UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS “ESPOG”

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: **RPC-SO-02-No.053-2021**

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del artículo
ESTUDIO DE UN SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) PARA BASE DE DATOS SQL SERVER CASO DE ESTUDIO: MINISTERIO DE RELACIONES EXTERIORES Y MOVILIDAD HUMANA
Línea de Investigación:
SEGURIDAD INFORMÁTICA
Campo amplio de conocimiento:
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
Autor:
Franklin Edwin Vela Vela
Tutor:
MSc. Pablo Marcel Recalde Varela

Quito – Ecuador

2022

APROBACIÓN DEL TUTOR

Yo, MSc. Pablo Marcel Recalde Varela con C.I: 171168505-5 en mi calidad de Tutor del proyecto de investigación titulado: Estudio de un Security Information and Event Management (SIEM) para base de datos SQL Server caso de estudio: Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH).

Elaborado por: Franklin Edwin Vela Vela, de C.I: 171388102-5, estudiante de la Maestría: Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL**, como parte de los requisitos sustanciales con fines de obtener el Título de Magíster, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2022

_____

Firma

ORCID: 0000-0001-7256-2836

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Franklin Edwin Vela Vela con C.I: 171388102-5, autor del proyecto de titulación denominado: Estudio de un Security Information and Event Management (SIEM) para base de datos SQL Server caso de estudio: Ministerio de Relaciones Exteriores Y Movilidad Humana. Previo a la obtención del título de Magíster en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2022

Firmado electrónicamente por:
FRANKLIN EDWIN VELA

Firma

ORCID: 0000-0002-0858-3680

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

La evolución que ha tenido la tecnología desde hace algunos años ha sido vertiginosa desde sus inicios con los mainframes hasta llegar a los Datacenter actuales, con equipos de comunicación básicos hasta los Firewall de nueva generación; de la misma manera que la tecnología ha evolucionado, los ataques informáticos también lo han hecho, es por este motivo que tener protegida la información de las organizaciones es fundamental; identificando amenazas se podrán aplicar correctivos a tiempo y evitar pérdidas hacia las entidades. Los ciberdelincuentes han crecido en conocimientos y herramientas tecnológicas, esto ha llevado a que se vuelvan más peligrosos, es primordial detectar ataques de manera oportuna lo cual podría convertirse en un desafío González et al., (2021).

Los datos considerados como críticos deben ser protegidos, se deben monitorear de manera constante para evitar accesos no autorizados, cambios no permitidos, indisponibilidad de servicios entre otros.

Según Naik, (2014), en la mayoría de los casos los datos críticos están almacenados en una base de datos que se puede definir como un área de almacenamiento donde pueden guardarse todos los datos relacionados, además de procesarlos. (pág. 5). Esto conlleva a que toda esa información sea custodiada y monitoreada para no ser afectada.

En la actualidad las organizaciones sean públicas o privadas tienen que proteger a sus bases de datos que manejan información crítica de ataques informáticos, existen datos que pueden ser publicados y otros que no, salvo que el dueño de esa información lo permita como se manifiesta en el Ecuador con la Ley Orgánica de Protección de Datos Personales tiene como «objeto y finalidad 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» (Ley Orgánica de Protección de Datos Personales.- RO Suplemento 459, del 26 de mayo del 2021, s. f.). Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela.

En el Ecuador en los últimos meses se han presentado ciberataques a gran escala en entidades públicas como privadas, un ejemplo se dio en el mes de junio del 2021, donde la operadora nacional de telecomunicaciones (CNT) sufrió un ataque informático con Malware del tipo Ransomware, este ataque afectó a los sistemas financieros, activaciones y recargas a celulares, la penetración del Malware causó intermitencias en el servicio Basantes, (2021).

Otro ataque informático se dio a un banco privado, este fue un Ransomware que colocó fuera de línea algunos servicios hacia el cliente Días, (2021).

Los ataques informáticos hacia bases de datos se han intensificado desde el inicio de la pandemia, existió un alto porcentaje de personas que fueron obligados a realizar teletrabajo, esto abrió una brecha de seguridad; básicamente porque no se conoce desde dónde ni cómo se accede a la red de datos de las organizaciones. En muchos casos los empleados se conectan remotamente a sus oficinas por medio de servicios de escritorio remoto desde equipos como: computadores, celulares, tablets, etc., esto generó una brecha de seguridad que ocasionó una ola de ciberataques, los delincuentes informáticos aprovechan las vulnerabilidades de equipos personales o de las empresas (sin antivirus, falta de actualizaciones, claves de acceso sencillas, etc.) que no eran supervisados por personal especializado, acompañado de políticas inexistentes, la angustia de buscar respuestas a los problemas generados por la propagación rápida y mortal del virus Bartolomé & Monteiro, (2021).

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 Security Information and Event Management (SIEM) que ayude a visualizar los ataques que se estén presentando en las bases de datos de una manera amigable.

En la actualidad los ataques informáticos han evolucionado, esto ha llevado a que la infraestructura tecnológica haya sido víctima de ciberataques, especialmente las bases de datos que contienen la información de las empresas estatales o privadas. Para afrontar tal amenaza, las instituciones que brindan servicios críticos se están enfocando de manera recurrente en la defensa de sus instalaciones de red. Un SIEM ayuda a la protección de la red mediante la realización de correlación centralizada de informes de activos de red Arango, (2016); esto ayuda a tener agrupada toda la información que se recoge de los logs en los dispositivos desplegados en la red, un SIEM ayuda a filtrar, administrar y de ser el caso tomar medidas preventivas y correctivas ante ataques informáticos.

Problema de investigación

El MREMH es una entidad pública en el Ecuador, maneja información sensible de migrantes e inmigrantes ecuatorianos y extranjeros en el país y el exterior.

Al ser un ministerio público está sujeta a la normativa legal la cual es de cumplimiento obligatorio, dentro de este ámbito se debe implementar controles que permitan la protección,

confidencialidad e integridad de la información como lo dispone el Esquema Gubernamental de Seguridad de la Información V2.0.

La Cancillería del Ecuador maneja varios sistemas para la gestión de información crítica, existen algunos motores de base de datos, siendo el más importante el motor SQL Server que aloja la data del sistema principal, este aplicativo no maneja un registro de auditoría, tampoco se tiene una herramienta que permita visualizar ataques ni informe sobre los mismos.

Con este antecedente, se puede plantear la pregunta:

¿Un Security Information and Event Management (SIEM), es una estrategia significativa para minimizar los efectos generados por ataques a las bases de datos SQL Server, además de ayudar al cumplimiento del EGSI V2 en el Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH)?

Objetivo general

Determinar si un SIEM se constituye en una estrategia significativa para minimizar los efectos generados por ataques a las bases de datos SQL Server en el MREMH mediante el estudio de una herramienta de correlación de eventos que ayude a fortificar el EGSI V2.0.

Objetivos específicos

Establecer las debilidades que provocan daños a las bases de datos de los diferentes sistemas informáticos.

Revisar qué aspectos del SIEM, facilitan la minimización de los efectos generados por ataques a partir de las debilidades detectadas a los datos críticos.

Comparar el Esquema Gubernamental de Seguridad de la Información Versión 2.0 antes del estudio y después del estudio de un SIEM.

Identificar qué componentes del SIEM ayudan a evitar ataques a la información del Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH).

Vinculación con la sociedad y beneficiarios directos:

El presente artículo está dirigido al personal de seguridad informática y administradores de base de datos de entidades públicas y privadas, quienes son responsables de dictar las políticas que rigen la protección de los datos, además de implementar las medidas que se crea pertinente para resguardar la información, también servirá como marco de referencia para una posible implementación de un SIEM en el Ministerio de Relaciones Exteriores y Movilidad Humana.

Dentro de los Objetivos de Desarrollo Sostenible de las Naciones Unidas el objetivo nueve indica que «Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación» ODS de las Naciones Unidas, (2017), con el presente estudio se pretende aportar de forma novedosa a la seguridad de la información, monitoreo y auditoría en las bases de datos SQL Server a través de un SIEM, lo que permitirá tener respuestas inmediatas ante ciberataques.

El estudio de un SIEM para el MREMH puede ayudar a cumplir con la normativa vigente en el Ecuador sobre protección y auditoría de datos en las entidades públicas, a continuación, se muestra en qué aspectos un SIEM se relaciona el EGSI V2.0; además, la Ley Orgánica de Protección de Datos Personales dicta que: los funcionarios que sean los encargados de manejar los datos de los ciudadanos deben ejecutar las acciones que sean necesarias para resguardar los datos personales ante cualquier amenaza que pueda vulnerar la seguridad de dicha información (Ley Orgánica de Protección de Datos Personales.- RO Suplemento 459, del 26 de mayo del 2021, s. f.).

El EGSI V2.0 menciona algunos controles relacionados con esta investigación como son:

Tabla 1
Controles relacionados con un SIEM

Control	***Descripción***
5.1.1	Política de control de acceso.
8.2.1	Controles contra Malware.
8.4.1	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

Nota. Tomado del Esquema Gubernamental de Seguridad de la Información versión 2

Como se describe en la Tabla 1 existen controles que se relacionan con la auditoría, registro, respuesta, etc., de eventos de seguridad en los que un SIEM podría ayudar; además, se debe llevar un control de los incidentes que se generen en las bases de datos, estos sucesos deben ser almacenados, para de ser requeridos en una auditoría forense estar disponible o cumplir con los dispuesto por la Contraloría General del Estado en lo referente al tiempo que se debe tener disponible la información y los cambios realizada en ella que son de siete años (Ley Orgánica de la Contraloría General del Estado.- RO Suplemento 595, del 12 de junio del 2002; reformas RO No.31 del 07 de julio del 2017, s. f., p. 12 Art. 71) .

El estudio de un Sistema de Gestión de Eventos e Información de Seguridad para la protección de las bases de datos ayudará a cumplir la normativa impuesta para el sector público, se podrá realizar un registro de las intromisiones que se puedan llevar a cabo en las bases de datos, estas van a hacer almacenadas y podrán ser analizados en busca de ataques y vulnerabilidades que se puedan presentar en los sistemas de la organización.

CAPÍTULO I: DESCRIPCIÓN DEL ARTÍCULO PROFESIONAL

1.1. Contextualización general del estado del arte

El auge de nuevas tecnologías ha provocado que la información se distribuye casi de manera inmediata al mundo con el uso de la Internet Abad, (2020); también se ha presentado un aumento de ataques a organizaciones, las nuevas técnicas usadas por los piratas cibernéticos han mejorado notablemente, esto conlleva a que el personal de seguridad informática fortalezca sus esfuerzos en mejorar las barreras de protección.

En el ámbito privado y público es crucial la protección de la información ya que es el activo más importante, para el acceso a los datos generalmente se usan sistemas de información, al momento de ingresar a estos se debe comprobar la identidad del usuario, validar los perfiles y permitir el ingreso según sea el caso Švarc & Strnad, (2021).

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 sin número 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).

Pulido et al., (2019) dicen que, una base de datos es una compilación de información organizada, de tal manera que se pueda acceder a ella de una manera ágil, ordenada, segura y confiable. (pág. 18). Las bases de datos deben ser independientes, es decir, no depende de ningún aplicativo; debe evitar la duplicidad de los datos, esto ayuda a optimizar el espacio y a gestionar la información de mejor manera, además se debe asegurar que la información está segura.

Existen varios mecanismos de defensa para proteger la información de las organizaciones entre ellos se tiene, Firewall de nueva generación que puede definirse como una técnica de seguridad enfocada a redes que puede ser hardware o software y pertenece a la tercera generación de tecnología de firewall Fernandez, (2019), estos no solamente bloquean puertos, además, inspeccionan aplicaciones; User and Entity Behavior Analytics (UEBA), se puede definir como el análisis del comportamiento de las personas que están conectadas una red de la organización Ramírez, (2020), un Security Information and Event Management podría definirse como sistema de seguridad que ayuda a identificar y de ser el caso responder a incidentes que podrían producirse dentro de una infraestructura, Network Access Control (NAC) es una técnica de ciberseguridad que evita que usuarios y dispositivos no autorizados ingresen a redes privadas y accedan a recursos confidenciales Vance, (2022),

Intrusion Prevention System (IPS) es una plataforma de software que analiza el contenido del tráfico de la red para detectar y responder a las vulnerabilidades Keary, (2019), Intrusion Detection System (IDS) es un sistema usado para identificar accesos no autorizados a un computador o a una red.

Vielberth & Pernul, (2018) describieron que, los sistemas SIEM permiten la automatización de la detección de incidentes y las reacciones posteriores para mitigar los incidentes inminentes o para preservar pruebas forenses. (pág. 1).

SIEM une a dos tecnologías de la seguridad que son Security Event Manager (SEM) ayuda a buscar patrones no comunes de acceso y los analiza casi en tiempo real y Security Information Management (SIM) que concentra los datos arrojados por el SEM en un repositorio central para ser examinados, esto ayuda a la creación de reportes que permiten a los administradores de seguridad a tomar decisiones de cómo atacar los incidentes.

Un SIEM posee varias capas como se muestra en la Figura 1.

Figura 1
Capas de un SIEM

Nota. Autoría propia

Las capas se describen a continuación Pazmiño & Pazmiño, (2018):

- 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 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.

La tecnología evoluciona constantemente, esto también influye en los SIEM, en la mayoría de las infraestructuras los SIEM cubren las necesidades de detección de amenazas, el envío de notificaciones, pero existen arquitecturas mucho más complejas que necesitan que los SIEM realicen tareas más completas de análisis.

Los SIEM de nueva generación deben contemplar aspectos a considerar como son: seguridad diversa, Fusión de datos OSINT (Open Source INTelligence), visualización mejorada, almacenamiento mejorado, integración con orquestación, automatización y respuesta de seguridad (SOAR) González et al., (2021).

El 10 de enero del 2020 el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) expidió el Esquema Gubernamental de Seguridad de la Información Versión 2.0, 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» Esquema Gubernamental de Seguridad de la Información, (2020). Con los hitos mencionados se obliga a las instituciones públicas a implementar controles dentro de la Infraestructura para minimizar los riesgos que se puedan producir por amenazas que aprovechan vulnerabilidades presentes; además, en el anexo 1 se muestra la disposición dada por la Coordinación General de Tecnologías de la Información (CGTIC) del MREMH para la implementación de EGSI V2.0. Con la utilización de un correlacionador de eventos podría ayudar a las organizaciones públicas a cumplir con los controles indicados.

