>La plataforma es práctica y utilizable</i>	3	9	3		
<i>Usaría la plataforma en un entorno real</i>	3	7	3	1	1
<i>Usaría la plataforma en un entorno de entrenamiento</i>	4	10			1
<i>Usaría la plataforma durante la fase de respuesta a una emergencia</i>	5	8	1		1
<i>Usaría la plataforma durante la fase de recuperación a una emergencia</i>	3	7	3	1	1
<i>Considero que el uso de la plataforma de interoperabilidad, puede ayudar a disminuir las comunicaciones innecesarias</i>	2	8	4		1
<i>Considero que mi organización se vería beneficiada de las capacidades entregadas por la plataforma</i>	3	7	3	1	1
<i>A pesar de las restricciones presupuestarias, mi organización podría desarrollar su propio adaptador y convertirse en un socio de financiamiento para la implementación de una plataforma de interoperabilidad</i>	1	5	5	2	2

Equivalencia: (1) cumple totalmente; (5) no cumple con nada.

Tabla 2 – Encuesta realizada al personal táctico y estratégico

5. Conclusiones y trabajos futuros

La interoperabilidad es la clave para que las organizaciones involucradas en la gestión de un desastre obtengan una respuesta integral que permita enfrentar cualquier tipo de desastre que se pueda presentar. Para esto, es necesario el intercambio permanente de información que permita, a las organizaciones implicadas, obtener una conciencia común de la situación, coordinar sus operaciones y colaborar.

Este artículo describe la arquitectura de una plataforma de interoperabilidad que permite a las organizaciones involucradas en la gestión de un desastre, intercambiar información a través de sus propios sistemas y herramientas informáticas. El núcleo de la arquitectura se encuentra en su Espacio de Información Compartida, el cual permite gestionar como una única entidad de almacenamiento, toda la información proveniente

de los sistemas de información integrados a la plataforma. El Espacio de Compartido de Información se asienta sobre una Base de Datos Distribuida No Relacional y una red de comunicaciones mallada, para segmentar la carga de trabajo entre todos los nodos de la plataforma, otorgándole disponibilidad, escalabilidad y resiliencia a la plataforma.

La funcionalidad de la plataforma se validó por medio de un prototipo desarrollado en base a la arquitectura descrita en este artículo y testeada dentro de un escenario simulado para un desastre. Se pudieron verificar las capacidades de la plataforma para facilitar el intercambio de información entre las organizaciones, y la información compartida fue utilizada por el personal táctico y estratégico para planificar y coordinar las operaciones de respuesta y recuperación.

La arquitectura propuesta, fue tomada como referencia para el desarrollo de la plataforma de interoperabilidad del proyecto europeo SECTOR (SECTOR, 2016), el cual fue parte del séptimo programa Marco de la Unión Europea para Investigación y Desarrollo Tecnológico (FP7) y terminó el pasado 2018. SECTOR tuvo como objetivo principal el mejorar la interconexión, coordinación y colaboración entre los sistemas para la gestión de desastres y crisis.

Respecto a los trabajos futuros, se están explorando otras alternativas para la implementación del Espacio de Información Compartida, en base a una BDD NoSQL orientada a documentos (Padhy et al., 2011; Li & Manoharan, 2013). Por otra parte, la interfaz hombre-máquina les permite a los administradores acceder a las herramientas de configuración y supervisión de la plataforma, sin embargo, su implementación deja la puerta abierta para el desarrollo de herramientas propias, que permitan personalizar y mejorar las ayudas disponibles para los usuarios. Actualmente, se está trabajando en el desarrollo de una herramienta propietaria que permita el intercambio de información de audio y vídeo en tiempo real.

