REVISTA ODIGOS

Período febrero - mayo 2023
Vol. 4, Núm. 1
rodigos@uisrael.edu.ec
https://doi.org/10.35290/ro.v4n1.2023.759 • e-ISSN: 2697-3405

Estudio de un sistema de seguridad de información y administración de eventos para base de datos SQL server. Caso de estudio: entidad pública

Study of a security information and event management for SQL Server database. Case study: public entity

Fecha de recepción: 2022-10-13 • Fecha de aceptación: 2023-01-04 • Fecha de publicación: 2023-02-10

Franklin Edwin Vela
Investigador Independiente, Ecuador
franklin_vela@hotmail.com
https://orcid.org/0000-0002-0858-3680

RESUMEN

La información de las organizaciones alojada en bases de datos es un activo muy importante que debe ser resguardada de ataques cibernéticos. En la investigación se identificaron amenazas que pueden poner en peligro el motor de base de datos SQL Server 2016 Standard y cómo estas podrían explotar las vulnerabilidades presentes Se propone realizar un estudio de un Security Information and Event Management (SIEM) para identificar si es una herramienta válida para disminuir los ataques que se puedan presentar en datos críticos; además, se revisan los controles que propone el Esquema Gubernamental de Seguridad de la Información Versión 2 (EGSI V2.0) en los que un SIEM

podría ayudar en su cumplimiento. Se evidenció que un SIEM detectó de manera oportuna incidentes de seguridad en la base de datos como son: ataques de inyección SQL, ataques de fuerza, entre otros; también se verificó que ayuda al cumplimiento de controles de EGSI V2.0 relacionados con control de accesos, seguridad de operaciones y gestión de incidentes de seguridad.

PALABRAS CLAVE: protección de datos, seguridad de datos, seguridad del Estado, programa informático, seguridad

ABSTRACT

The organizations' information hosted in databases is a very important asset and must be protected from cyber-attacks. In the investigation, threats than endanger the SQL Server 2016 Standard database engine were identified, and how it could exploit the present vulnerabilities. It is proposed to conduct a study of a Security Information and Event Manager (SIEM) to identify if it is a valid tool to reduce the attacks that critical data may suffer. Also, it was analyzed how a SIEM would contribute to comply with the controls of the Information Security Government Scheme version 2.0 (EGSI v2.0). It was demonstrated that a SIEM detected security incidents in the database in a timely manner such as: SQL injection attacks, force attacks, among others. It was also verified that it helps to comply with those EGSI V2.0 controls related to access control, operations security, and security incident management.

KEYWORDS: data protection, data security, state security, software, security

Introducción

El auge de nuevas tecnologías ha provocado que la información se distribuye casi de manera inmediata al mundo con el uso del internet (Abad, 2020); esta información es almacenada en bases de datos, en ellas se almacenan los datos apreciados como críticos, por lo que deben ser protegidos, los incidentes de seguridad ponen en riesgo la triada de la seguridad que es confidencialidad, integridad y disponibilidad; se debe buscar la manera de mitigar los ciberataques que se puedan producir.

La Ley Orgánica de Protección de Datos Personales tiene como objetivo “garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección” (Asamblea Nacional, 2021). Los funcionarios públicos deben garantizar que los datos personales sean protegidos y respaldados, de no acatar la ley existirán sanciones.

El Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) expidió el EGSI V2.0, el cual es de implementación obligatoria en el sector público en el Ecuador; “esta normativa trata de resguardar «la confidencialidad, integridad y disponibilidad de la información por medio de la ejecución de un proceso de gestión de riesgos de seguridad de la información y la selección de controles para el tratamiento de los riesgos identificados” (Corte Constitucional del Ecuador, 2020); el esquema mencionado obliga a las instituciones públicas a implementar métodos de protección y seguimiento dentro de la infraestructura para minimizar, los riesgos que se puedan producir por amenazas que aprovechan vulnerabilidades presentes.

Los ataques informáticos hacia bases de datos se han intensificado desde el inicio de la pandemia, la angustia de buscar respuestas a los problemas generados por la propagación rápida y mortal del virus (Bartolomé y Monteiro, 2021), hizo que las personas naveguen de manera asidua por el internet. Además, existió un alto porcentaje de personas que fueron obligados a realizar teletrabajo, esto abrió una brecha de seguridad; los empleados se conectan remotamente a sus oficinas por medio de servicios de escritorio remoto desde equipos como: computadores, celulares, *tablets*, etc., esto es aprovechado por delincuentes informáticos para acceder a la red de las organizaciones.

Un desafío crítico para muchas organizaciones modernas es comprender cómo minimizar el costo de administrar y proteger sus activos de información y sistemas comerciales (Jacobs et al., 2020). Esto podría darse utilizando un SIEM que ayude a visualizar los ataques que se estén presentando de una manera amigable.

El presente artículo está dirigido al personal que tiene como función la seguridad de los datos dentro de las organizaciones, ellos son responsables de dictar las políticas que rigen la protección de las bases de datos; además, tiene como objetivo realizar un estudio de un SIEM sobre la base de datos SQL Server 2016 Standard para una posible implementación en las entidades públicas del Ecuador.

Metodología

Para la investigación se utilizó el método bibliográfico comparativo, se procedió a leer literatura sobre el funcionamiento de los Security Information and Event Management, casos de estudio, artículos de investigación, tesis, implementaciones; además, se identificaron los controles del EGSI V2.0 en los que un SIEM puede ayudar en su cumplimiento. También se analizó el comportamiento de esta herramienta para conocer su capacidad de detección ante ataques que se pueden dar en un motor de base de datos.

Se plantea analizar cómo un SIEM para las bases de datos en una entidad pública ayudaría a mejorar los controles del EGSI V2.0, estudiando el estado de los parámetros de la normativa antes del estudio y posterior al mismo.

Luego del estudio se muestran las conclusiones con las que se define si un correlacionador de eventos es un aporte valedero a la protección de una base de datos SQL Server 2016 Standard y ayuda a la implementación del EGSI V2.0 en una entidad pública, el motor de base de datos analizado es el principal repositorio con la que actualmente se trabaja en la organización.

