

- <https://biblioteca.sistedes.es/biblioteca/conferencias/jisbd/jisbd-2017-la-laguna/>
- Inicio
- Noticias

- Acerca de la Biblioteca
- Conferencias
- Jornadas de Ingeniería del Software y Bases de Datos (JISBD)
- JISBD 2017 (La Laguna)

JISBD 2017 (La Laguna)

Ruiz, F. (Ed.), Actas de las XXII Jornadas de Ingeniería del Software y Bases de Datos (JISBD 2017). La Laguna (Tenerife), septiembre de 2017.

Las XX Jornadas de Ingeniería del Software y Bases de Datos (JISBD 2015) se han celebrado en La Laguna del 19 al 21 de julio de 2017, como parte de las Jornadas SISTEDES.

El programa de JISBD 2017 se ha organizado en torno a sesiones temáticas o *tracks*. A continuación se detalla el contenido de las actas:

- Preliminares
- Comités
- Conferencia invitada: Dr. Don Gotterbarn
- Tutoriales
- Salón de la Fama
- Track ASV – Arquitecturas Software y Variabilidad
- Track GD – Gestión de Datos
- Track ISDM – Ingeniería del Software Dirigida por Modelos
- Track ISGB – Ingeniería del Software Guiada por Búsqueda
- Track IWSP – Ingeniería Web y Sistemas Pervasivos
- Track MEISSI – Métodos Empíricos en Ingeniería del Software y Sistemas de Información
- Track PSM – Proceso Software y Metodologías

- Track RCP – Requisitos, Calidad y Pruebas

Propuesta de Marco para el Gobierno de la Seguridad en Entornos Big Data

Julio Moreno, Manuel A. Serrano, Eduardo Fernández-Medina

Grupo de investigación Alarcos, Universidad de Castilla la Mancha, Ciudad Real, España
{julio.moreno | manuel.serrano | eduardo.fdezmedina}@uclm.es

Resumen. Big Data ya es una realidad en el día a día de muchas compañías. Cuando se implanta un entorno Big Data en una organización, este se debe adaptar a las características de la misma. Para poder alcanzar una garantía de seguridad mientras se respetan las características inherentes de la organización se requiere una adecuada función de gobierno. Para lograr este objetivo hemos creado una propuesta de marco para el gobierno de la seguridad en entornos Big Data denominada marco GSB. Este marco de gobierno toma como base los estándares internacionales relacionados con el gobierno de las TI, como por ejemplo COBIT, y lo adapta a las necesidades específicas de un entorno de Big Data. El objetivo final del marco GSB es cubrir todo su ciclo de vida de forma segura.

Palabras clave: Big Data, Seguridad de la información, Gobierno de las TI.

1 Introducción

En los últimos años, los datos han incrementado su importancia en compañías de casi cualquier ámbito siendo imprescindibles para llevar a cabo sus actividades diarias y para ayudar a la alta dirección a alcanzar los objetivos de negocio y, gracias a ello, tomar las mejores decisiones basadas en la información extraída de dichos datos [1]. Es más, cada vez producimos un mayor volumen de datos [2]. Además, estos datos en su mayoría tienen un formato no estructurado, lo cual, complica su análisis por medio de los sistemas tradicionales. Este inconveniente no desanima a las organizaciones, que cada vez son más conscientes de la importancia de los datos, y de los beneficios que pueden obtener del análisis de este gran volumen y variedad de datos [3]. La suma de todos estos factores hace que sea necesario un nuevo paradigma de análisis de datos, este nuevo paradigma es Big Data [4].

Con cada nueva tecnología surgen nuevos problemas, Big Data no es una excepción. Estos problemas se encuentran relacionados no sólo con el volumen o la variedad de los datos, sino también con su privacidad y su seguridad, ya que, Big Data no fue concebido en un primer momento como un entorno seguro [5]. Por otro lado, cuando se añade un nuevo sistema a una compañía, este se debe adaptar a las particularidades de la misma. Por ello, se antoja necesario un marco de gobierno flexible que ayude a la alta dirección de las distintas organizaciones a gestionar la seguridad de este nuevo sistema de análisis de datos. Cuando se habla de un marco de gobierno en el entorno Big Data hay que tener en cuenta que se tratará de una parte de un mayor programa de

gobierno de la información, y que este marco formulará políticas relacionadas con la optimización, obtención de privacidad y seguridad, y monetización del uso del entorno Big Data mediante el alineamiento con los objetivos de negocio de la compañía [6].

Por ello, el objetivo de este artículo será exponer nuestra propuesta de marco para el gobierno de la seguridad en entornos Big Data. Para la creación de esta propuesta de marco de gobierno nos hemos basado en distintos estándares relacionados con el gobierno de las tecnologías de la información (TI), como COBIT y CMMI. Apoyado en las indicaciones dadas en dichos estándares y teniendo en cuenta el estudio sobre seguridad en Big Data realizado se ha sustentado la creación del marco GSB (Gobierno de la Seguridad en Big Data). Este artículo tiene la siguiente estructura: primero se hará una introducción a los trabajos que tienen relación con nuestra propuesta, a continuación, se expone cuál es nuestra propuesta y, finalmente, una sección en la que se abordan las conclusiones y trabajo futuro.