Investigaciones previas realizadas

Al realizar la investigación se han encontrado gran variedad de estudios en la metodología como son: estudios, artículos científicos, propuestas de mejora, implementación de SIEM, se han seleccionado los que más concordancia tienen con el artículo propuesto; a continuación, se listan estos trabajos:

En el artículo realizado por Cómbita, (2018) titulado «IMPORTANCIA DE LA GESTIÓN CENTRALIZADA DE REGISTROS EN UN CORRELACIONADOR DE EVENTOS (SIEM) EN UNA ORGANIZACIÓN» indica que:

- La infraestructura en las organizaciones genera logs y no se puede realizar un análisis de los registros por separado, es necesario relacionarlos y deben ser almacenados en un solo repositorio.
- Existen herramientas SIEMs de pago y otras de código libre, la elección dependerá de las necesidades y presupuestos de las instituciones.

- Si se llegará a presentar algún problema en el cual sea necesario un estudio forense, un SIEM ayuda a este proceso ya que guarda los registros de incidentes de seguridad presentados.

En la investigación realizada por Vielberth & Pernul, (2018) titulado «A security Information and Event Management Pattern» explica que:

- Un sistema SIEM permite detectar y responder de manera automática a ataques a las vulnerabilidades de las organizaciones.
- Implementar un sistema SIEM permite recopilar y normalizar logs importantes de los diferentes componentes tecnológicos, almacena y centraliza información relevante.
- La mayoría de SIEMs permiten distribuir sus componentes en ambientes diferentes, por ejemplo, un SIEM de base de datos podría tener su almacenamiento en la nube y la demás arquitectura en un Data Center local.

En el artículo académico realizado por González et al., (2021) llamado «SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM): ANALYSIS, TRENDS AND USAGE IN CRITICAL INFRASTRUCTURES» señala lo siguiente:

- Los factores políticos, económicos, sociales, tecnológicos, legales y ambientales producirán una evolución de los SIEMs a mediano y largo plazo.
- En la actualidad los SIEMs permiten una detección y en lo posible una reacción automatizada de amenazas, pero en muchos casos para infraestructuras críticas se requiere la intervención de los operadores para realizar acciones correctivas.
- A futuro algunas de las mejoras que podrán darse en los SIEMs son las siguientes: los SIEMs cubrirán más ámbitos de la seguridad, fusión de datos OSINT traducido como inteligencia de fuentes abiertas (Open Source Intelligence), mejor visualización de resultados, optimización del almacenamiento, Integración con Security Orchestration Automation and Response (SOAR), administración de una enorme cantidad de datos a través de indexación; implementación de inteligencia artificial (AI) que dará capacidades predictivas al SIEM, útiles para el análisis de anomalías, comportamiento del tráfico de red, herramientas y usuarios.
- El futuro de los SIEMs debe tener en consideración la evolución y sofisticación de los ataques informáticos, el aumento en el uso de dispositivos móviles, más personas utilizando redes sociales y cambios en la regulación.

En el trabajo de Investigación elaborado por Bonilla, (2017) titulado «ELABORACIÓN DE UNA METODOLOGÍA DE DETECCIÓN Y MITIGACIÓN DE VULNERABILIDADES DE

BASE DE DATOS Y SU INCIDENCIA EN LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA AUTOMEKANO CÍA. LTDA., DE LA CIUDAD DE AMBATO» explica que:

- Los ataques hacia las bases de datos son de dos tipos, los que no requieren autenticación por ejemplo la explotación de Buffer Overflow y los que requieren autenticación, para este se requiere credenciales válidas para acceder a los motores de base de datos.
- Existen amenazas de seguridad para base de datos, entre ellas se tiene: abuso de exceso de privilegios, abuso legítimo de privilegios, elevación de privilegios, SQL Injection, software de base de datos sin parches, características en los motores de bases de datos que no son necesarias, registros de auditoría débiles, entre otras.
- Las vulnerabilidades presentes en las bases de datos deben contar con estrategias de detección y prevención coherentes.

En el estudio de Hashim, (2018) que lleva el nombre de «Challenges and Security Vulnerabilities to Impact on Database Systems» muestra que:

- La protección de las bases de datos se centra en los siguientes puntos, confidencialidad de la información, integridad de los datos que reposan en los repositorios de datos, accesibilidad a la data que debe estar disponible para consultarla.
- Indica que las amenazas para una base de datos son, abuso de privilegios, abuso de privilegios legítimos, elevación de privilegios, vulnerabilidades en los motores de base de datos, inyección de SQL, auditoría no robusta, denegación de servicios, vulnerabilidades en protocolos de comunicación a las bases de datos, autenticación débil, exposición de los respaldos de base de datos.

De los artículos analizados se puede desprender que, los SIEMs son herramientas de suma importancia para prevenir ataques hacia los diferentes componentes de una infraestructura de red, ayudan a recolectar, procesar y almacenar incidentes de seguridad.

Las bases de datos constituyen el activo más importante para las organizaciones, en ellas se guarda, procesa y distribuye información que hace funcionar las entidades, estás presentan vulnerabilidades que de no ser identificadas podrían ocasionar serios problemas a los datos de las organizaciones.

Un SIEM permite guardar los eventos que se dan en las bases de datos, si se llegará a presentar algún problema en el cual sea necesario un estudio forense, la herramienta ayuda a este proceso ya que guarda los registros de incidentes de seguridad presentados.

1.2. Proceso investigativo metodológico

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 puede ayudar a su cumplimiento, también se analizó el comportamiento de un SIEM para conocer su capacidad de detección ante ataques que se pueden dar en un motor de base de datos.

Se plantea analizar como un SIEM para las bases de datos del MREMH 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 SIEM es un aporte valedero a la protección de una base de datos SQL Server 2016 y ayuda a la implementación del EGSI V2.0 en el MREMH.

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

Primero se definió los tipos de ataques que se pueden presentar en las bases de datos, los encontrados fueron:

Amenazas internas: se centran en ataques que se generan dentro de las organizaciones ya sea por personal que desea hacer daño (personas descontentas por su sueldo), una persona ajena a la organización que de alguna manera obtuvo claves de acceso a las bases de datos, tal vez por ingeniería social que utiliza diferentes métodos y técnicas para lograr infiltrarse a las instituciones mediante los empleados Prado, (2021), este tipo de amenaza es muy frecuente en las entidades y se produce por no manejar un control adecuado los perfiles de acceso.

Vulnerabilidades de software de bases de datos: se refiere a cualquier aplicativo que tenga acceso a las bases de datos, generalmente los proveedores que venden el software para administrar los gestores de bases de datos entregan de manera periódica parches o actualizaciones a su software, el cual cierra brechas de seguridad o minimiza el impacto de un ataque que aproveche una vulnerabilidad.

Ataques de inyección SQL: el ataque hacia las bases de datos más común es inyección SQL, es una clase de ataque informático que explota fallas existentes en sistemas web. Los delincuentes informáticos invaden las bases de datos de SQL (Structure Query Language) introduciendo software dañino por medio de código, puede incluir funciones con elementos de entrada Bonilla, (2017), con este tipo de ataque los intrusos pueden obtener los datos críticos de las organizaciones, pudiendo sufrir pérdidas económicas y lo peor, pérdida de reputación.

Pistas de auditoría débiles: la auditoría en la base de datos es muy importante, permite conocer qué acciones se realizan sobre ella, transacciones, actualización de información, entre otras, la auditoría permite realizar un análisis forense, la ausencia de pistas fuertes permitirá realizar acciones que no queden registradas.

Ataques de denegación de servicio: también llamado como DoS por sus siglas en inglés Denial of Service, en este el hacker satura el servidor de la base de datos con demasiadas peticiones, hasta el punto de que el equipo no logra atender los pedidos legítimos de usuarios válidos, y la base de datos deniega el acceso a la información.

Malware: los ciberdelincuentes utilizan técnicas avanzadas para explotar vulnerabilidades presentes en las bases de datos, pueden aprovechar huecos de seguridad utilizando diferentes técnicas, como son spear phsing y malware para ingresar a información en las organizaciones y extraer datos.

Privilegios excesivos: se produce cuando a los usuarios se les da acceso más allá de sus funciones, lo que podría ser usado para obtener información sensible de la cual no se debe conocer, por ejemplo, si a un agente consular del MREMH se le da acceso de lectura a una base de datos de trámites podría usar ese perfil para realizar trámites no autorizados.

Abuso de privilegios: los usuarios pueden abusar de los privilegios asignados a ellos para realizar tareas no permitidas, por ejemplo, un agente consular del MREMH tiene permisos para consultar datos personales de ecuatorianos que residen en el exterior, podría exportar la información a un archivo y utilizarlo para fines no autorizados.

Elevación de privilegios: las vulnerabilidades en las bases de datos podrían ocasionar que un usuario con permisos de lectura pueda tener permisos de escritura, por ejemplo, si un

atacante produce un desbordamiento de búfer podría elevar los permisos normales a los de administrador.

Luego se definió el software SIEM que se usará para el estudio, siendo este EventLog Analyzer de ManageEngine, el cual fue implementado en el caso de estudio desde hace poco tiempo y no ha sido aún configurado para analizar su comportamiento.

Las ventajas que se tienen con este SIEM según (*Auditoría de bases de datos | Software de auditoría de bases de datos - ManageEngine EventLog Analyzer*, s. f.) son:

- Gestión integral: compila información del manejo de cuentas de usuario de la base de datos, informa en tiempo real sobre eventos de seguridad, además de guardar la información.
- Monitoreo de la actividad de la base de datos: verifica la actividad de los usuarios dentro del motor de base de datos.
- Monitoreo del log del servidor de base de datos: valida los inicios de sesión a la base de datos.
- Monitoreo de la seguridad de la base de datos: análisis de la base de datos para detectar los posibles ataques a la misma.
- Análisis exhaustivo: realiza un análisis exhaustivo de los logs del servidor de base de datos para entender de mejor manera el comportamiento del equipo.

Al ser un entorno de producción y al encontrarse en una etapa de estudio, se realizó la configuración de un servidor de pruebas, contenía la copia de una base de datos para realizar los test necesarios y validar el funcionamiento del SIEM.

Luego se procedió a realizar la configuración de las alarmas, cuando se presente una amenaza o ataque, llegará una alarma vía correo electrónico a los administradores de infraestructura para que tomen las medidas que sean necesarias.

Finalmente se realiza un análisis de los resultados que entregan los reportes de la herramienta y poder definir si es una alternativa viable de solución para detectar amenazas a las bases de datos del Ministerio de Relaciones Exteriores y Movilidad Humana y si es un instrumento que ayude a cumplir con los controles del EGSI V2.0.

En la Figura 2 se muestran las etapas que se darían para el estudio de un Security Information and Event Management para base de datos en el Ministerio De Relaciones Exteriores y Movilidad Humana.

Figura 2
Etapas de estudio SIEM

Nota. Autoría propia

1.3. Análisis de resultados

El Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) por medio del Acuerdo Ministerial No. 006-2021, en el Artículo 1 pública 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» Política de Ciberseguridad, (2021).

Al ser una política que rige para el sector público la Cancillería del Ecuador debe buscar los mecanismos para potenciar la ciberseguridad, esta se enfocará en la seguridad informática del motor de base de datos SQL Server.

En el anexo 2 se evidencia la instrucción al personal que es responsable de la ejecución de EGSI V2.0 en cual instruye que, se realice entrega de verificables que muestren la aplicación de los controles.

1.3.1. Situación actual de amenazas hacia las bases de datos

Una vez identificadas las amenazas para las bases de datos en el MREMH, se ha elaborado una comparativa en la cual se establece la situación actual de las vulnerabilidades sin la utilización de un SIEM.

Tabla 2
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

Vulnerabilidad de base de datos	***Situación actual***	***Impacto***
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 qué 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

Nota. Autoría propia

Como se observa en la Tabla 2, las vulnerabilidades en las bases de datos de SQL Server en el MREMH se encuentran en un grado medio - alto de criticidad, los huecos de seguridad no han sido atendidos, no existen herramientas que permitan monitorear si existe alguna vulnerabilidad o no.

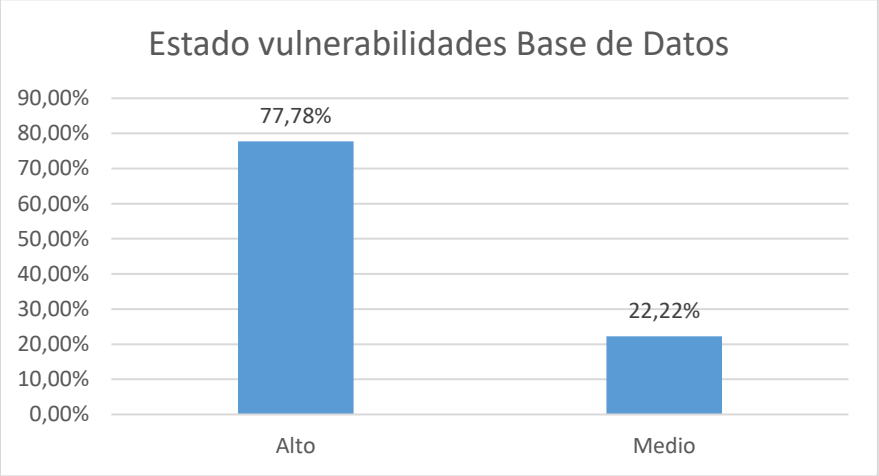
La Tabla 3 muestra el porcentaje del impacto hacia las bases de datos por las vulnerabilidades detectadas.

Tabla 3
Impacto de vulnerabilidades en las bases de datos

Impacto	No. Vulnerabilidades	Porcentaje
Alto	7	77,78%
Medio	2	22,22%
Total	**9**	**100,00%**

Nota. Autoría propia

Figura 3
Estado de vulnerabilidades Base de datos



Nota. Autoría propia

En la Figura 3 se evidencia que el 77,78 % de las amenazas tienen un estado crítico, esto significa que, si un atacante vulnera las seguridades perimetrales o incluso desde la red interna, sería fácil poder acceder a datos críticos de la organización sin que se presente algún tipo de registro de lo acontecido; 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.