Etapas del proceso investigativo:

- Definir vulnerabilidades en una base de datos.
- Establecer el SIEM a utilizar.
- Estudiar las características del SIEM para protección de bases de datos SQL Server.
- Configuración de alertas en el SIEM.
- Valorar la situación actual de las bases de datos.
- Valorar la situación actual de los controles del EGSI V2.0.
- Evaluar situación propuesta de las bases de datos con el SIEM.
- Evaluar situación propuesta de los controles del EGSI V2.0 con el SIEM.
- Analizar resultados.

2.1 Conceptos generales

Martínez y Tejada (2019, p.15) indican que una base de datos es un conjunto de información relacionada agrupada y organizada; desde la perspectiva informática, una base de datos es un sistema que está formado por una agrupación de datos almacenados en medios que permiten el acceso de manera directa a ellos y un conjunto de aplicativos que manipulen esa información.

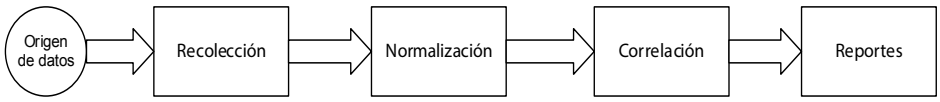
Un Security Information and Event Management (SIEM) genera un estudio en línea de las alarmas de seguridad informática suscitadas en el *hardware* y *software* de la infraestructura (Cómbita, 2018). Un SIEM permite la automatización de la detección de incidentes y las reacciones

posteriores para mitigar los incidentes inminentes; al mismo tiempo ayuda a preservar pruebas forenses (Vielberth & Pernul, 2018).

Un sistema SIEM está formado por dos tecnologías de seguridad, un Security Event Manager (SEM) tiene como misión detectar patrones de acceso fuera de lo común en tiempo real, y un Security Information Management (SIM) que permite centralizar eventos de seguridad para almacenarlos e interpretarlos en tiempo real, ayudando a una reacción de manera expedita.

Figura 1

Capas de un SIEM



Las capas de un correlacionador de eventos según Pazmiño y Pazmiño (2018) son:

- Recolección de eventos: en esta capa el SIEM recolecta los eventos de los diferentes dispositivos desplegados en la infraestructura (*Firewall*, bases de datos, IPS, IDS, etc.) para ser enviados a la capa de normalización.
- Capa de normalización, su misión es normalizar todos los registros que son recogidos en el SIEM, de tal forma que una vez culminada esta etapa tengan el mismo estándar de datos y sigan a la capa de correlación.
- Capa de correlación: tienen el objetivo principal de crear relaciones entre los registros y los eventos de seguridad que se presenten en los diferentes dispositivos desplegados en la red, si encuentra alguna anomalía lo notifica.
- Capa de reporte: se encarga de estudiar los datos enviados por la capa de correlación, los procesa y genera reportes que serán presentados a los administradores de seguridad.

Un SIEM ayuda a los administradores de infraestructura a desarrollar políticas de seguridad y administrar eventos desde diferentes fuentes (González et al., 2021). En los motores de bases de datos un SIEM sirve para recolectar todos los registros (accesos a la base de datos, cambios en los datos, intentos de ataques, etc.) que se producen, centralizarse y definir qué acciones realizar si se da algún tipo de evento no controlado o inesperado.

Las principales amenazas encontradas en una base de datos son: amenazas internas, vulnerabilidades de *software* de bases de datos, ataques de inyección SQL, pistas de auditoría débiles, ataques de denegación de servicio, *malware*, privilegios excesivos, abuso de privilegios, elevación de privilegios (Hashim, 2018).

Los controles a los que un SIEM ayuda en la ejecución del EGSI V2.0 son: 5.1.1 Política de control de acceso; 8.2.1 Controles contra *malware*, Registro de eventos; 8.4.2 Protección de los registros de información; 8.4.3 Registros de administración y operación; 8.6.1 Gestión de las vulnerabilidades técnicas; 8.7.1 Controles de auditoría de sistemas de información;

12.1.1 Responsabilidades y procedimientos; 12.1.2 Reporte de los eventos de seguridad de la información; 12.1.3 Reporte de debilidades de seguridad de la información; 12.1.4 Apreciación y decisión sobre los eventos de seguridad de la información; 12.1.5 Respuesta a incidentes de seguridad de la información; 12.1.6 Aprendizaje de los incidentes de seguridad de la información (Corte Constitucional del Ecuador, 2020).

Resultados

Al pasar los años, la tecnología ha evolucionado en lo referente a protección de infraestructura, ya sea redes, servidores o base de datos, siendo lo último lo más apetecido por los *hackers*. Si los datos críticos caen en manos de los delincuentes informáticos pueden solicitar un rescate, vender esa información, o un sinnúmero de problemas a la confidencialidad de la información; los ciberataques desafían la manera tradicional en que las organizaciones se defendían y puede ocasionar inestabilidad (Cano, 2020).

El MINTEL, por medio del Acuerdo Ministerial **nº** 006-2021, en el artículo 1 publica la Política de Ciberseguridad, dentro de sus objetivos y líneas de acción indica como un objetivo lo siguiente: "potenciar las capacidades de detección, previsión, prevención y gestión de los incidentes cibernéticos, al igual que el manejo de crisis de ciberseguridad de manera oportuna, efectiva, eficiente y coordinada" (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021). Esta política debe buscar los mecanismos para potenciar la ciberseguridad, esta se enfocará en la seguridad informática del motor de base de datos SQL Server.

3.1 Amenazas hacia las bases de datos SQL Server antes del SIEM

En la *Tabla 1* se muestra el estado actual de las amenazas que se tiene en las bases de datos SQL Server 2016 de una entidad pública antes de utilizar un SIEM; se observa que las vulnerabilidades en las bases de datos tienen un impacto medio-alto de criticidad, los huecos de seguridad no han sido atendidos, no existen herramientas que permitan monitorear si existe alguna vulnerabilidad o si se está siendo atacado, la respuesta a incidentes es reactiva, se reacciona una vez que se produce el ataque.