Referencias

- ACNUR. (2012). Manual para situaciones de emergencia. *United Nations High Commissioner for Refugees*. Recuperado de <https://www.acnur.org/fileadmin/Documentos/Publicaciones/2012/1643.pdf>
- Apache Software Foundation. (2017). Apache Cassandra. *Apache Software Foundation*. Recuperado de <http://cassandra.apache.org/>
- Blanchard, B. W. (2008). Guide to Emergency Management and Related Terms, Definitions, Concepts, Acronyms, Organizations, Programs, Guidance, Executive Orders & Legislation: A Tutorial on Emergency Management, Broadly Defined, Past and Present. *Center for Homeland Defense and Security*. Recuperado de <https://www.hsdl.org/?abstract&did=>
- DataStax. (2016). Apache Cassandra Documentation. *Apache Software Foundation*. Recuperado de <http://cassandra.apache.org/doc/latest/>
- DESTRIERO. (2017). FP7 European Union. *DESTRIERO*. Recuperado de <http://www.destriero-fp7.eu/>

- Doi, Y., Sato, Y., Ishiyama, M., Ohba, Y., & Teramoto, K. (2012). XML-less EXI with code generation for integration of embedded devices in web based systems. En 2012 3rd IEEE International Conference on the Internet of Things (pp. 76-83). DOI: 10.1109/IOT.2012.6402307
- FEMA. (s. f.). Department of Homeland Security US. *FEMA*. Recuperado de <https://www.fema.gov/>
- Han, J., E, H., Le, G., & Du, J. (2011). Survey on NoSQL database. En 2011 6th International Conference on Pervasive Computing and Applications (pp. 363-366). DOI: 10.1109/ICPCA.2011.6106531
- IEEE Standard Computer Dictionary. (1991). A Compilation of IEEE Standard Computer Glossaries. IEEE Std 610, 1-217. DOI: 10.1109/IEEESTD.1991.106963
- InaSAFE. (2017). Indonesian and Australian Governments. *InaSAFE*. Recuperado de <http://inasafe.org/>
- FEMA. (2015). Fundamentals of Emergency Management. *FEMA*. Recuperado de <https://emilms.fema.gov/ISO230d/FEMO101000.htm>
- ISO/TC 223 Societal Security. (s. f.). International Organization for Standardization. *ISO/TC 223*. Recuperado de <http://www.isotc223.org/>
- Jaiswal, G., & Mishra, M. (2013). Why use Efficient XML Interchange instead of Fast Infoset. En 2013 3rd IEEE International Advance Computing Conference (IACC) (pp. 925-930). DOI: 10.1109/IAdCC.2013.6514350
- Li, Y., & Manoharan, S. (2013). A performance comparison of SQL and NoSQL databases. En 2013 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM) (pp. 15-19). DOI: 10.1109/PACRIM.2013.6625441
- NATO. (2012). Overview of the Joint C3 Information Exchange Data Model. *Public.mip-interop.org*. Recuperado de https://public.mip-interop.org/Public%20Document%20Library/04-Baseline_3.1/Interface-Specification/JC3IEDM/JC3IEDM-Metamodel-Specification-3.1.4.pdf
- Padhy, R. P., Patra, M. R., & Satapathy, S. C. (2011). RDBMS to NoSQL: Reviewing Some Next-Generation Non -Relational Database's. *Journal of Advanced Engineering Science and Technologies*, 11, 015-030.
- SECTOR. (2016). FP7 European Union. *SECTOR*. Recuperado de <http://www.fp7-sector.eu/>
- TR'Sistemas. (2017). Productos - TRS. *TR'Sistemas*. Recuperado de <http://www.trsisistemas.com/productos.php>
- United Nations. (2017). The United Nations Office for Disaster Risk Reduction. *UNISDR*. Recuperado de <https://www.unisdr.org/>
- Williams, A. (2010). Agility and Interoperability for 21st Century Command and Control. *The International C2 Journal*, 1(4), 1-30. Recuperado de <https://pdfs.semanticscholar.org/c422/307eb0d04ec421a9fec1efd1b38051493cb6.pdf>

© 2019. This work is published under <https://creativecommons.org/licenses/by-nc-nd/4.0/>(the “License”). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License.