1.3.2. Situación actual de controles del EGSI V2.0 en el MREMH

Según el Artículo 1 del Acuerdo Ministerial No. 025-2019 El Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), expidió el Esquema Gubernamental de Seguridad de la Información EGSI versión 2.0 que es de implementación obligatoria en el sector público que depende de la Función Ejecutiva.

El MREMH ha realizado la implementación del EGSI V2.0 en forma parcial, existen políticas, procedimientos y otros aspectos teóricos que recomienda la norma, pero no existen herramientas que ayuden a evaluar el cumplimiento de los controles.

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, los mismos son en los que es necesario el registro, almacenamiento y disponibilidad de eventos, según la Ley Orgánica de la Contraloría General del Estado es de siete años.

En la Tabla 4 se observa trece controles del EGSI V2.0 que fueron evaluados por el MREMH en los que se hace necesaria la implementación de herramientas tecnológicas que ayuden a gestionar incidentes de seguridad y manejan una base ese 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 4
Estado actual de controles del EGSI V2.0 en el MREMH

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

Dominio	Categoría	Objetivos de control	Control	Observación	Estado
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

Dominio	Categoría	Objetivos de control	Control	Observación	Estado
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

Nota. Autoría propia

En la Tabla 5 se observa el porcentaje de cumplimiento de los controles que fueron analizados para esta investigación

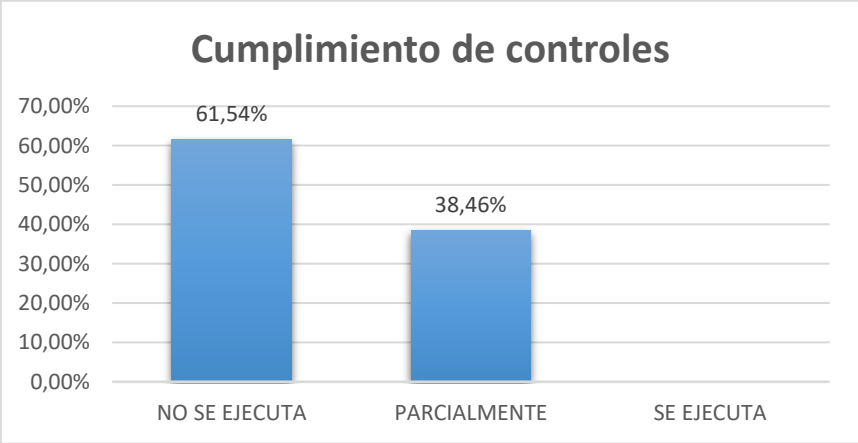
Tabla 5
Cumplimiento de controles

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

Nota. Autoría propia

En la Figura 4 se muestra que el 61,54% de los controles analizados en el MREMH no están cumpliendo los lineamientos requeridos, un 38, 46% cumplen la normativa parcialmente y ningún hito cumple al 100% lo dispuesto por el MINTEL.

Figura 4
Cumplimiento controles EGSI V 2.0



Nota. Autoría propia

Al momento el Ministerio de Relaciones Exteriores y Movilidad Humana no cuenta con un recolector de logs de base de datos que permita identificar de manera temprana ataques informáticos que se puedan presentar, se tiende a reaccionar cuando el problema se presenta y no se puede ser proactivo para identificar vulnerabilidades de manera temprana.

El personal encargado de la administración de las bases de datos es insuficiente para estar analizado todos los eventos de error que se puedan dar, esto genera que se pierda información de seguridad.

Como se muestra en la Figura 4 los controles analizados no cumplen con lo dispuesto en el EGSI V2.0, no se tiene una recolección, almacenamiento ni administración centralizada de los incidentes de seguridad que se presenten.

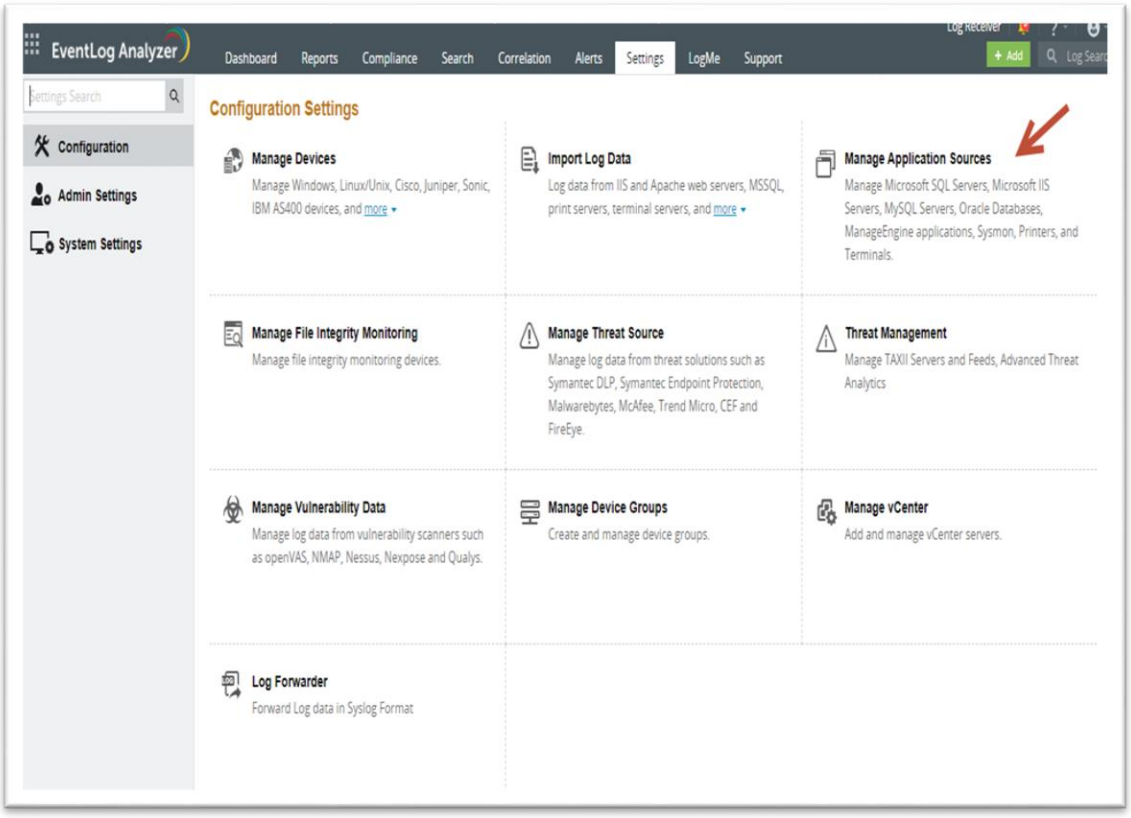
1.3.3. Estudio de un SIEM para base de datos SQL Server

Luego de la evaluación de controles del EGSI V2.0 en el MREMH se inició la puesta en marcha del SIEM EventLog Analyzer, el software se encontraba instalado, pero no configurado.

Se realizó la configuración de un servidor con el sistema operativo (S.O.) Windows Server 2016 Standard, el motor de base de datos es SQL Server 2016 Standard, además, se configuró una copia de una base de datos de producción. La arquitectura se encuentra en un ambiente controlado que no afecta a servicios ni demás equipos.

Se ingresó a la herramienta al servidor de base de datos de pruebas, como se muestra en la Figura 5.

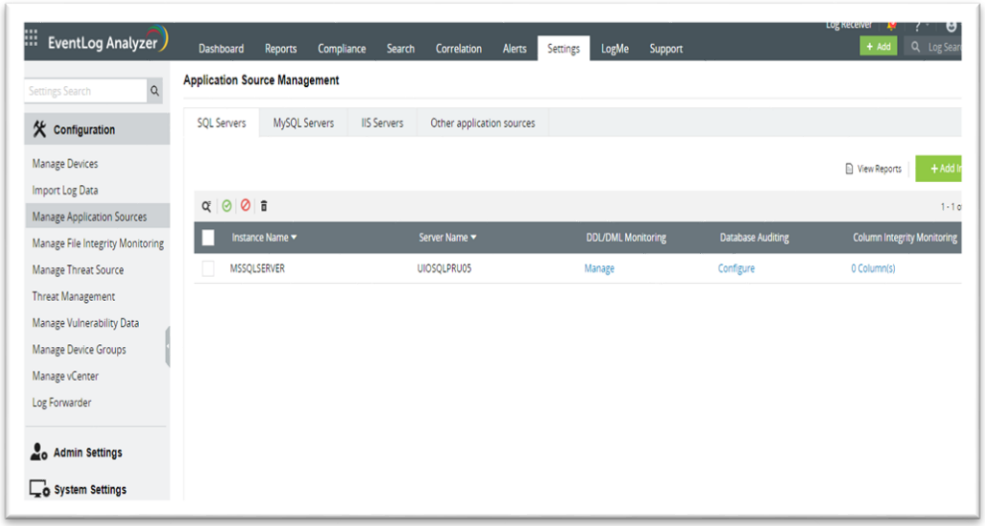
Figura 5
Dashboard para agregar servidores de base de datos



Nota. Tomado de consola de administración EventLog Analyzer

Se configuraron los datos de acceso al servidor como usuario y clave de S.O., además de datos para la conexión a la base de datos, como se muestra en la Figura 6.

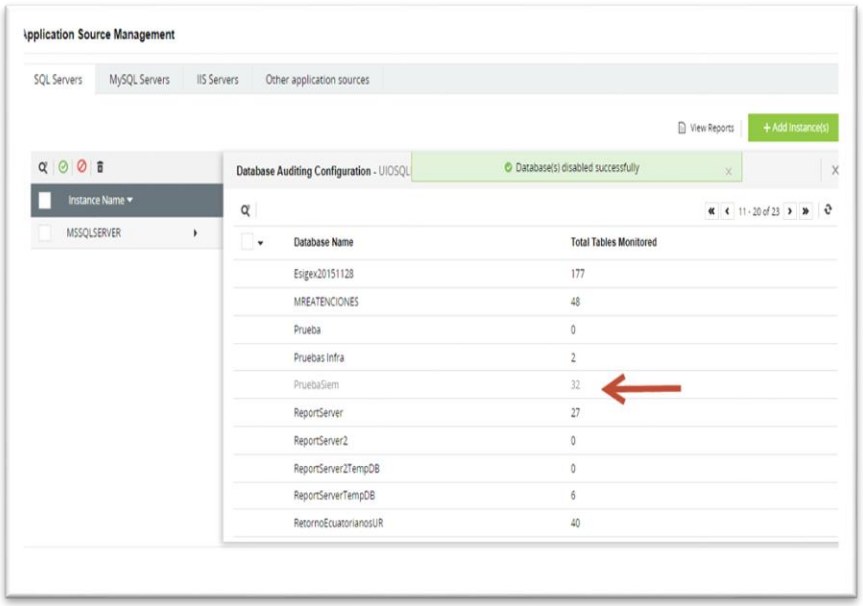
Figura 6
Configuración de servidor de base de datos



Nota. Tomado de consola de administración EventLog Analyzer

Para el análisis se selecciona la base de datos, en este caso “PruebaSiem”, como se muestra en la Figura 7.

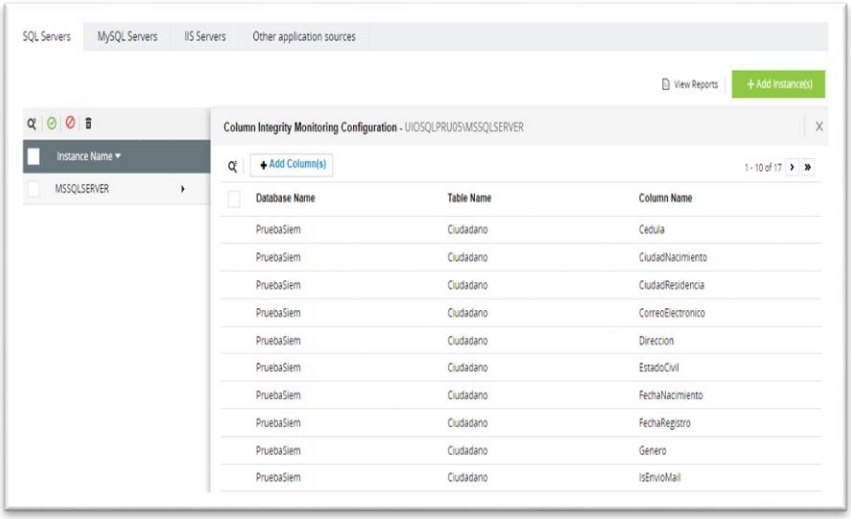
Figura 7
Base de datos de prueba



Nota. Tomado de consola de administración EventLog Analyzer

Se escogió las tablas y campos que se van a auditar, es decir, verificar que cambios se realizan sobre las mismas, como se muestra en la Figura 8.

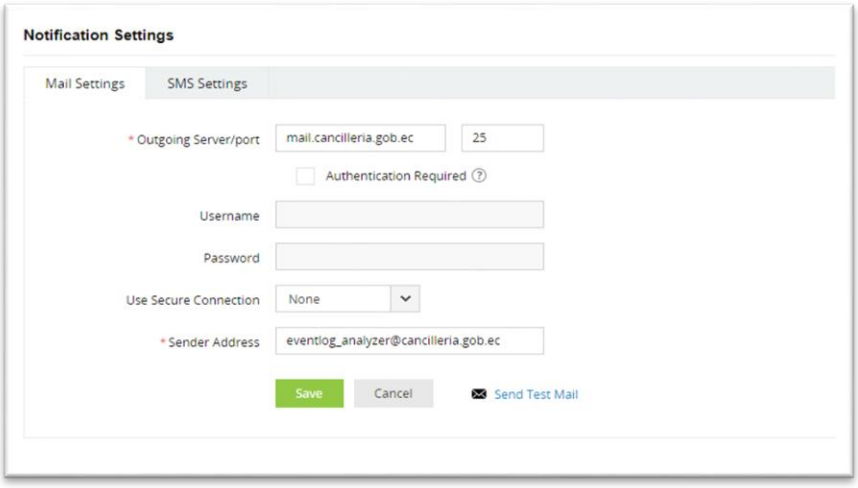
Figura 8
Tablas para auditar



Nota. Tomado de consola de administración EventLog Analyzer

Se configuro las notificaciones de los incidentes que se puedan presentar, en este caso se escogió las alertas por medio de emails, 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 9.