Tabla 1

Estado Actual de Amenazas en la Base Datos SQL Server

Vulnerabilidad de base de datos	Situación actual	Impacto
Amenazas internas	No se tiene una bitácora que identifique, la creación, modificación o eliminación de usuarios de base de datos.	Alto
Vulnerabilidades de software	No se posee una herramienta que realice un despliegue de las actualizaciones en el motor de base de datos, los updates se los realiza de forma manual.	Medio
Ataques de inyección SQL	No existe algún método para identificar si las bases de datos están siendo atacadas por este ataque.	Alto

Pistas de auditoría débiles	No existen pistas de auditoría habilitadas dentro del motor de base de datos, se considera que al activar esta característica se perderán recursos que afecten al funcionamiento del servicio.	Alto
Ataques de denegación de servicio	Se posee herramientas propias del motor de base de datos para identificar sesiones conectadas, pero no se tiene centralizado los logs de inicio de sesión, esto no permite medir si existen más conexiones de las usuales que consuman los recursos del servidor y ocasionen su colapso.	Alto
Malware	Al momento se tiene instalado antivirus para detectar malware en los servidores de base de datos, esto implica que se debe esperar a que el proveedor actualice sus bases para estar protegido, no existe defensa para malware del día cero.	Medio
Privilegios excesivos	No se mantiene un registro de los usuarios creados, es difícil identificar qué sentencias SQL han sido ejecutadas.	Alto
Abuso de privilegios	Es difícil identificar que hacen los usuarios dentro de las bases de datos, no se tiene una auditoría de las tablas.	Alto
Elevación de privilegios	No se puede visualizar que sentencias SQL tipo DDL y DML se ejecutan, esto no permite a los operadores verificar si los usuarios están realizando actividades no permitidas.	Alto

La *Tabla 2* muestra el porcentaje del impacto hacia las bases de datos por las vulnerabilidades detectadas, el 77,78% de las amenazas tienen un estado crítico; esto implica que un atacante puede acceder a datos de la organización sin que se presente algún tipo de registro de lo sucedido, el 22,22% están en estado medio, lo que representa que con conocimientos medios sobre cómo explotar las vulnerabilidades un *hacker* podría acceder a la información.

Tabla 2

Impacto de Vulnerabilidades en las Bases de Datos

Impacto	N° Vulnerabilidades	Porcentaje
Alto	7	77,78%
Medio	2	22,22%
Total	9	100,00%

3.2 Estado actual de controles del EGSI V2.0 antes de implementar un SIEM

Se han identificado las secciones del EGSI V2.0, en las cuales un SIEM para base de datos puede ayudar a subir el índice de cumplimiento de los controles; estos son los que necesitan registro, almacenamiento y disponibilidad de los incidentes de seguridad.

En la *Tabla 3* se observan trece controles de EGSI V2.0 que fueron evaluados por una entidad pública en los que se hace necesaria la implementación de herramientas tecnológicas que ayuden a gestionar incidentes de seguridad y manejan una base de datos que archive estos eventos, es así como se sugirió la utilización de un SIEM el cual ayudaría a mejorar el estado de los hitos para el cumplimiento de la norma; además, se agregó una columna para las observaciones donde se indica el avance o de ser el caso implementación del control. El estado actual de los hitos maneja tres opciones; NO SE EJECUTA, significa que el control no se cumple, no existe ningún documento

que respalde su desarrollo ni consta de alguna herramienta tecnológica que ayude a la ejecución; PARCIALMENTE, se refiere a que existe un documento (política, procedimiento, proceso, etc.) que avale el control, pero no tiene un *software* que ayude al monitoreo y control del hito; SE EJECUTA, el control está integrado completamente.

Tabla 3

Estado Actual de Controles del EGSI V2.0 en una Entidad Pública

Dominio	Categoría	Objetivos de control	Control	Observación	Estado
5 Control de acceso	5.1 Requisitos institucionales para el control de acceso	5.1.1 Política de control de acceso	Elaborar, implementar y socializar la política de control de acceso a los sistemas de información, de acuerdo con la necesidad institucional y considerando la seguridad de la información.	Se encuentra creada la política de control de accesos, no existe un repositorio donde se guardan los *logs* de acceso a las bases de datos.	PARCIALMENTE
8 Seguridad de las operaciones	8.2 Protección contra un *malware*	8.2.1 Controles contra *malware*	Implementar controles para detectar, prevenir y recuperarse de afectaciones de *malware*, en combinación con la concientización adecuada a los usuarios.	Se tiene instalado en los servidores antivirus licenciados, no se puede visualizar si un equipo está siendo atacado por un *malware*.	PARCIALMENTE
	8.4 Registro y monitoreo	8.4.1 Registro de eventos	Implementar el procedimiento para registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.	No existen procedimientos para registrar eventos ni almacenamiento de estos.	NO SE EJECUTA
		8.4.2 Protección de los registros de información	Establecer el procedimiento para proteger contra posibles alteraciones y accesos no autorizados la información de los registros	No existe un repositorio central para almacenar los cambios que se realizan sobre las bases de datos, no se puede realizar un estudio forense de ser requerido.	NO SE EJECUTA
		8.4.3 Registros de administración y operación	Registrar, proteger y revisar regularmente de acuerdo con las necesidades de la institución; las actividades del administrador y del operador del sistema.	No existe un repositorio central para almacenar registros, no se puede realizar un análisis de ser requerido.	NO SE EJECUTA
	8.6 Gestión de la vulnerabilidad técnica	8.6.1 Gestión de las vulnerabilidades técnicas	Elaborar e Implementar la política de monitoreo continuo sobre los sistemas en producción, detectar vulnerabilidades técnicas, adoptar las medidas necesarias para afrontar el riesgo asociado.	No se tiene definido un procedimiento para el registro de vulnerabilidades, no se registran los ataques que se puedan presentar en las bases de datos.	NO SE EJECUTA

