RESUMEN ANALÍTICO EN EDUCACIÓN - RAE –	UNIVERSIDAD CATÓLICA de Colombia

FACULTAD INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
BOGOTÁ D.C.

AÑO DE ELABORACIÓN: 2015

TÍTULO: GUÍA METODOLÓGICA PARA LA GESTIÓN CENTRALIZADA DE REGISTROS DE SEGURIDAD A TRAVÉS DE UN SIEM

AUTOR (ES): AVELLA CORONADO, Julián David, CALDERÓN BARRIOS, Leonardo Fabio y MATEUS DÍAZ, Cristian Andrés

DIRECTOR(ES)/ASESOR(ES):

VELANDIA, John A.

MODALIDAD:

PÁGINAS: 102 **TABLAS:** X **CUADROS:** 4 **FIGURAS:** 2 **ANEXOS:** 11

CONTENIDO:

PALABRAS CLAVES: ESTANDARES, GUÍA, EVENTOS, REGISTROS, NORMAS, SIEM

RESUMEN ANALÍTICO EN EDUCACIÓN - RAE –	UNIVERSIDAD CATÓLICA de Colombia

DESCRIPCIÓN: La Seguridad de la información en las organizacones, día tras día toma mayor relevancia por su importancia en la conservación de los datos y el daño que puede sufrir una organización cuando se vulnera su información. Las organizaciones deben implementar mecanismos para evitar que se materialice esta situación y es por ello que este proyecto busca guiar a las empresas en la implementacion de una herramienta que los ayude a prevenir e identificar situaciones de riesgo con la información y sistemas de la organización.

METODOLOGÍA: El enfoque de esta investigación es de carácter cualitativo, toda vez que se basa en las características y descripciones ya definidas para las soluciones SIEM de uso libre, y en un proceso de observancia en la implementación de un SIEM, proponiendo una guía metodológica que ayude en este proceso a las organizaciones.
Esta investigación es comparativa y proyectiva. Comparativa en cuanto se expondrán las características y descripciones de diferentes herramientas SIEM de uso libre y proyectiva, ya que una vez que se analicen las diferentes características de estas herramientas se propondrá una guía metodológica que ayude a su entendimiento y funcionalidad con el proceso de implementación en un caso de prueba.

CONCLUSIONES: Mediante este trabajo se identifican y se proponen fases para implementar un Sistema de Gestión de Registros, como parte fundamental en la arquitectura de la gestion de logs y para cumplir los objetivos en la seguridad de la información. Para las fases propuestas dependiendo de la estructura que maneja la empresa y la herramienta seleccionada, es posible obviar o adicionar algunas.

FUENTES:

Dave Shackleford, SANS Institute. (Octubre de 2014). SANS Institute (SysAdmin Audit, Networking and Security Institute). Obtenido de SANS Institute (SysAdmin Audit, Networking and Security Institute) Web Site: http://www.sans.org/reading-room/whitepapers/analyst/analyticsintelligence-survey-2014-35507

Force, J. T. (04 de 2013). National Institud of Standards and Technology (SP) 800-53. Recuperado el 31 de 05 de 2015, de Special Publication (SP) 800-53, Revision 4: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Jerry Shenk, SANS Institute. (Mayo de 2012). SANS Institute (SysAdmin Audit, Networking and Security Institute). Obtenido de SANS Institute (SysAdmin Audit,

Networking and Security Institute) Web Site: http://www.sans.org/reading-room/whitepapers/analyst/eighth-annual-2012- log-event-management-survey-results-sorting-noise-35230

Karen Kent, M. S. (Septiembre de 2006). National Institute of Standards and Technology. Obtenido de National Institute of Standards and Technology Web Site: http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

Netwrix Corporation. (2014). Netwrix Corporation. Obtenido de Netwrix Corporation Web Site: http://www.netwrix.com/download/documents/2014_SIEM_Efficiency_Survey_Report.pdf

Securosis blog. (25 de Agosto de 2010). Securosis. Obtenido de Securosis Blog: https://securosis.com/assets/library/reports/Securosis_Understanding_Selecting_SIEM_LM_FINAL.pdf

Swift, D. (4 de Noviembre de 2010). SANS Institute (SysAdmin Audit, Networking and Security Institute). Obtenido de SANS Institute (SysAdmin Audit, Networking and Security Institute) Web Site: http://www.sans.org/reading- 62 room/whitepapers/auditing/successful-siem-log-management-strategiesaudit-compliance-33528

CHUVAKIN, DR Anton A.; SCHMIDT, Kevin J.y PHILLIPS Chrispher. Logging AND Log Management The authoritative Guide to understanding the concepts Surrounding Logging and Log Management. Waltham: Elsevier, 2013.

LISTA DE ANEXOS:

RESUMEN ANALÍTICO EN EDUCACIÓN - RAE –	UNIVERSIDAD CATÓLICA de Colombia

Anexo K. Guía metodológica.