Figura 9
Configuración de notificaciones



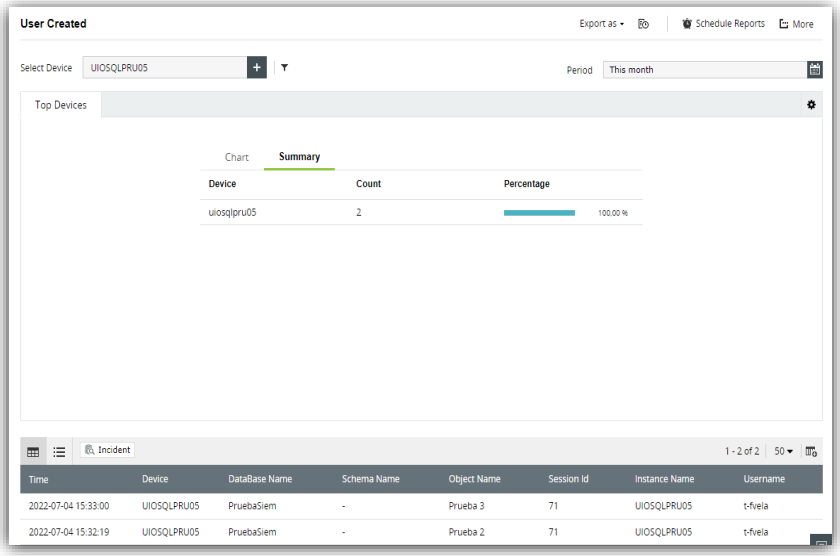
Nota. Tomado de consola de administración EventLog Analyzer

Una vez configurado el SIEM tuvo una prueba de concepto de tres meses tiempo en el cual la herramienta recopilo incidentes de seguridad, esto generó datos para realizar el análisis.

Para remediar las vulnerabilidades presentes en las bases de datos, se estudió que opciones del SIEM pueden ser usadas para solventar los huecos de seguridad, los hallazgos se describen a continuación:

Amenazas Internas: se observa que la herramienta permite visualizar algunas opciones para identificar las acciones que los usuarios realizan dentro del motor de base de datos, como la modificación de cuentas privilegiadas y cuentas normales, identificar motivos por los cuales falla el inicio de sesión, como se muestra en la Figura 10.

Figura 10
Inicios de sesión a base de datos



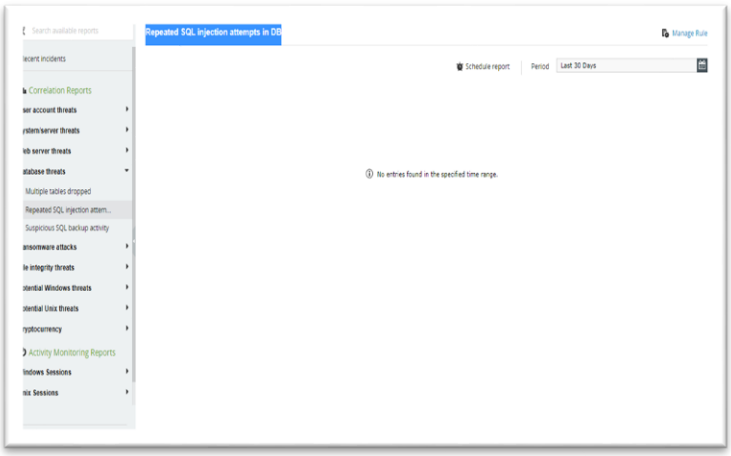
Nota. Tomado de consola de administración EventLog Analyzer

Vulnerabilidades de software: hasta el momento del estudio, la herramienta no maneja un control de actualizaciones de software de base de datos, es recomendable que la descarga e instalación de parches de seguridad sea manual y controlada, de preferencia se debe realizar en un ambiente de pruebas, validar que los servicios que están instalados no sean afectados después de la actualización.

Ataques de inyección SQL: el SIEM estudiado permite realizar un control de este tipo de ataques, su correlacionador de eventos permite personalizar paso a paso las acciones a tomar para detener el ataque, por ejemplo, podría bloquear al usuario que ha intentado vulnerar la seguridad, iniciar un proceso de apagado de la base de datos entre otras, hasta

el momento del estudio no se pudo identificar este tipo de ataque, como se muestra en la Figura 11.

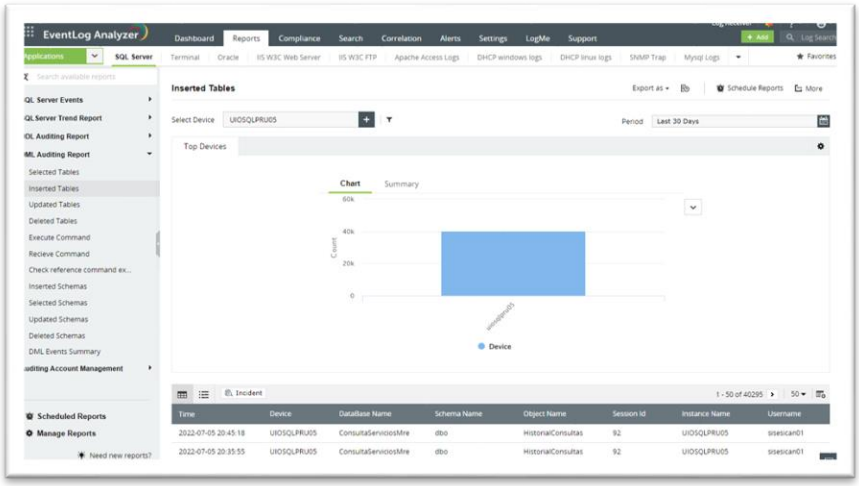
Figura 11
Ataques de Inyección de SQL



Nota. Tomado de consola de administración EventLog Analyzer

Pistas de auditoría débiles: el SIEM tiene algunas opciones para el manejo de auditoría, permite la revisión de sentencias de lenguaje de definición de datos (DDL) para administrar los objetos dentro de la base de datos (creación, eliminación, modificación de tablas, vistas, etc.); además, permite auditar los cambios usando sentencias de lenguaje de manipulación de datos (DML) que modifican los datos dentro de la base (inserción, actualización y borrado registros en las tablas), permite identificar la fecha, base de datos, esquema, usuario y objeto que fue alterado, como se muestra en la Figura 12.

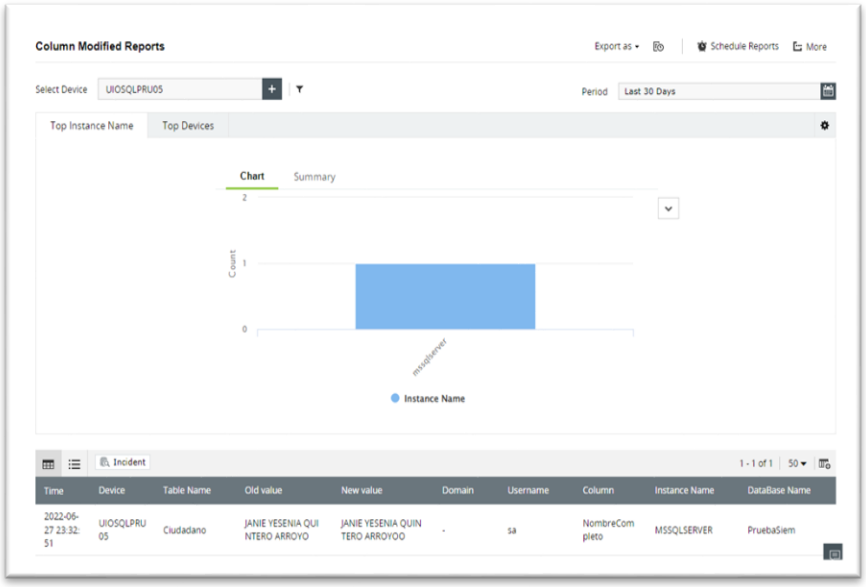
Figura 12
Inserciones a una tabla



Nota. Tomado de consola de administración EventLog Analyzer

En la Figura 13 se observa la granularidad a la que se puede llegar con la auditoría que trae la herramienta, para esto se actualizó un campo en una tabla y se evidencio los valores anteriores y actuales.

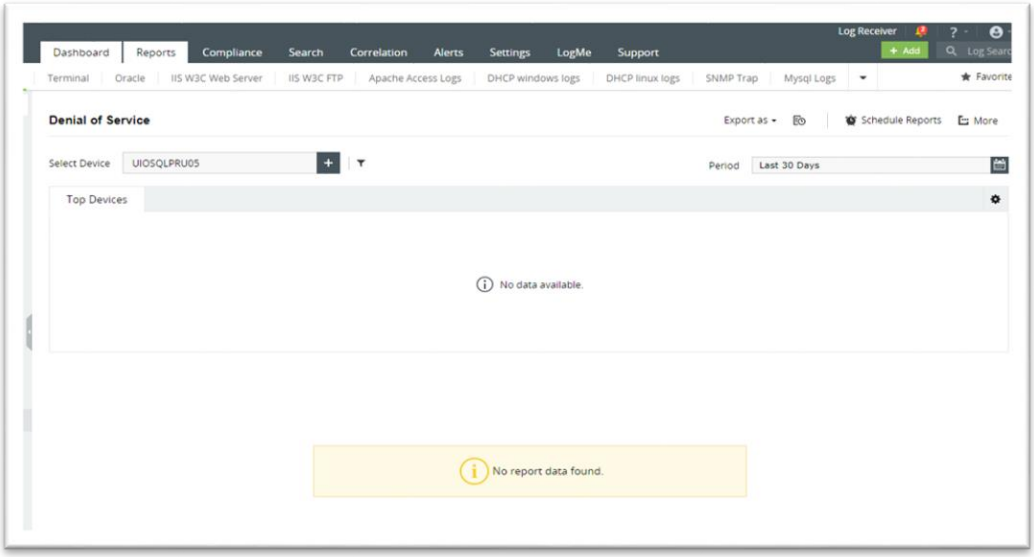
Figura 13
Actualización de un campo en una tabla



Nota. Tomado de consola de administración EventLog Analyzer

Ataques de denegación de servicio DoS: el aplicativo tiene la opción de detectar este tipo de ataques y enviar alertas a los operadores si se producen, al momento del estudio no se muestran intrusiones a la infraestructura, como se muestra en la Figura 14.

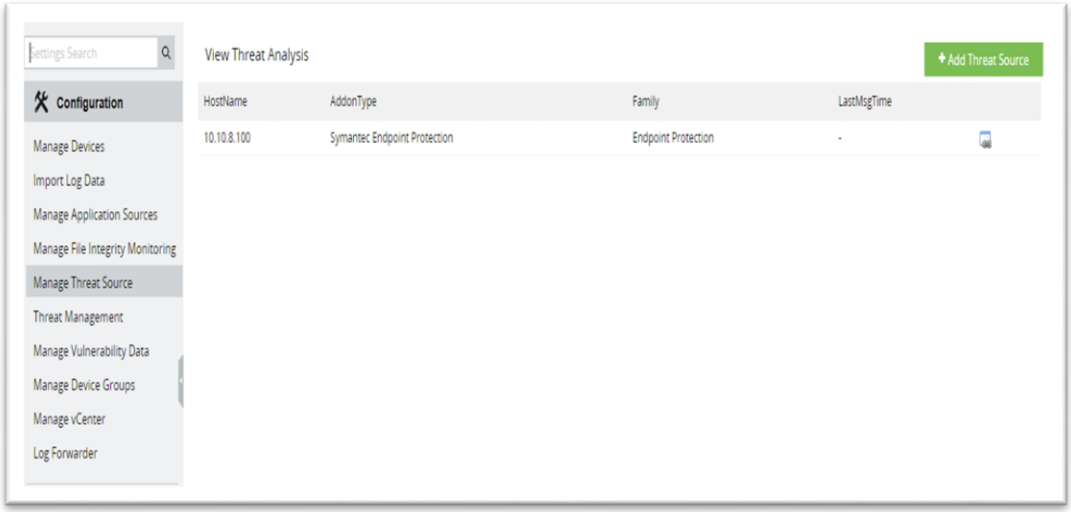
Figura 14
Detección de ataque de DOS



Nota. Tomado de consola de administración EventLog Analyzer

Malware: el correlacionador de eventos se integra con diversas fuentes, como son los antivirus Symantec, McAfee, FireEye, Malwarebytes, etc., el SIEM examina los datos de las herramientas de análisis de amenazas, estos los presenta como informes de fácil lectura, como se muestra en la Figura 15.

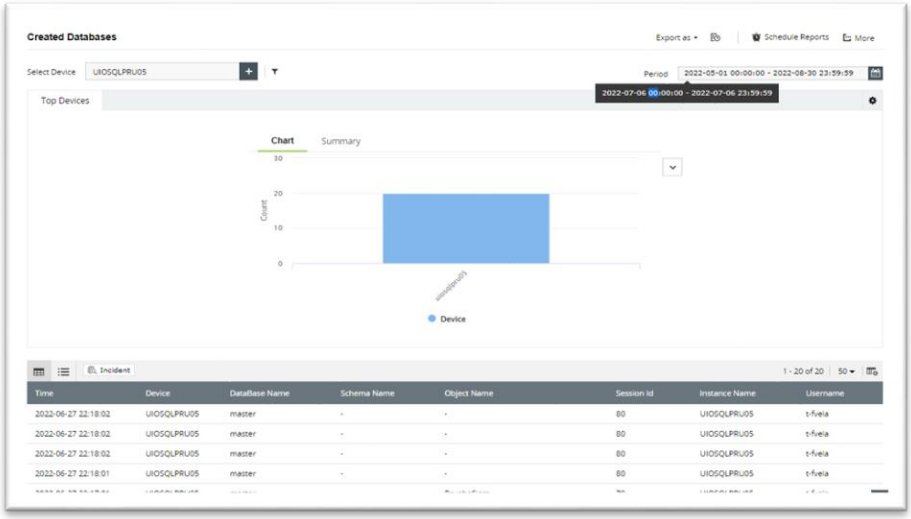
Figura 15
Integración con antivirus Symantec



Nota. Tomado de consola de administración EventLog Analyzer

Privilegios excesivos: el SIEM permite observar y almacenar información de los objetos de base de datos que fueron modificados, además permite monitorear que data es alterada, ayuda a tener un control de cambios, puede auditar si un usuario está realizando tareas que no son de su competencia para tomar las medidas correctivas necesarias, como se muestra en la Figura 16.