	8.7 Consideraciones sobre la auditoría de sistemas de información	8.7.1 Controles de auditoría de sistemas de información	Planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas en producción con el objetivo de minimizar las interrupciones en los procesos relacionados con la institución.	No existen registros de las acciones que se realizan sobre las bases de datos.	NO SE EJECUTA
12 Gestión de incidentes de seguridad de la información	12.1 Gestión de los incidentes de seguridad de la información y mejoras	12.1.1 Responsabilidades y procedimientos	Establecer formalmente responsabilidades y procedimientos para asegurar una respuesta rápida, efectiva y acorde a los Incidentes de seguridad de la Información que pueden ocurrir en la Institución.	No existe un procedimiento definido, ni tampoco una herramienta que permita tener respuestas inmediatas y envío de notificaciones a los responsables de mitigar incidentes de seguridad.	PARCIALMENTE
		12.1.2 Reporte de los eventos de seguridad de la información	Elaborar, implementar y socializar el procedimiento formal para reportar los eventos de seguridad de la información, a través de los canales respectivos.	Se realizan reportes posteriores a los ataques, no existen alertas tempranas.	PARCIALMENTE
		12.1.3 Reporte de debilidades de seguridad de la información	Los funcionarios de la institución, contratistas o terceras partes deben obligatoriamente registrar y reportar, cualquier debilidad probable en la seguridad de la información, en los sistemas o servicios de información de la institución.	Se reportan vulnerabilidades detectadas de forma manual, no existe una herramienta que detecte los huecos de seguridad de manera temprana.	PARCIALMENTE
		12.1.4 Apreciación y decisión sobre los eventos de seguridad de la información	Evaluar los eventos de seguridad de la información y decidir si se clasifican como incidentes de seguridad de la información.	Al no tener una herramienta que correlacione eventos no se puede evaluar los incidentes de seguridad en las bases de datos.	NO SE EJECUTA
		12.1.5 Respuesta a incidentes de seguridad de la información	Aplicación de procedimientos establecidos, para responder ante incidentes de seguridad de la información.	Al no contar con una herramienta que reporte incidentes de seguridad en las bases de datos, no se tiene una respuesta rápida.	NO SE EJECUTA
		12.1.6 Aprendizaje de los incidentes de seguridad de la información	Utilizar el conocimiento obtenido para analizar y resolver Incidentes de seguridad de la información, para reducir la probabilidad y/o impacto de incidentes en el futuro, aplicando los controles adecuados.	Al no contar con un colector de eventos de seguridad para base de datos, no se puede resolver de manera rápida los incidentes.	NO SE EJECUTA

En la *Tabla 4* se muestra el porcentaje de cumplimiento de los controles que fueron analizados para esta investigación, se observa que el 61,54% de los controles estudiados en la entidad pública no están cumpliendo los lineamientos requeridos, un 38,46% cumplen la normativa parcialmente y ningún hito cumple al 100% lo dispuesto por el MINTEL.

Tabla 4

Cumplimiento de Controles

Estado	N° Controles	Porcentaje
No se ejecuta	8	61,54%
Parcialmente	5	38,46%
Se ejecuta	0	0,00%
Total	13	100,00%

Se hace necesario el uso de una herramienta tecnológica que ayude al personal a gestionar los incidentes de seguridad y puedan enfocar sus esfuerzos a tareas para subsanar los eventos detectados.

3.3 Arquitectura propuesta para el estudio de un Security Information And Event Management para base de datos SQL Sever

En la *Figura 2* se muestra la arquitectura propuesta que se usó para realizar el estudio de un SIEM para base de datos SQL Server en una entidad pública.

Figura 2

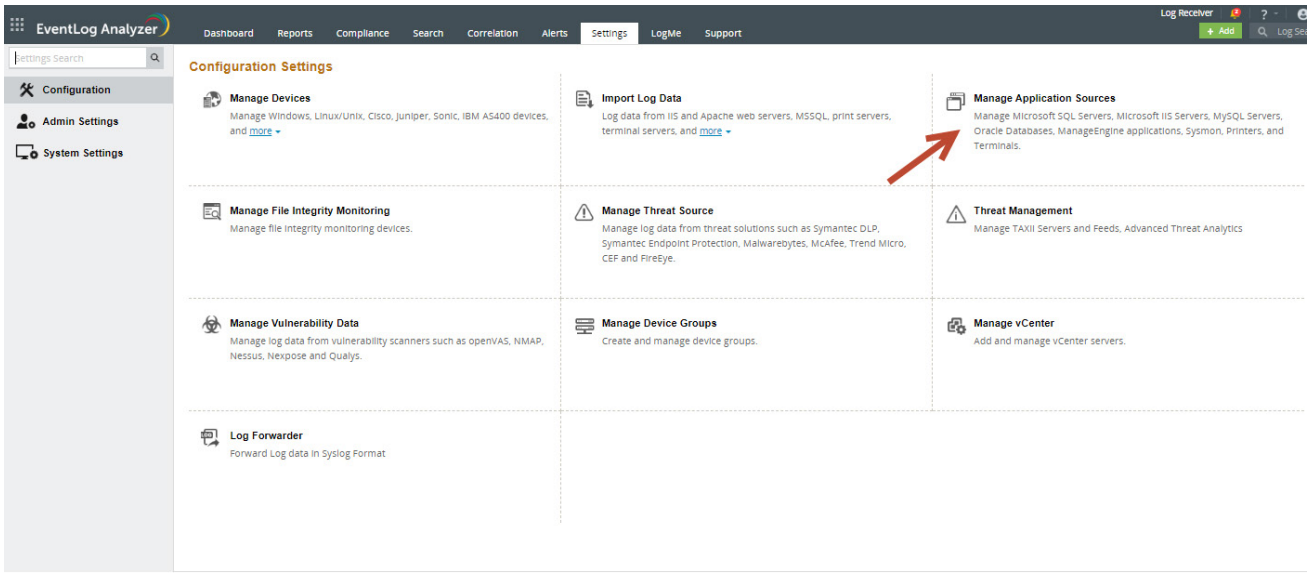
Arquitectura Propuesta

La arquitectura muestra una máquina virtual con el sistema operativo Windows Server 2016 Standard que tiene instalado el SIEM; este correlacionador de eventos maneja una base de datos PostgreSQL, las pruebas fueron realizadas en un ambiente controlado.

Para la investigación se ingresaron dos servidores de base de datos; el primero es de producción y el segundo de pruebas. En la *Figura 3* se muestra la consola para agregar bases de datos al SIEM. El servidor de producción sirvió para recolectar información de los eventos de seguridad de la base de datos SQL Server 2016 Standard sin realizar ninguna afectación a la data; el equipo de pruebas fue usado para revisar eventos de seguridad dentro de las bases de datos que requerían modificaciones en sus objetos como son tablas, usuarios, entre otros.