2 Trabajo relacionado

El término Big Data se refiere a un entorno que permite el análisis y gestión de mayores cantidades de datos que las técnicas tradicionales de procesamiento de datos. Big Data supone un cambio en comparación con dichas técnicas tradicionales en tres formas distintas: la cantidad de datos (volumen), la tasa de generación y transmisión de datos (velocidad) y los tipos de datos estructurados y no estructurados que puede manejar (variedad). Estas propiedades son conocidas como las tres Vs básicas de Big Data. El uso de Big Data en una compañía permite desarrollar un conocimiento más profundo del propio negocio lo que supone una gran ventaja competitiva [7].

Para conseguir que las medidas de seguridad adoptadas en una compañía sean efectivas, estas se tienen que encontrar alineadas con los objetivos y políticas de la empresa, además de gestionarse de forma conjunta, no de forma aislada. Para ello, se establece un gobierno de la seguridad [8]. Para la construcción de nuestra propuesta de marco de gobierno de la seguridad hemos tomado el estándar COBIT como base. COBIT [9] es un marco de gobierno de las tecnologías de la información que proporciona una serie de buenas prácticas y actividades para la dirección con el objetivo de alinear los requerimientos de control con los aspectos técnicos y los riesgos de negocio aumentando el valor de las organizaciones gracias a la tecnología. COBIT divide sus 34 procesos genéricos en cuatro dominios. Estos procesos son una serie de actividades unidos con una delimitación cuyo objetivo es lograr un resultado medible. Como forma de guía para el establecimiento y mejora de los procesos propuestos por COBIT, ISACA recomienda usar CMMI.

CMMI [10] es una colección de buenas prácticas y modelos cuyo objetivo es mejorar los procesos dentro de las organizaciones. Para ello, utiliza distintos niveles para evaluar el estado de los procesos de una organización. En nuestro caso, utilizaremos las buenas prácticas de las distintas áreas de proceso de CMMI como forma de facilitar la implementación de nuestra propuesta de marco GSB, y a su vez, poder determinar el estado de madurez en qué se encuentra dicho proceso.

3 Marco GSB

Nuestra propuesta de marco de gobierno denominada GSB (Gobierno de la Seguridad en entornos Big Data) tiene como objetivo cubrir el gobierno de la seguridad en un entorno Big Data durante todo su ciclo de vida. Se basa en tres pilares fundamentales: las características de seguridad de Big Data que fueron estudiadas mediante un *Systematic Mapping Study* realizado previamente [11], la estructura propuesta por COBIT de dominios de proceso y procesos como forma de generar el esqueleto, y CMMI como forma de hacer más accesible la implementación de los procesos de nuestro caso del marco GSB siguiendo sus recomendaciones y buenas prácticas.

Así, se han realizado una serie de modificaciones en los cuatro dominios de COBIT para adecuarlos a las necesidades específicas de nuestro marco. Además, se ha añadido un quinto dominio para el análisis de seguridad en Big Data. A continuación, se listan los cinco dominios que forman nuestra propuesta de marco GSB:

- **Planificación y organización (PO):** cubre la estrategia y las tácticas de la empresa, y busca identificar cómo Big Data puede contribuir al negocio.
- **Análisis de seguridad en Big Data (AS):** este dominio se encuentra compuesto de una serie de procesos necesarios para abordar la problemática de seguridad en entornos Big Data de forma más específica.
- **Diseño e implementación segura de Big Data (DI):** Con este dominio se busca llevar a cabo la estrategia en cuanto al entorno Big Data y cómo se debe realizar el diseño e implementación del entorno Big Data.
- **Operación segura de Big Data (OS):** este dominio busca abordar cómo se gestiona la seguridad de un entorno Big Data, una vez que este ya ha sido implementado en la compañía.
- **Monitorización y evaluación (ME):** este dominio evalúa el desempeño del sistema en cuanto a indicadores de seguridad, además también incluye un proceso de auditoría externa.

Una vez definidos los diferentes dominios que forman nuestra propuesta, se han ido analizando los procesos propuestos por COBIT para obtener los diferentes procesos que forman nuestra propuesta. Estos procesos pueden permanecer igual que en COBIT, sufrir modificaciones para adaptarlos a las necesidades específicas de seguridad de un entorno Big Data o haber sido creados de cero para incluir algún aspecto importante sobre gobierno de seguridad en Big Data que no forma parte de COBIT. En el Anexo I se recogen los diferentes dominios y procesos que forman nuestra propuesta.