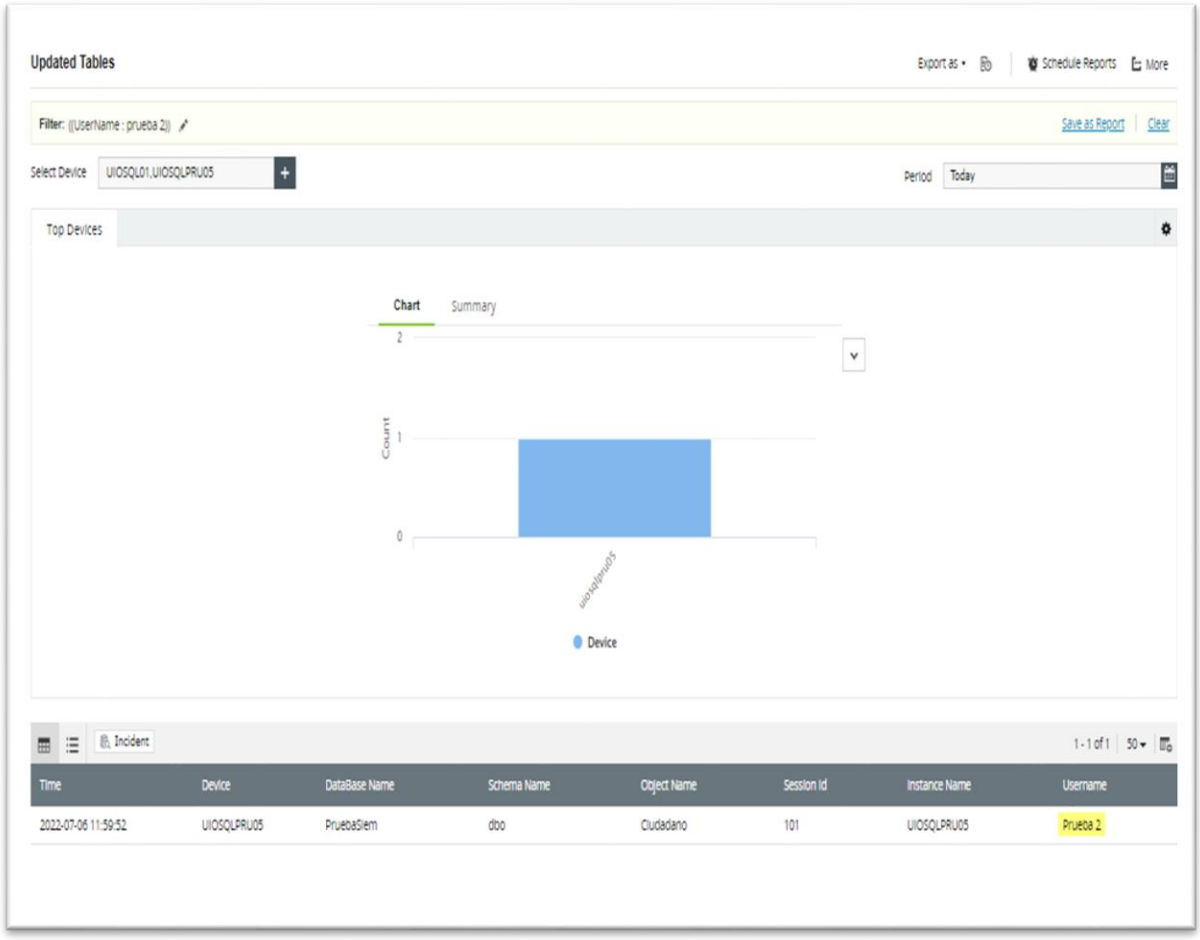
Figura 16
Creación de una base de datos por un usuario



Nota. Tomado de consola de administración EventLog Analyzer

Abuso de privilegios: un usuario con ciertos permisos, por ejemplo, de lectura de base de datos trata de hacer una actualización a una tabla a la que no lo tiene permitido, en el ejemplo el usuario Prueba 2 tiene permisos de lectura y trata de hacer una actualización a una tabla, el SIEM registra el incidente, como se muestra en la Figura 17.

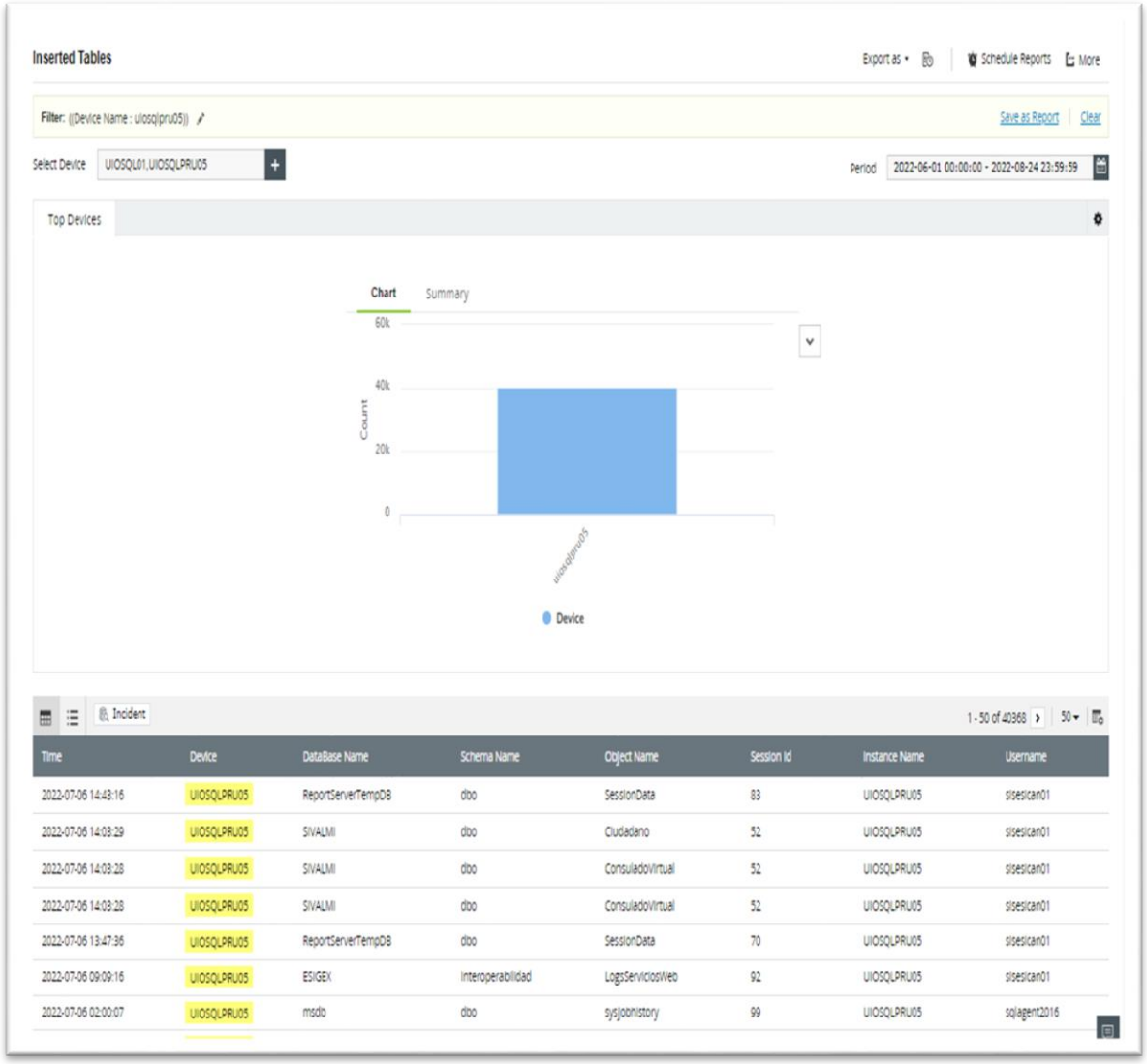
Figura 17
Registro de actualización de tabla



Nota. Tomado de consola de administración EventLog Analyzer

Elevación de privilegios: con los reportes generados por un SIEM se puede detectar qué acciones se realizan sobre la base de datos, con estos informes se puede observar si un usuario con permisos específicos trata de realizar actividades que no le competen, como se muestra en la Figura 8.

Figura 18
Inserciones a una tabla

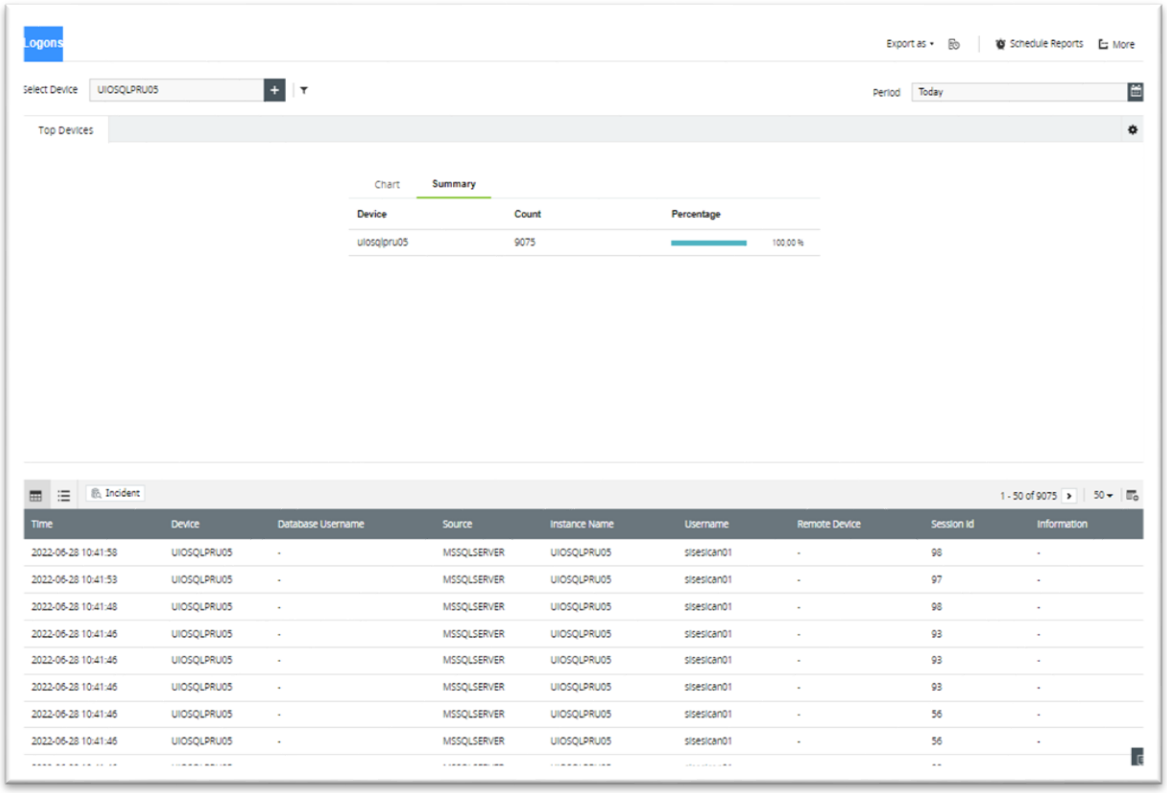


Nota. Tomado de consola de administración EventLog Analyzer

Luego del despliegue de la herramienta de SIEM EventLog Analyzer y el correspondiente monitoreo, se evaluaron los ataques que podrían darse en la base de datos y en qué medida esas vulnerabilidades fueron fortalecidas para el cumplimiento del EGSI, los resultados se presentan a continuación:

Control 5.1.1 Política de control de acceso: se pudo verificar que se realiza un monitoreo de los usuarios que hacen inicio de sesión, con la fecha y hora, como se muestra en la Figura 19.

Figura 19
Inicio de sesión de usuarios a la base de datos



Nota. Tomado de consola de administración EventLog Analyzer

Control 8.2.1 Controles contra Malware: la herramienta permite realizar una detección de dos maneras:

La primera ejecuta la integración con software antivirus que es usado como fuente de amenazas para el SIEM, en el caso del MREMH es un Symantec, estos registros son analizados para prevenir ataques de día cero, y otros tipos de virus, con esto se ayuda a mejorar la seguridad informática de las organizaciones, como se muestra en la Figura 20.