Figura 3

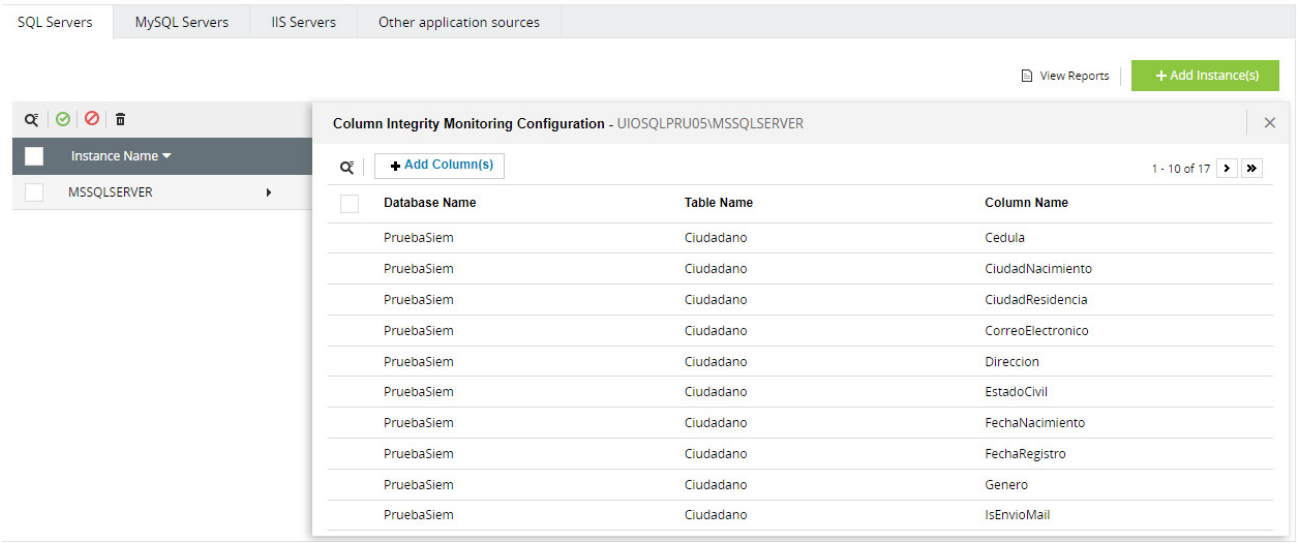
Dashboard para Agregar Servidores de Base de Datos



En la *Figura 4* se muestran algunas tablas que fueron auditadas.

Figura 4

Tablas para Auditar



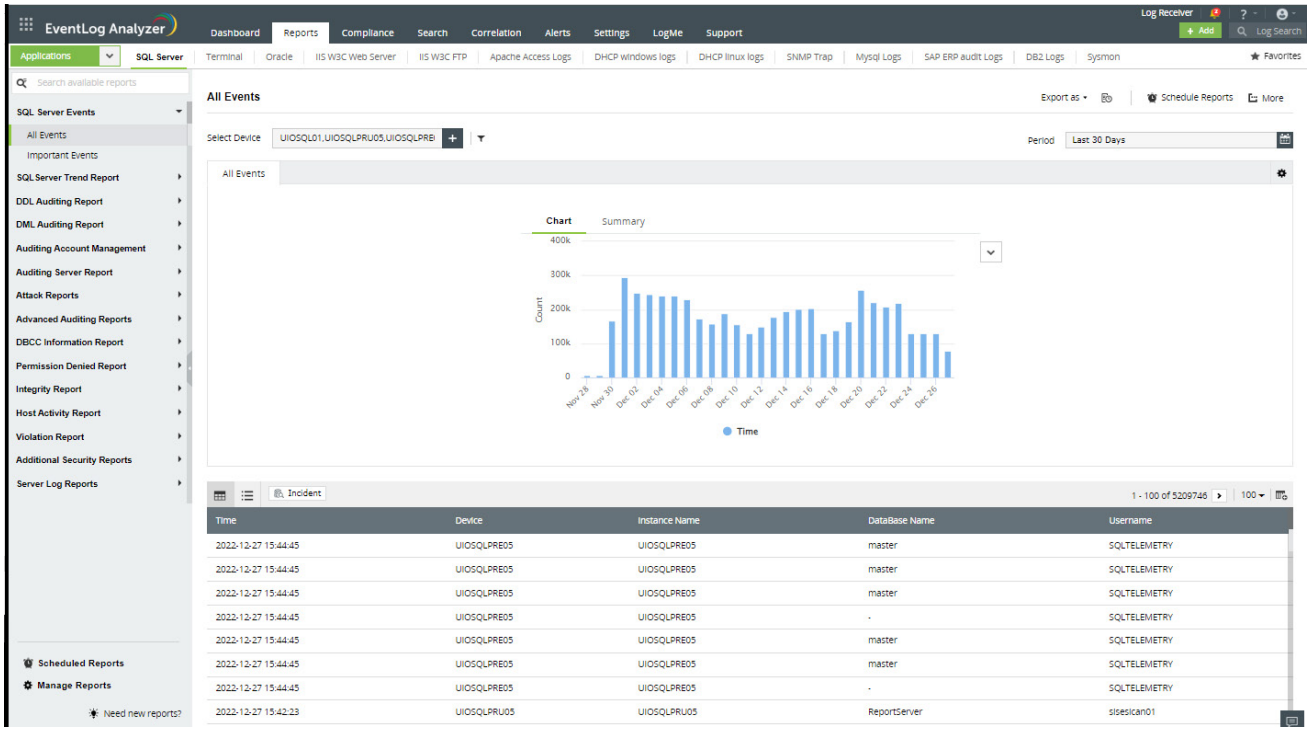
El correlacionador de eventos utilizado para el estudio tiene las siguientes características (*Auditoría de bases de datos | Software de auditoría de bases de datos - ManageEngine EventLog Analyzer*, s. f.):

- Gestión integral.
- Monitoreo de la actividad de la base de datos.
- Monitoreo del *log* del servidor de base de datos.
- Monitoreo de la seguridad de la base de datos.
- Análisis exhaustivo.

El SIEM examinado maneja una variedad de reportes que permite a los operadores tener una visión amplia de los problemas de seguridad que se pueden presentar en las bases de datos. Un ejemplo de los reportes se muestra en la *Figura 5*.