Finalmente, CMMI nos permite añadir una nueva dimensión a nuestro marco de gobierno, que además de facilitar la implementación de los procesos con sus áreas de proceso y buenas prácticas, nos proporciona la posibilidad de evaluar la madurez de los diferentes procesos que forman nuestra propuesta. En el Anexo I, se muestra un ejemplo de cómo se relacionan las diferentes áreas de proceso de CMMI con los procesos definidos para el marco GSB, así como la relación con los niveles de madurez que propone CMMI.

4 Conclusiones y trabajo futuro

En este artículo se ha expresado la necesidad de crear un marco de gobierno de la seguridad para entornos Big Data que permita abordar la problemática de la seguridad durante todo su ciclo de vida. Para cumplir dicho objetivo se ha creado una propuesta de marco de gobierno bajo el nombre de marco GSB. Dicho marco toma como base la organización en dominios de procesos de COBIT. Nuestra propuesta de marco se divide en cinco dominios fundamentales los cuales, a su vez, se encuentran compuestos por 45 procesos relacionados con asegurar entornos Big Data. Además, como forma de hacer más sencilla la implantación de nuestro marco en una compañía, se ha integrado los distintos procesos con las áreas de proceso de CMMI. Finalmente, como trabajo futuro expresar la necesidad de definir con mayor detalle los diferentes controles y actividades que forman cada uno de los procesos, los cuales, deben ser específicos para entornos Big Data. Una vez realizadas estas inclusiones se validará nuestra propuesta de marco en un entorno real.

Agradecimientos

Este trabajo ha sido financiado por el proyecto SEQUOIA (Ministerio de Economía y Competitividad y Fondo Europeo de Desarrollo Regional FEDER, TIN2015-63502-C3-1-R) y por el proyecto SERENIDAD (Consejería de Educación, Ciencia y Cultura de la Junta de Comunidades de Castilla La Mancha, y Fondo Europeo de Desarrollo Regional FEDER, PEII-2014-045-P).

Referencias

1. Mayer-Schönberger, V., Cukier, K.: Big Data: A Revolution that Will Transform how We Live, Work, and Think. Houghton Mifflin Harcourt (2013).
2. S. Sagiroglu, D. Sinanc: Big data: A review. Collab. Technol. Syst. CTS 2013 Int. Conf. On. 42–47 (2013).
3. S. Sharma: Rise of Big Data and related issues. 2015 Annu. IEEE India Conf. INDICON. 1–6 (2015).
4. Eynon, R.: The rise of Big Data: What does it mean for education, technology, and media research? Learn. Media Technol. 38, 237–240 (2013).
5. Sharma, P.P., Navdeti, C.P.: Securing big data hadoop: a review of security issues, threats and solution. Int J Comput Sci Inf Technol. 5, (2014).
6. Soares, S.: Big Data Governance: An Emerging Imperative. Mc Pr Llc, Boise (2013).
7. Dijcks, J.P.: Oracle: Big data for the enterprise. Oracle White Pap. (2012).
8. Brotby, W.K.: Information Security Governance: Guidance for Information Security Managers. ISACA (2007).
9. ISACA, I.S.A. and C.A.: Cobit 5 A Business Framework for the Governance and Management of Enterprise. ISACA (2012).
10. Team, C.P.: CMMI for Development, Version 1.3 (CMU/SEI-2010-TR-033). Software Engineering Institute. Carnegie Mellon University (2010).
11. Moreno, J., Serrano, M.A., Fernández-Medina, E.: Main Issues in Big Data Security. Future Internet. 8, 44 (2016).

Anexo I – Dominios y procesos del marco GSB, y su relación con las áreas de proceso de CMMI

El objetivo de este anexo, es mostrar los diferentes dominios y procesos que forman el marco GSB. La Figura 1 recoge la división de los 45 procesos que componen nuestra propuesta en los 5 dominios.



Figura 1. Dominios y procesos del marco GSB

En la Tabla I se muestra la relación entre los procesos del dominio 2 sobre análisis de seguridad en Big Data con las áreas de proceso y niveles de madurez de CMMI.

Tabla I. Relación entre procesos y áreas de proceso de CMMI en el dominio 2

Procesos del dominio	Niveles de madurez y áreas de proceso			
	Nivel 2	Nivel 3	Nivel 4	Nivel 5
Análisis de seguridad en Big Data (AS)				
AS1 Definir requisitos de seguridad del entorno Big Data	REQM	RD		OID
AS2 Identificar diferentes alternativas de Big Data disponibles	CM, PPQA, REQM	DAR, RD, RSKM, TS, VAL, VER		
AS3 Análisis de seguridad de las diferentes alternativas de Big Data	PPQA, REQM	DAR, TS		
AS4 Determinar modelo del entorno Big Data	CM	DAR, OPD, PI, VAL, VER	QPM	OID
AS5 Análisis de riesgos del entorno	PMC	DAR, RSKM	QPM	