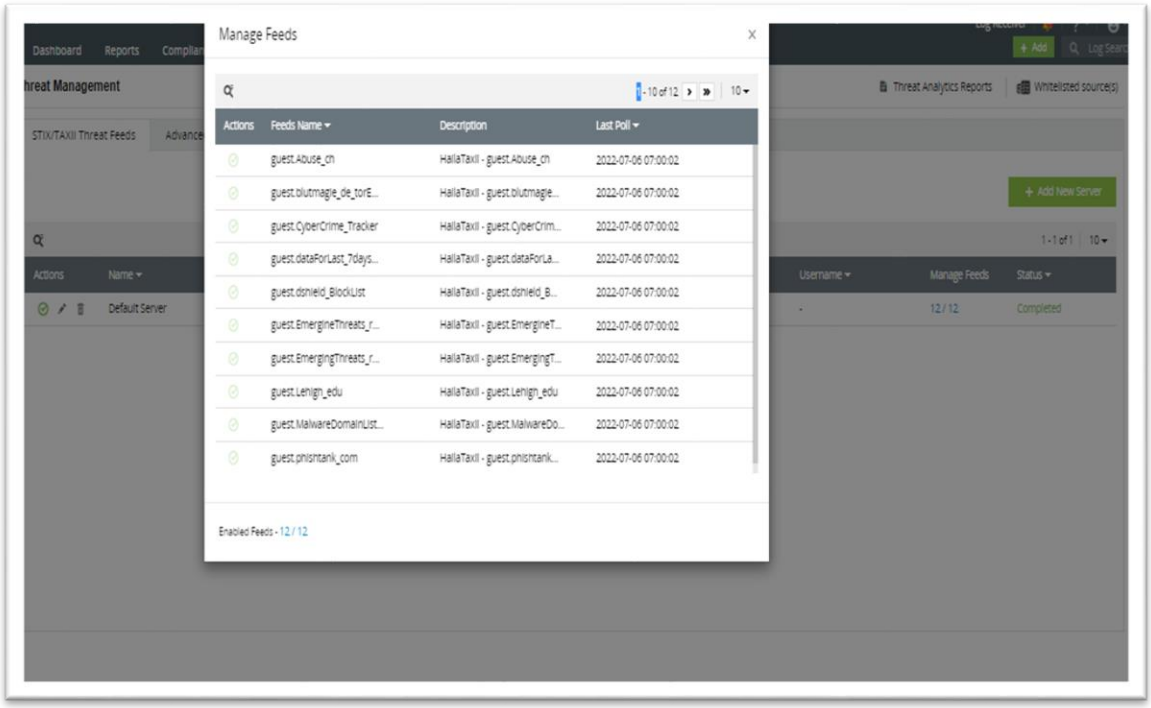
Figura 20
Configuración de servidor de antivirus

Nota. Tomado de consola de administración EventLog Analyzer

Otro método que usa el SIEM para ayudar a controlar el Malware es utilizar bases de datos de fuentes de ataques internacionales como, STIX, TAXII y AlienVault OTX, esto ayuda a tener actualizada las bases de conocimiento y detener ciberataques, como se muestra en la Figura 21.

Figura 21

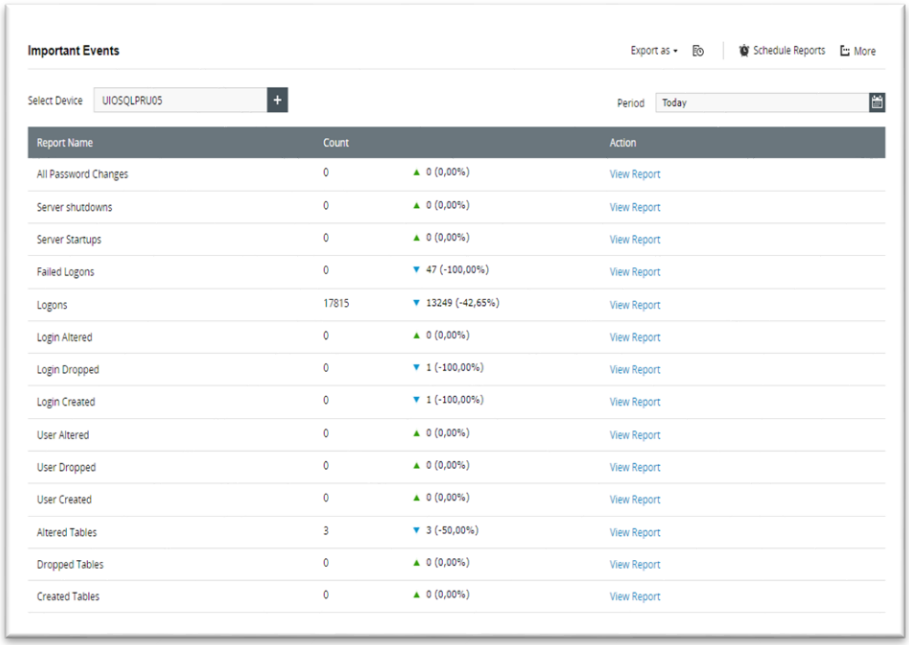
Fuentes de amenazas más destacadas



Nota. Tomado de consola de administración EventLog Analyzer

Control 8.4.1 Registro de eventos: el SIEM estudiado cumple con este hito ya que se puede visualizar cómo se almacenan todos los registros generados por las bases de datos, como se muestra en la Figura 22.

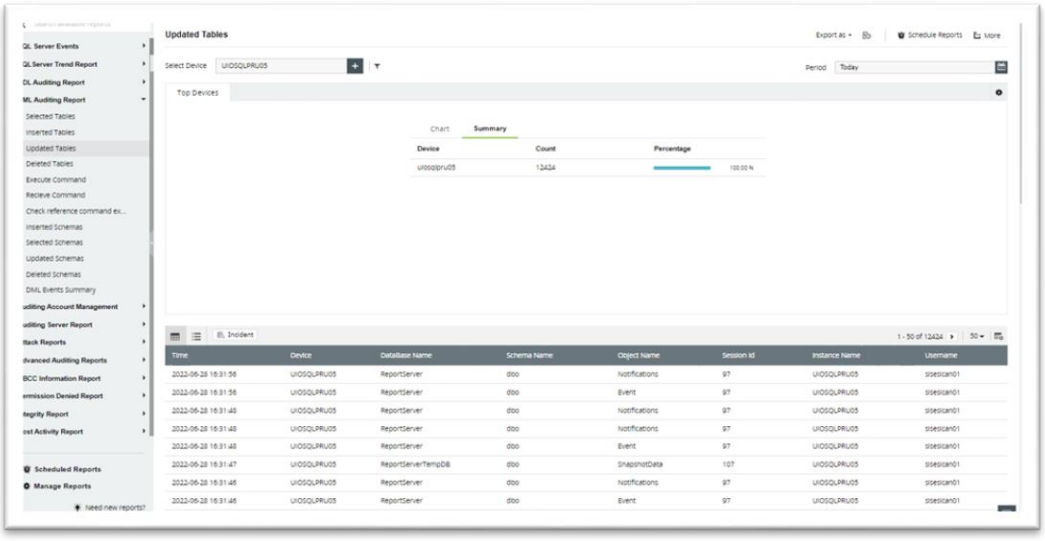
Figura 22
Registro de eventos en SIEM



Nota. Tomado de consola de administración EventLog Analyzer

Control 8.4.2 Protección de los registros de información: el correlacionador de eventos permite verificar las sentencias de selección, inserción, borrado y actualización que se dan en las tablas, el SIEM maneja una base de datos que es accesible solamente desde la herramienta y no es manipulable, como se muestra en la Figura 23.

Figura 23
Actualizaciones a una tabla

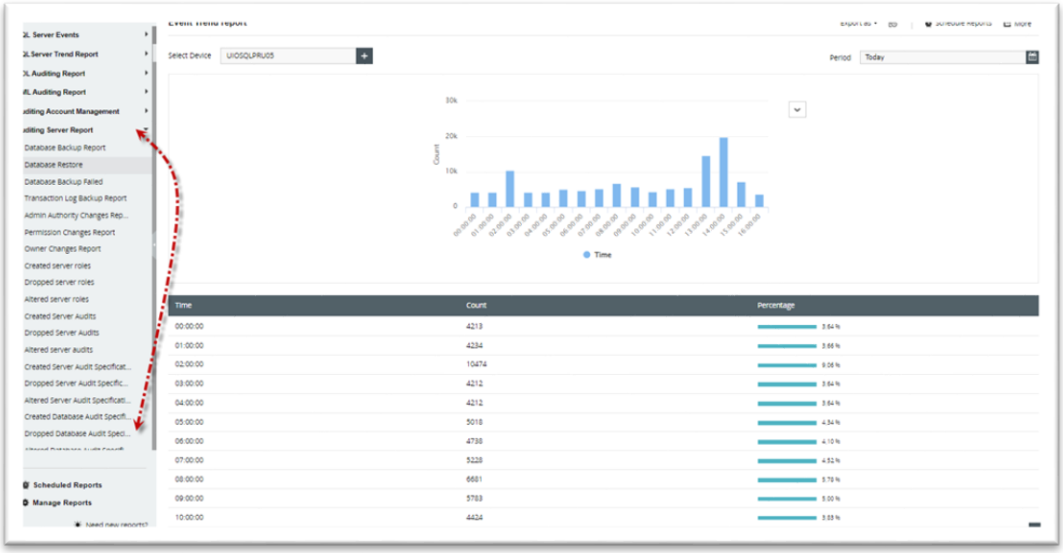


Nota. Tomado de consola de administración EventLog Analyzer

Control 8.4.3 Registros de administración y operación: el aplicativo permite monitorear las acciones realizadas por el administrador de base de datos y los operadores que se conectan a los datos críticos, como se evidencia en la Figura 24 se observa las estadísticas de cambios realizados sobre objetos.

Figura 24

Eventos de administración de base de datos

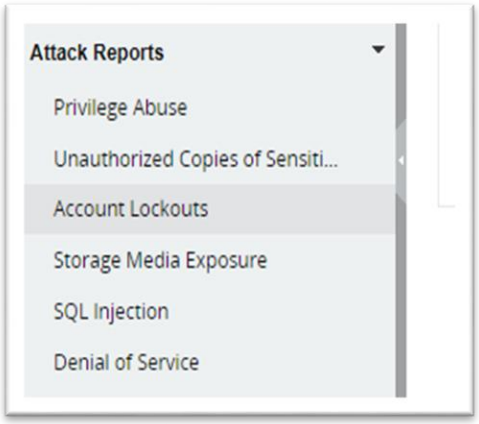


Nota. Tomado de consola de administración EventLog Analyzer

Control 8.6.1 Gestión de las vulnerabilidades técnicas: el SIEM estudiado presenta algunas herramientas que permiten gestionar las debilidades que se pueden presentar, por ejemplo, el abuso de privilegios, copias sin autorización de los datos, ataques de inyección de SQL, denegación de servicios entre otros, todos se encuentran almacenados para de ser el caso analizarlos posteriormente, como se muestra en la Figura 25.

Figura 25

Reportes de vulnerabilidades que se pueden detectar

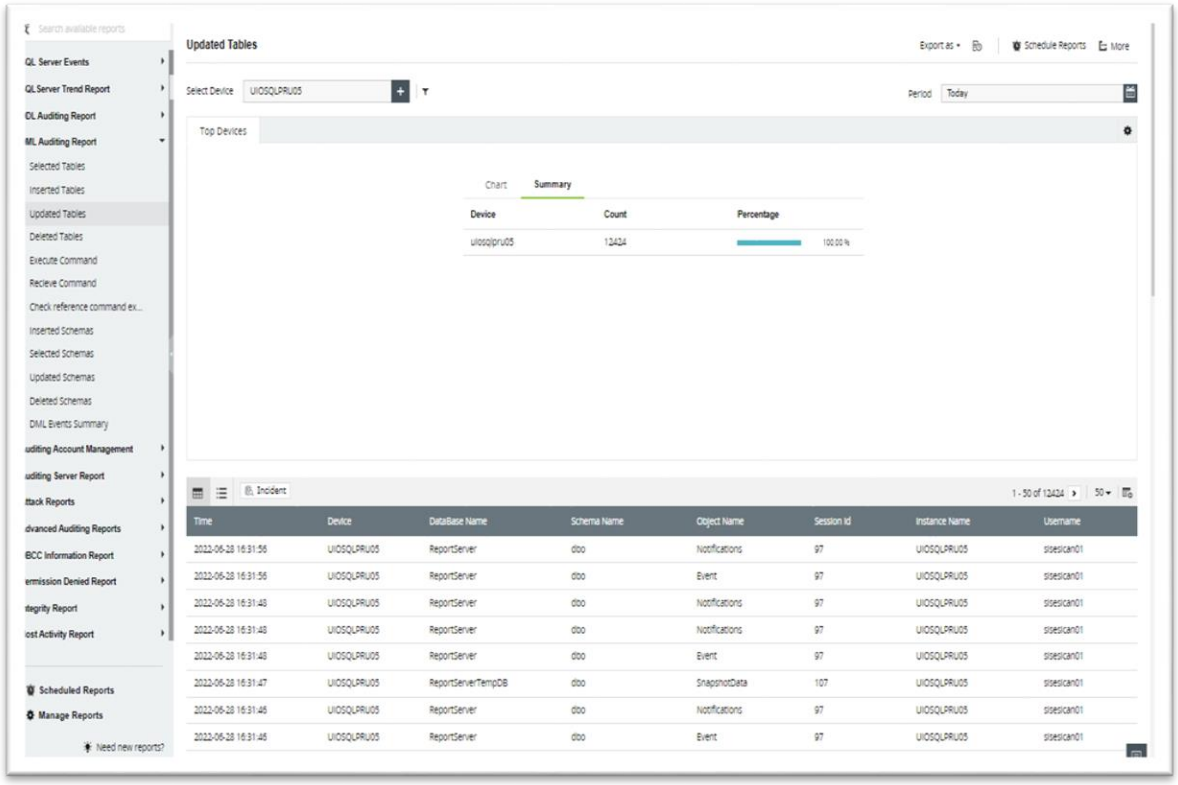


Nota. Tomado de consola de administración EventLog Analyzer

Control 8.7.1 Controles de auditoría de sistemas de información: el correlacionador de eventos permite verificar las sentencias de selección, inserción, borrado y actualización que se dan en las tablas, se puede llevar una auditoría de las acciones que se producen, como se muestra en la Figura 26.