Figura 5

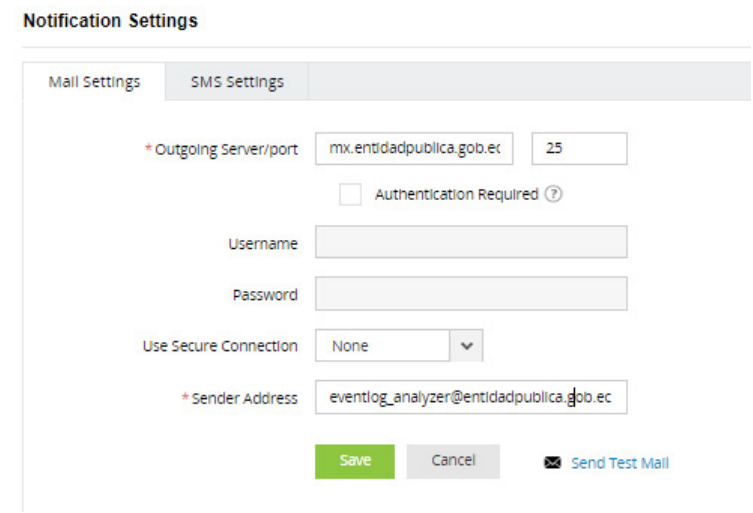
Reportes SIEM



Se configuraron las notificaciones de los incidentes que se puedan presentar; en este caso se escogió el envío de alertas por medio de correo electrónico, se cuenta con servidores de correo de Microsoft que permiten una integración fácil con la herramienta; se seleccionó un operador al cual le llegarán las notificaciones, como se muestra en la *Figura 6.*

Figura 6

Configuración de Notificaciones



3.4 SIEM Mitigación de ataques a bases de datos con un SIEM

Después del estudio del SIEM se identificaron qué características podrían ser usadas para remediar las vulnerabilidades presentes en las bases de datos de la entidad pública, evidenciando que el impacto de las amenazas cambió.

En la *Tabla 5* se observa como un SIEM ayuda a mitigar los ataques a las bases de datos, existen amenazas que cambiaron de estado crítico a medio y de medio a bajo, esto significa que el monitoreo y recolección de registros de eventos de seguridad ayudan notablemente a mejorar la seguridad y disminuir posibles intrusiones a los datos críticos de la entidad pública.

Tabla 5

Mitigación de Ataques a las Bases de Datos SQL Server con un SIEM

Vulnerabilidades	Situación actual	Situación propuesta con un SEIM	Impacto
Amenazas internas	No se tiene una bitácora que identifique, la creación, modificación o eliminación de usuarios de base de datos.	El SIEM recoge eventos de seguridad de las bases de datos requeridas y los almacena.	Bajo
Vulnerabilidades de software	No se posee una herramienta que realice un despliegue de las actualizaciones en el motor de base de datos, los updates se los realiza de forma manual.	El SIEM estudiado no posee una característica para controlar actualizaciones del gestor de base de datos.	Medio
Ataques de inyección SQL	No existe algún método para identificar si las bases de datos están siendo atacadas por este ataque.	El SIEM Eventlog Analyzer permite detectar de manera automática este tipo de ataques, también toma acciones correctivas.	Medio
Pistas de auditoría débiles	No existen pistas de auditoría habilitadas dentro del motor de base de datos, se considera que al activar esta característica se perderán recursos que afecten al funcionamiento del servicio.	Los registros de eventos de seguridad son recolectados de manera ordenada por el SIEM, se mejora la identificación de evidencias para un proceso forense digital.	Bajo
Ataques de denegación de servicio	Se posee herramientas propias del motor de base de datos para identificar sesiones conectadas, pero no se tiene centralizado los logs de inicio de sesión, esto no permite medir si existen más conexiones de las usuales, que consuman los recursos del servidor y ocasionen su colapso.	La herramienta tiene un módulo que permite de manera automática la identificación del ataque DoS, se pueden tomar acciones correctivas inmediatamente.	Medio
Malware	Al momento se tiene presente antivirus para detectar malware en los servidores de base de datos, esto implica que se debe esperar a que el proveedor actualice sus bases para estar protegido, no existe defensa para malware del día cero.	Eventlog Analyzer puede relacionarse con las bases de datos de proveedores de antivirus, además con fuentes de información sobre ataques, esto ayuda a mitigar ataques de día cero.	Bajo
Privilegios excesivos	No se mantiene un registro de los usuarios creados, es difícil identificar qué sentencias SQL han sido ejecutadas.	La herramienta SIEM, permite monitorear que acciones se realizan sobre los objetos de las bases de datos, así como en la data.	Bajo
Abuso de privilegios	Es difícil identificar qué hacen los usuarios dentro de las bases de datos, no se tiene una auditoría de las tablas.	Eventlog Analyzer, genera reportes sobre las tareas que los usuarios realizan o tratan de realizar sobres los datos.	Bajo
Elevación de privilegios	No se puede visualizar que sentencias SQL tipo DDL y DML se ejecutan, esto no permite a los operadores verificar si los usuarios están realizando actividades no permitidas.	Se recopila ordenadamente todos los eventos de seguridad de las bases de datos en el SIEM, se observa que acciones DDL y DML se ejecutan.	Bajo

La *Tabla 6* muestra que existe un porcentaje del 33,33% de vulnerabilidades que tienen un estado medio, el 66,67% de vulnerabilidades son mitigadas con la ayuda de un SIEM y no existen amenazas en estado crítico que afecten a las bases de datos.

En resumen, se nota que la seguridad hacia los datos críticos ha mejorado sustancialmente.

Tabla 6

Impacto de Vulnerabilidades en las Bases de Datos con un SIEM

Estado	N° Vulnerabilidades	Porcentaje
Crítico	0	0,00%
Medio	3	33,33%
Bajo	6	66,67%
Total	9	100,00%

3.5 Situación propuesta de controles de EGSI V2.0 con un SIEM

Luego de la instalación y configuración del SIEM, se volvieron a analizar los trece controles, se verificó que con, la recolección de *logs* de seguridad, envío de notificaciones de alertas hacia los operadores, correlación de eventos, definición de reglas propias, entre otros se minimizó la probabilidad de que las vulnerabilidades de las bases de datos sean explotadas, ayudando al cumplimiento del EGSI V2.0.