Figura 26

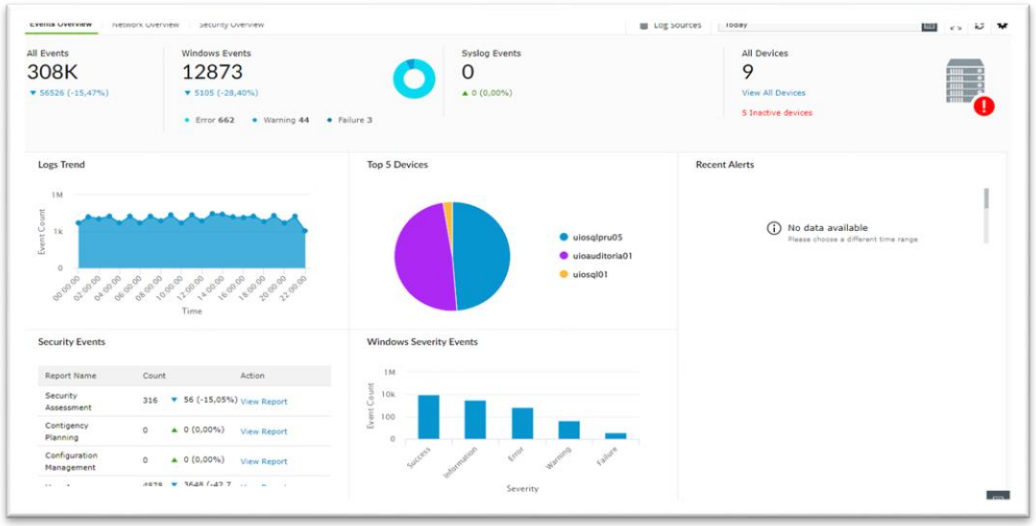
Registro de actualización de tablas en una base de datos



Nota. Tomado de consola de administración EventLog Analyzer

Control 12.1.1 Responsabilidades y procedimientos: la herramienta Eventlog Analyzer estudiada, posee una pantalla de monitoreo que permite a primera vista comprobar que ataques o incidentes de seguridad se pueden presentar en los servidores de base de datos, se tiene una panorámica global para el monitoreo; además es configurable, se ingresa a que usuarios se enviarán las alarmas para que tomen las acciones de mitigación, como se muestra en la Figura 27.

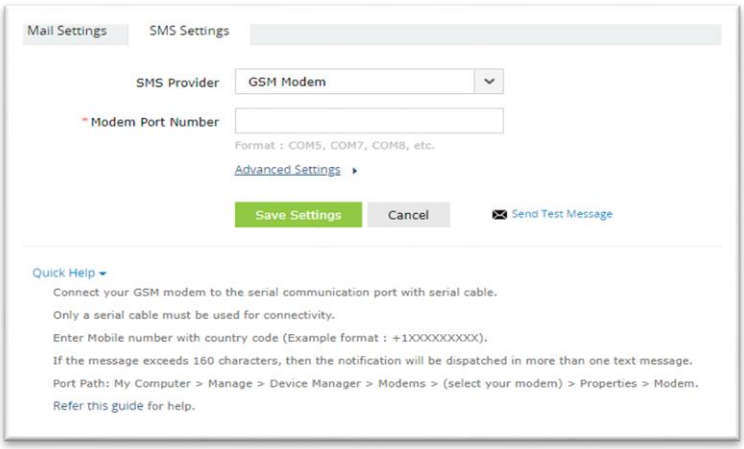
Figura 27
Dashboard de SIEM



Nota. Tomado de consola de administración EventLog Analyzer

Control 12.1.2 Reporte de los eventos de seguridad de la información: se puede recibir incidentes de seguridad por correo electrónico y mensajes SMS, esto ayuda a los operadores a tener una reacción rápida ante ciberataques, como se muestra en la Figura 28.

Figura 28
Configuración de notificaciones electrónicas

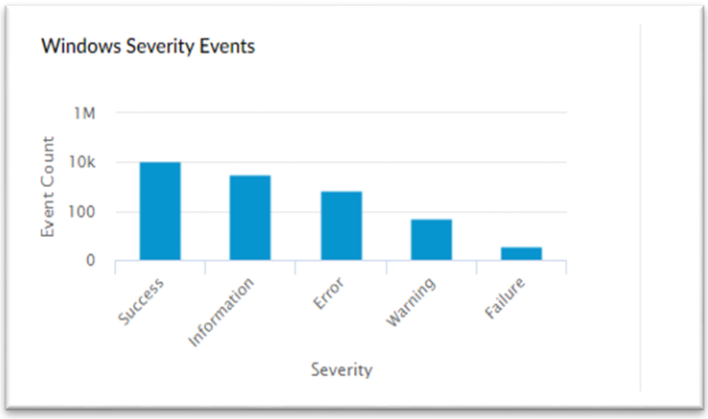


Nota. Tomado de consola de administración EventLog Analyzer

Control 12.1.3 Reporte de debilidades de seguridad de la información: al tener un SIEM se puede centralizar toda la información en un solo lugar y no dispersa en sistemas propios de las herramientas que son difíciles de administrar, esto permite hacer una correlación de eventos que muestran ataques a las bases de datos en tiempo real, como se muestra en la figura 25.

Control 12.1.4 Apreciación y decisión sobre los eventos de seguridad de la información: con un SIEM se puede clasificar que eventos de seguridad son verdaderas amenazas o son parte normal del funcionamiento de una base de datos, como se muestra en la Figura 29.

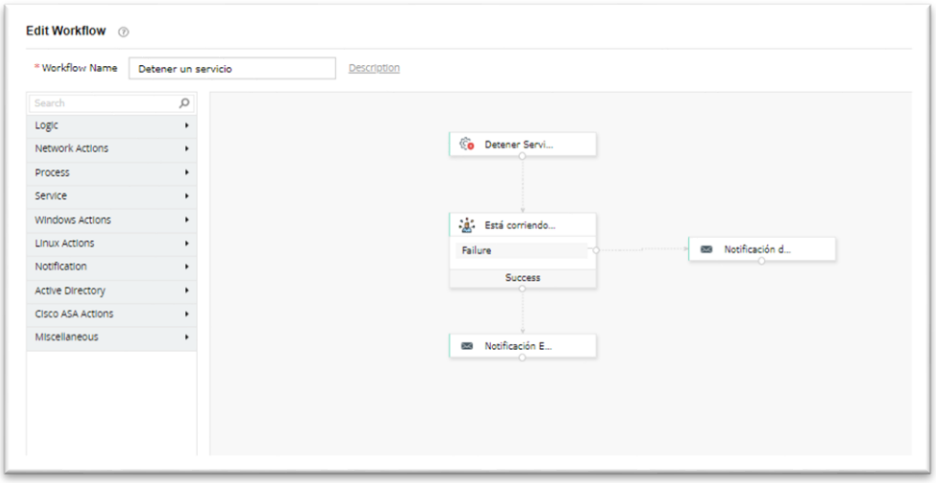
Figura 29
Severidad de eventos Windows



Nota. Tomado de consola de administración EventLog Analyzer

Control 12.1.5 Respuesta a incidentes de seguridad de la información: al contar con un SIEM se puede centralizar el monitoreo de incidentes de seguridad, esto permite tener una respuesta ágil ante las amenazas, además el utilitario permite parametrizar los pasos a seguir para mitigar un ataque, como se muestra en la Figura 30 se puede realizar tareas personalizadas para reaccionar a eventos no controlados.

Figura 30
Workflow para detener un servicio

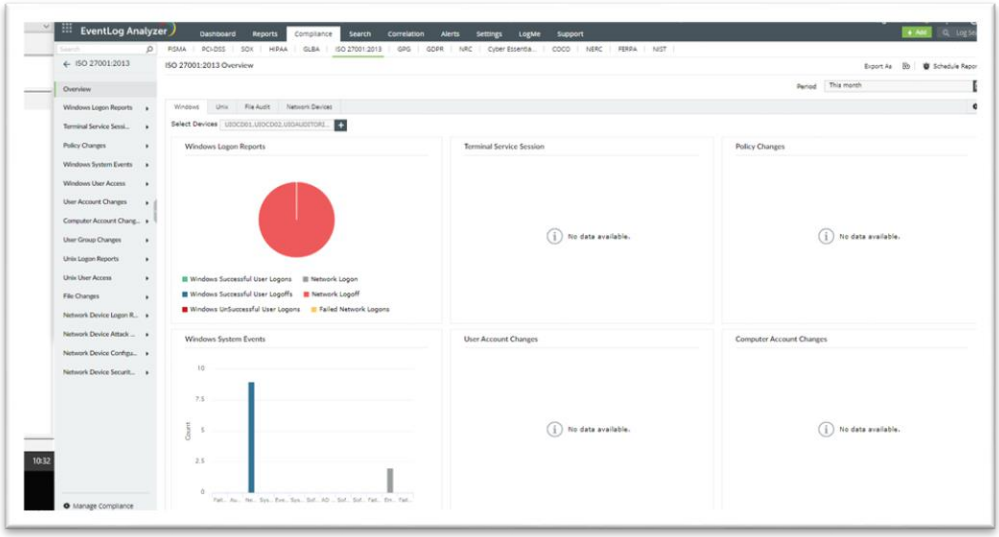


Nota. Tomado de consola de administración EventLog Analyzer

Control 12.1.6 Aprendizaje de los incidentes de seguridad de la información: la herramienta ayuda a permanecer en un constante aprendizaje para mejorar los métodos de protección, el SIEM trata de cerrar las vulnerabilidades que se puedan presentar, esto se puede realizar con los informes que la herramienta permite generar. Permite crear reportes de cumplimiento de normativas internacionales, como se muestra en la Figura 31.

Figura 31

Reporte para la ISO 27001:2013



Nota. Tomado de consola de administración EventLog Analyzer

Como se muestra un SIEM asiste de manera favorable al cumplimiento de EGSI V2.0, en los hitos analizados, detecta amenazas que se registran en una base de datos, generando alertas tempranas, ayudando a los operadores a realizar su trabajo de mejor manera.

1.3.4. Situación propuesta de amenazas hacia las bases de datos con un SIEM

Para remediar las vulnerabilidades presentes en las bases de datos del MREMH se revisó que opciones del SIEM pueden ser usadas para detener los ataques, los hallazgos encontrados demuestran que el SIEM es de mucha ayuda a mitigar los ataques que se puedan producir.

La Tabla 6 muestra como un SIEM aporta 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 Cancillería.

Tabla 6
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

Vulnerabilidades	*Situación actual*	*Situación propuesta con un SEIM*	*Impacto*
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

Vulnerabilidades	***Situación actual***	***Situación propuesta con un SEIM***	***Impacto***
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

Nota. Autoría propia

En la Tabla 7 se observa 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.

Tabla 7
Impacto de vulnerabilidades en las bases de datos con un SIEM

Estado	No. Vulnerabilidades	Porcentaje
Crítico	0	0,00%
Medio	3	33,33%
Bajo	6	66,67%
Total	**9**	**100,00%**

Nota. Autoría propia

1.3.5. Situación propuesta de controles de EGSI V2.0 en el MREMH

Después de la instalación y configuración del SIEM Eventlog Analyzer, se evaluó los trece controles que se fortalecieron, se comprobó que a través de la recolección de logs de seguridad y envío de notificaciones hacia los operadores 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 8, 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 el MREMH.

Tabla 8

Estado propuesto de controles del EGSI V2.0 en el MREMH 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

Dominio	*Categoría*	*Objetivos de control*	*Control*	*Observación*	*Control reforzado*	*Estado*
		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 Eventlog Analyzer 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

Dominio	*Categoría*	*Objetivos de control*	*Control*	*Observación*	*Control reforzado*	*Estado*
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 detecte 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

Dominio	*Categoría*	*Objetivos de control*	*Control*	*Observación*	*Control reforzado*	*Estado*
		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 EventLog Analyser 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

Nota. Autoría propia

Tabla 9
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%**

Nota. Autoría propia

La Tabla 9 muestra como el 83,33% de los controles podrían estar implementados en su totalidad y el 16,67% tendrían la implementación parcial, esto se debe a que aún no se han definido políticas o procedimientos para tener una implementación exitosa.

CAPÍTULO II: ARTÍCULO PROFESIONAL

2.1. Resumen

La información de las organizaciones alojada en bases de datos son un activo muy importante, apetecido por los cibercriminales, el Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH) maneja datos críticos de ciudadanos nacionales y extranjeros, estos deben ser protegidos de ataques cibernéticos que pueden extraerlos y utilizarlos de manera fraudulenta.

En la investigación se identificaron amenazas que pueden poner en peligro el motor de base de datos SQL Server 2016 Standard y cómo estás 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 de esta entidad.

Se estudió como un SIEM ayudaría a cumplir con los controles del Esquema Gubernamental de Seguridad de la Información Versión 2.0 (EGSI V2.0), además, se realizó una comparativa del cumplimiento de los hitos antes y después de utilizar un SIEM.

a. Palabras clave:

SIEM, MREMH, EGSI, BDD, Seguridad.

2.2. Abstract

The information of the organizations hosted in databases is a very important asset, desired by cybercriminals, the Ministry of Foreign Affairs and Human Mobility (MREMH) manages critical data of national and foreign citizens, these must be protected from cyber-attacks that can extract and use them fraudulently.

In the investigation, threats were identified that can endanger the SQL Server 2016 Standard database engine and how they could exploit the present vulnerabilities, it is proposed to carry out a study of a Security Information and Event Management (SIEM) to identify if it is a valid tool. to reduce the attacks that can occur on critical data of this entity.

It was proposed how a SIEM would help to comply with the controls of the Government Information Security Scheme Version 2.0 (EGSI V2.0), in addition, a comparison of compliance with the milestones was made before and after using a SIEM.

a. Keywords

SIEM, MREMH, EGSI, BDD, Security.

2.3. Introducción

La tecnología en los últimos años ha evolucionado de una manera vertiginosa, las bases de datos en las organizaciones son considerados en activo más importante, en ellas se almacena los datos apreciados como críticos, por lo que se debe proteger a la información sensible, los incidentes de seguridad ponen en riesgo la triada de la seguridad confidencialidad, integridad y disponibilidad; se debe buscar la manera de mitigar ciberataques.

En el Ecuador, el sector público ha sido objeto de ataques informáticos que tratan de obtener información o simplemente causar indisponibilidad de los sistemas publicados hacia el Internet. Dentro de los servicios que son consumidos existen datos que pueden ser publicados y otros que no, salvo que la persona lo permita (Ley Orgánica de Protección de Datos Personales.- RO Suplemento 459, del 26 de mayo del 2021, s. f., p. 14 Art. 7).