En la *Tabla 7*, se observa que una herramienta SEIM aporta al fortalecimiento de los controles del EGSI V2.0. Los trece controles analizados se reforzaron y podrían ser implementados en su totalidad en la entidad pública.

Tabla 7

Estado Propuesto de Controles del EGSI V2.0 con un SIEM

Dominio	Categoría	Objetivos de control	Control	Observación	Control reforzado	Estado
5 Control de Acceso	5.1 Requisitos institucionales para el control de acceso	5.1.1 Política de control de acceso	Elaborar, implementar y socializar la política de control de acceso a los sistemas de información, de acuerdo con la necesidad institucional y considerando la seguridad de la información.	Elaborar, implementar y socializar la política de control de acceso a los sistemas de información, de acuerdo con la necesidad institucional y considerando la seguridad de la información.	El SIEM, centraliza los incidentes de seguridad, permite monitorear y tener respaldos de la información de eventos de seguridad para futuros análisis.	SE EJECUTA

8 Seguridad de las operaciones	8.2 Protección contra un malware	8.2.1 Controles contra malware	Implementar controles para detectar, prevenir y recuperarse de afectaciones de malware, en combinación con la concientización adecuada a los usuarios.	Se tiene instalado en los servidores antivirus licenciados, no se puede visualizar si un equipo está siendo atacado por un malware.	La herramienta SIEM permite recolectar información de los servidores de antivirus, además de tener actualizada la base de conocimientos de fuentes internacionales para prevenir ataques.	SE EJECUTA
	8.4 Registro y monitoreo	8.4.1 Registro de eventos	Implementar el procedimiento para registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.	No existen procedimientos para registrar eventos, ni almacenamiento de estos.	SIEM recolecta eventos de seguridad de las diferentes bases de datos SQL Server, esto permite ser proactivos ante algún tipo de ataque.	SE EJECUTA
		8.4.2 Protección de los registros de información	Establecer el procedimiento para proteger contra posibles alteraciones y accesos no autorizados la información de los registros	No existe un repositorio central para almacenar que cambios se realizan sobre las bases de datos, no se puede realizar un estudio forense de ser requerido.	Los logs de seguridad son almacenados en el SIEM, estos no pueden ser modificados.	SE EJECUTA
		8.4.3 Registros de administración y operación	Registrar, proteger y revisar regularmente de acuerdo con las necesidades de la institución; las actividades del administrador y del operador del sistema.	No existe un repositorio central para almacenar registros, no se puede realizar un análisis de ser requerido.	La herramienta SIEM almacena los eventos en una base de datos de manera segura, el frond end de la aplicación permite visualizar de manera gráfica los eventos de seguridad.	SE EJECUTA
	8.6 Gestión de la vulnerabilidad técnica	8.6.1 Gestión de las vulnerabilidades técnicas	Elaborar e implementar la política de monitoreo continuo sobre los sistemas en producción, detectar vulnerabilidades técnicas, adoptar las medidas necesarias para afrontar el riesgo asociado.	No se tiene definido un procedimiento para el registro de vulnerabilidades, no se registran los ataques que se puedan presentar en las bases de datos.	La política no ha sido redactada, pero el SIEM, detecta amenazas hacia las bases de datos de manera temprana, además, notifica a los técnicos para que de ser el caso mitiguen el ataque o programen a la herramienta para que esté lo haga.	PARCIALMENTE

	8.7 Consideraciones sobre la auditoría de sistemas de información	8.7.1 Controles de auditoría de sistemas de información	Planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas en producción con el objetivo de minimizar las interrupciones en los procesos relacionados con la institución.	No existen registros de las acciones que se realizan sobre las bases de datos.	EL correlacionador de eventos recopila los incidentes de seguridad generados, permite tener una rotación de log parametrizable, estos registros no pueden ser accedidos por los operadores, solo por el aplicativo, permite realizar un análisis forense.	SE EJECUTA
12 Gestión de incidentes de seguridad de la información	12.1 Gestión de los incidentes de seguridad de la información y mejoras	12.1.1 Responsabilidades y procedimientos	Establecer formalmente responsabilidades y procedimientos para asegurar una respuesta rápida, efectiva y acorde a los Incidentes de seguridad de la Información que pueden ocurrir en la Institución.	No existe un procedimiento definido, tampoco una herramienta que permita tener respuestas inmediatas y envío de notificaciones a los responsables de mitigar incidentes de seguridad.	No existe el procedimiento, pero el SIEM permite notificar al operador sobre la amenaza, esto permite que la persona se enfoque en buscar una solución y no que la ocasionó.	PARCIALMENTE
		12.1.2 Reporte de los eventos de seguridad de la información	Elaborar, implementar y socializar el procedimiento formal para reportar los eventos de seguridad de la información, a través de los canales respectivos.	Se realizan reportes posteriores a los ataques, no existe alertas tempranas.	Existe el procedimiento, la herramienta analizada permite parametrizar reportes sobre los ataques, estos pueden ser enviados por correo electrónico o mensajes SMS, lo que hace que la detección sea más fácil.	SE EJECUTA
		12.1.3 Reporte de debilidades de seguridad de la información	Los funcionarios de la institución, contratistas o terceras partes deben obligatoriamente registrar y reportar, cualquier debilidad probable en la seguridad de la información, en los sistemas o servicios de información de la institución.	Se reportan vulnerabilidades detectadas de manera manual, no existe una herramienta que detecta las vulnerabilidades de manera adelantada.	Las vulnerabilidades detectadas se guardan en la base de datos de la herramienta, se reporta sobre la amenaza inmediatamente al funcionario designado, de existir una tarea programada se ejecuta la acción automáticamente.	SE EJECUTA
		12.1.4 Apreciación y decisión sobre los eventos de seguridad de la información	Evaluar los eventos de seguridad de la información y decidir si se clasifican como incidentes de seguridad de la información.	Al no tener una herramienta que correlacione eventos, no se puede evaluar los incidentes de seguridad en las bases de datos.	El SIEM detecta más fácilmente las amenazas hacia las bases de datos SQL Server, los dashboards de la herramienta permiten visualizar estadísticas sobre ataques e identificar qué tipo de amenaza se presenta.	SE EJECUTA

	12.1.5 Respuesta a incidentes de seguridad de la información	Aplicación de procedimientos establecidos, para responder ante incidentes de seguridad de la información.	Al no contar con una herramienta que muestre los reportes de incidentes de seguridad en las bases de datos, no se tiene una respuesta rápida.	El SIEM permite responder de manera rápida a los incidentes de seguridad, ya que cuenta con estadísticas de ataques y envíos de notificaciones.	SE EJECUTA
	12.1.6 Aprendizaje de los incidentes de seguridad de la información	Utilizar el conocimiento obtenido para analizar y resolver Incidentes de seguridad de la información, para reducir la probabilidad y/o impacto de incidentes en el futuro, aplicando los controles adecuados.	Al no contar con un colector de eventos de seguridad para base de datos, no se puede resolver de manera rápida los incidentes.	Los ataques detectados por el SIEM permiten a los operadores aprender de los incidentes y reaccionar de manera oportuna.	SE EJECUTADO

En la *Tabla 8* se muestra como el 83,33% de los controles podrían estar implementados en su totalidad y el 16,67% tendrían una implementación parcial, esto se debe a que, pese a tener la herramienta tecnológica funcionando y gestionando los eventos de seguridad, no se han elaborado las políticas y procedimientos restantes, esto coadyuva a no cumplir con el EGSI V2.0 en su totalidad.

Tabla 8

Cumplimiento de Controles con un SIEM

Estado	No. Controles	Porcentaje
No se ejecuta	0	0,00%
Parcialmente	2	16,67%
Se ejecuta	10	83,33%
Total	12	100,00%

Conclusiones

El SIEM posee *dashboards* de fácil interpretación, estos ayudan a los operadores a identificar los ataques que se presentan, se tienen además alertas que son enviadas por correo electrónico que permiten una intervención inmediata para detener los ataques que se están presentando. También, maneja una base de datos que guarda todos los eventos registrados y ayudan a realizar auditorías; la herramienta tiene integrado reportes que son parametrizables, estos pueden servir como entregables para el cumplimiento del EGSI V2.0; de lo comentado se puede concluir que un SIEM es una estrategia válida para mitigar ataques a los datos críticos y ayudan a fortificar al EGSI V2.0.

El estudio ayudó a identificar las principales vulnerabilidades presentes en las bases de datos SQL Server 2016 Standard, como estas podrían ser explotadas de no ser mitigadas a tiempo, pudiendo comprometer la información almacenada en ellas.

El SIEM estudiado detectó de manera oportuna los incidentes de seguridad que se presentaron sobre las bases de datos SQL Server Standard. Esto se dio gracias a los módulos que la herramienta maneja, algunos de ellos son: correlacionador de eventos que permite definir los patrones de ataque y cómo responder ante ellos, permite diseñar alertas que notifiquen a los operadores de infraestructura sobre ataques recibidos, contiene gran cantidad de reportes sobre los incidentes de seguridad presentados, reportes sobre correlación de eventos predefinidos, entre otros.

Se identificó y analizó qué controles del EGSI V2.0 se relacionan con un SIEM y cómo ayudaría a mejorar la seguridad de las bases de datos SQL Server 2016 Standard; se describieron los problemas que se presentan en una entidad pública en la actualidad sin utilizar el correlacionador de eventos y se muestra el fortalecimiento de los hitos después del estudio.

Del análisis realizado se desprende que la implementación de un SIEM para la detección y mitigación de ataques a las bases de datos es un aporte sustancial para mejorar la seguridad de toda la infraestructura, y es un soporte importante para el cumplimiento de la normativa vigente en el Ecuador.

Referencias

Abad, W. (2020). Ciberataques: desafíos en el ciberespacio. *Revista de la Academia del Guerra del Ejército Ecuatoriano*, *13*(1), 13. https://doi.org/10.24133/age.n13.2020.11

Asamblea Nacional. (26 de mayo del 2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial. Quinto Suplemento 459. https://bit.ly/3AqdT2M

Bartolomé, M., y Monteiro Lima, A. (2021). El ciberespacio, durante y después de la pandemia covid-19. *Revista Academia de Guerra del Ejército Ecuatoriano*, *14*(1), 67-76. https://dx.doi.org/10.24133/age.n14.2021.06

Cano, J. (2020). Ciberataques. *Revista Sistemas*, (157), 67-74. https://doi.org/10.29236/sistemas.n157a6

Cómbita, J. (2018). *Importancia de la gestión centralizada de registros en un correlacionador de eventos (SIEM) en una organización*. Universidad Piloto de Colombia http://repository.unipiloto.edu.co/handle/20.500.12277/4676

Corte Constitucional del Ecuador. (2020). *Acuerdo Ministerial 025-2019*. https://bit.ly/3QIeWAA

González-Granadillo, G., González-Zarzosa, S. & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors (Basel, Switzerland)*, *21*(14). https://doi.org/10.3390/s21144759

Hashim, H. (2018). Challenges and Security Vulnerabilities to Impact on Database Systems. *Al-Mustansiriyah Journal of Science*, *29*(2), 117-125. https://doi.org/10.23851/mjs.v29i2.332

Jacobs, J., Romanosky, S., Adjerid, I. & Baker, W. (2020). Improving vulnerability remediation through better exploit prediction. *Journal of Cybersecurity*, *6*(1), tyaa015. https://doi.org/10.1093/cybsec/tyaa015

Martínez, D., y Tejada, L. (2019). *Manual de bases de datos*. Universidad Abierta para Adultos (UAPA).

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2021). *Acuerdo Ministerial 006-2021.* https://bit.ly/3JWprho

Pazmiño, C., y Pazmiño, J. (2018). *Implementación de un Correlacionador de Eventos basado en software libre para la detección de ataques informáticos en la Empresa Eléctrica. Tesis de titulación de la Escuela Superior Politécnica de Chimborazo*. [Tesis de Grado, Escuela Superior Politécnica De Chimborazo] http://dspace.espoch.edu.ec/handle/123456789/8445
Vielberth, M., & Pernul, G. (2018). *A Security Information and Event Management Pattern.* Universität Regensburg http://doi.org/10.5283/epub.41139