La Ley Orgánica de Protección de Datos Personales publicada en año 2021 tiene como objetivo y finalidad «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» (Ley Orgánica de Protección de Datos Personales.- RO Suplemento 459, del 26 de mayo del 2021, s. f., p. 9 Art. 1). 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 Esquema Gubernamental de Seguridad de la Información Versión 2.0 (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» Esquema Gubernamental de Seguridad de la Información, (2020). Los controles mencionados obligan 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 aprovechen vulnerabilidades presentes. La utilización de un correlacionador de eventos podría ayudar a las organizaciones públicas a cumplir con los controles que emana el EGSI V2.0.

El Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH), tiene dentro de sus motores de bases de datos al SQL Server 2016 Standard en diferentes servidores, no se lleva un control de los eventos de seguridad que se generan, no existe un repositorio para almacenarlos y procesarlos.

El presente artículo está dirigido al personal que tiene como función la seguridad de los datos dentro de las organizaciones, quienes son responsables de dictar las políticas que rigen la protección de las bases de datos, además, tiene como objetivo realizar un estudio de un System Information and Event Management (Sistema de Gestión de Eventos e Información de Seguridad) o sus siglas en inglés (SIEM) sobre la base de datos SQL Server 2016 Standard para una posible implementación en el Ministerio de Relaciones Exteriores y Movilidad Humana.

2.4. 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 puede ayudar a su cumplimiento, también se analizó el comportamiento de un SIEM para conocer su capacidad de detección ante ataques que se pueden dar en un motor de base de datos.

Se plantea analizar como un SIEM para las bases de datos del MREMH 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 SIEM 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 el MREMH.

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

2.4.1. Conceptos generales

Martínez & Tejada, (2019) 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. (pág. 15).
Los datos manejados por la Cancillería son considerados sensibles, esto conlleva a que sean monitoreados de manera continua para evitar accesos no permitidos e indisponibilidad.

El MREMH cuenta con una diversidad de sistemas desarrollados por la institución y otros adquiridos a proveedores externos, los aplicativos son usados las veinticuatro horas del día en todo el mundo, ya que el Ecuador tiene Embajadas y Consulados repartidos en todo el globo; la mayoría de información es almacenada en el motor de base de datos principal que es SQL Server 2016 Standard.

Security Information and Event Management (SIEM), estos entregan un estudio en línea de las alarmas de seguridad informática suscitadas en el hardware y software de la infraestructura Cómbita, (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.

Un SIEM posee varias capas como se muestra en la Figura 1.

Las capas se describen a continuación Pazmiño & Pazmiño, (2018):

- 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 culminado esta etapa tengan el mismo estándar de datos y sigan a la capa de correlación.
- Capa de correlación: tienen el objetivo principal 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.

La tecnología evoluciona constantemente, esto también influye el correlacionador de eventos, en la mayoría de infraestructura los SIEMs cubren las necesidades de detección de amenazas y envío de notificaciones, pero existen arquitecturas mucho más complejas que necesitan que los SIEM realicen tareas más especialidades.

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 esperado.

2.4.2. Investigaciones previas realizadas

Dentro de la literatura investigada se puede mencionar lo siguiente:

En el artículo realizado por Cómbita, (2018) titulado «IMPORTANCIA DE LA GESTIÓN CENTRALIZADA DE REGISTROS EN UN CORRELACIONADOR DE EVENTOS (SIEM) EN UNA ORGANIZACIÓN» indica que:

- La infraestructura en las organizaciones genera logs y no se puede realizar un análisis de los registros por separado, es necesario relacionarlos y deben ser almacenados en un solo repositorio.
- Existen herramientas SIEMs de pago y otras de código libre, la elección dependerá de las necesidades y presupuestos de las instituciones.
- Si se llegará a presentar algún problema en el cual sea necesario un estudio forense un SIEM ayuda a este proceso ya que guarda los registros de incidentes de seguridad presentados.

En la investigación realizada por Vielberth & Pernul, (2018) titulado «A security Information and Event Management Pattern» explica que:

- Un sistema SIEM permite detectar y responder de manera automática a ataques a las vulnerabilidades de las organizaciones.
- Implementar un sistema SIEM permite recopilar y normalizar logs importantes de los diferentes componentes tecnológicos, almacena y centraliza información relevante.
- La mayoría de SIEMs permiten distribuir sus componentes en ambientes diferentes, por ejemplo, un SIEM de base de datos podría tener su almacenamiento en la nube y la demás arquitectura en un Data Center local.

En el artículo académico realizado por González et al., (2021) llamado «SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM): ANALYSIS, TRENDS AND USAGE IN CRITICAL INFRASTRUCTURES» señala lo siguiente:

- Los factores políticos, económicos, sociales, tecnológicos, legales y ambientales producirán una evolución de los SIEMs a mediano y largo plazo.

- En la actualidad los SIEMs permiten una detección y en lo posible una reacción automatizada de amenazas, pero en muchos casos para infraestructuras críticas se requiere la intervención de los operadores para realizar acciones correctivas.
- A futuro algunas de las mejoras que podrán darse en los SIEMs son las siguientes: los SIEMs cubrirán más ámbitos de la seguridad, fusión de datos OSINT traducido como inteligencia de fuentes abiertas (Open Source Intelligence), mejor visualización de resultados, optimización del almacenamiento, Integración con Security Orchestration Automation and Response (SOAR), administración de una enorme cantidad de datos a través de indexación; implementación de inteligencia artificial (AI) que dará capacidades predictivas al SIEM, útiles para el análisis de anomalías, comportamiento del tráfico de red, herramientas y usuarios.
- El futuro de los SIEMs debe tener en consideración la evolución y sofisticación de los ataques informáticos, el aumento en el uso de dispositivos móviles, más personas utilizando redes sociales y cambios en la regulación.

En el trabajo de Investigación elaborado por Bonilla, (2017) titulado «ELABORACIÓN DE UNA METODOLOGÍA DE DETECCIÓN Y MITIGACIÓN DE VULNERABILIDADES DE BASE DE DATOS Y SU INCIDENCIA EN LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA AUTOMEKANO CÍA. LTDA., DE LA CIUDAD DE AMBATO» explica que:

- Los ataques hacia las bases de datos son de dos tipos, los que no requieren autenticación por ejemplo la explotación de Buffer Overflow y los que requieren autenticación, para este se requiere credenciales válidas para acceder a los motores de base de datos.
- Existen amenazas de seguridad para base de datos, entre ellas se tiene: abuso de exceso de privilegios, abuso legítimo de privilegios, elevación de privilegios, SQL Injection, software de base de datos sin parches, características en los motores de bases de datos que no son necesarias, registros de auditoría débiles, entre otras.
- Las vulnerabilidades presentes en las bases de datos deben contar con estrategias de detección y prevención coherentes.

En el estudio de Hashim, (2018) que lleva el nombre de «Challenges and Security Vulnerabilities to Impact on Database Systems» muestra que:

- La protección de las bases de datos se centra en los siguientes puntos, confidencialidad de la información, integridad de los datos que reposan en los repositorios de datos, accesibilidad a la data que debe estar disponible para consultarla.

- Indica que las amenazas para una base de datos son, abuso de privilegios, abuso de privilegios legítimos, elevación de privilegios, vulnerabilidades en los motores de base de datos, inyección de SQL, auditoría no robusta, denegación de servicios, vulnerabilidades en protocolos de comunicación a las bases de datos, autenticación débil, exposición de los respaldos de base de datos.

De los artículos analizados se puede desprender que, los SIEMs son herramientas de suma importancia para prevenir ataques hacia los diferentes componentes de una infraestructura de red, ayudan a recolectar, procesar y almacenar incidentes de seguridad.

Las bases de datos constituyen el activo más importante para las organizaciones, en ellas se guarda, procesa y distribuye información que hace funcionar las entidades, estás presentan vulnerabilidades que de no ser identificadas podrían ocasionar serios problemas a los datos de las organizaciones.

Un SIEM permite guardar los eventos que se dan en las bases de datos, si se llegará a presentar algún problema en el cual sea necesario un estudio forense un SIEM ayuda a este proceso ya que guarda los registros de incidentes de seguridad presentados.

2.4.3. Identificación de amenazas

Las principales amenazas encontradas en una base de datos son:

Amenazas internas: las amenazas internas es una de las causas principales de intrusiones de seguridad informática hacia los motores de base de datos, esto se debe a que los administradores de la infraestructura entregan usuarios con permisos elevados incluso con acceso a realizar tareas de administración Prado, (2021), por ejemplo, una persona ajena a la organización que de alguna manera obtuvo claves de acceso a las bases de datos tal vez por ingeniería social, que utiliza diferentes métodos y técnicas para lograr infiltrarse a las instituciones mediante los empleados, este tipo de amenaza es muy frecuente en las entidades y se produce por no manejar un control adecuado de los perfiles de acceso.

Vulnerabilidades de software de bases de datos: los ciberdelincuentes centran sus esfuerzos en encontrar y atacar vulnerabilidades en todo tipo de software, incluidas herramientas de administración de bases de datos. Los proveedores de software de bases de datos propietarios y aplicativos de administración libres generan actualizaciones de seguridad de manera periódica para corregir vulnerabilidades aprovechables, el no actualizar los aplicativos según sugerencias de las empresas creadoras aumenta la exposición de ser atacados.

Ataques de inyección SQL: se produce cuando existe introducción de sentencias SQL o noSQL camufladas en consultas SQL válidas, estás generalmente se lanzan en aplicativos web o encabezados HTTP, en la mayoría de los casos las organizaciones no aplican buenas prácticas en la programación, esto implica que las bases de datos queden expuestas por fallas presentes en sistemas web. Los delincuentes informáticos buscan bases de datos de SQL (Structure Query Language) para inyectar código malicioso a través del lenguaje, puede incluir procedimientos con parámetros de entrada Bonilla, (2017), con este tipo de ataque los intrusos pueden obtener los datos críticos de las organizaciones, pudiendo sufrir pérdidas económicas y lo peor pérdida de reputación.

Pistas de auditoría débiles: la auditoría en la base de datos es muy importante, permite conocer qué acciones se realizan sobre ella, transacciones, actualización de información, entre otras, la auditoría permite realizar un análisis forense, la ausencia de pistas fuertes permitirán realizar acciones que no queden registradas.

Ataques de denegación de servicio: son aquellos en los que atacantes llenan el servidor de base de datos, con un sinnúmero de solicitudes que el equipo consume sus recursos a tal punto que no puede atender las peticiones legítimas y de personas reales, esto conlleva a que el servidor colapse y se inhiba.

Malware: es un software programado por atacantes que tiene como objetivo aprovechar vulnerabilidades y causar daños a las bases de datos, se puede transmitir desde cualquier dispositivo infectado de la red que conecte al servidor de base de datos.

Privilegios excesivos: se produce cuando a los usuarios se les da acceso más allá de sus funciones, lo que podría ser usado para obtener información sensible que solo personal autorizado maneje, por ejemplo, si a un agente consular del MREMH se le da acceso de lectura a una base de datos de trámites podría usar ese perfil para realizar trámites no autorizados.

Abuso de privilegios: los usuarios pueden abusar de los privilegios asignados a ellos para realizar tareas no permitidas, por ejemplo, un agente consular del MREMH tiene permisos para consultar datos personales de ecuatorianos que residen en el exterior, podría exportar la información a un archivo y utilizarlo para fines no autorizados.

Elevación de privilegios: las vulnerabilidades en las bases de datos podrían ocasionar que un usuario con permisos de lectura pueda tener permisos de escritura, por ejemplo, si un atacante produce un desbordamiento de búfer podría elevar los permisos normales a los de administrador.

2.4.4. Controles del EGSI V2.0

El 10 de enero del 2020 el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) expidió el Esquema Gubernamental de Seguridad de la Información Versión 2.0, 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» Esquema Gubernamental de Seguridad de la Información, (2020). En los hitos mencionados se obliga a las instituciones públicas a implementar controles dentro de la Infraestructura para minimizar los riesgos que se puedan producir por amenazas que aprovechan vulnerabilidades que estén presentes; además, en el anexo 1 se muestra la disposición dada por la Coordinación General de Tecnologías de la Información (CGTIC) del MREMH para la implementación de EGSI V2.0. Con la utilización de un correlacionador de eventos se podría ayudar a las organizaciones públicas a cumplir con los controles indicados.

Los controles del EGSI V2.0, con los que un SIEM para base de datos podría ayudar en su implementación son los que se muestran en la Tabla 1.

2.5. Resultados – Discusión

2.5.1. Amenazas hacia las bases de datos SQL Server antes del SIEM

En la Tabla 2 se muestra el estado actual de las amenazas que se tiene en las bases de datos SQL Server 2016 del MREMH 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 se produce el ataque.

La Tabla 3 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 críticos 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.

2.5.2. 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 4 se observa trece controles de EGSI V2.0 que fueron evaluados por el MREMH en los que se hace necesaria la implementación de herramientas tecnológicas que ayuden a gestionar incidentes de seguridad y manejan una base ese 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

En la Tabla 5 se observa el porcentaje de cumplimiento de los controles que fueron analizados para esta investigación, se observa que el 61,54% de los controles estudiados en el MREMH no están cumpliendo los lineamientos requeridos, un 38,46% cumplen la normativa parcialmente y ningún hito cumple al 100% lo dispuesto por el MINTEL.

En la actualidad existen dos personas que administran alrededor de 70 bases de datos, se tiene que el 70% de estas se alojan en el Sistema de Gestión de Base de Datos (SGBD) SQL Server Standard, la transaccionalidad es elevada y se hace imposible el seguimiento y monitoreo constante de los eventos de seguridad que se producen en las mismas.

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.

2.5.3. Descripción de SIEM utilizado para el estudio

El SIEM utilizado para el estudio fue Eventlog Analyzer, mismo que se encontraba instalado, pero sin configuraciones, dentro de las características que el SIEM maneja se tiene las siguientes:

- 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.

Se utilizó una máquina virtual con el sistema operativo Windows Server 2016 Standard donde se tiene instalado el SIEM, las pruebas fueron realizadas en un ambiente controlado.

Para la investigación se ingresaron dos servidores de base de datos como muestra la Figura 5, uno que es de producción y otro que es usado para pruebas; el servidor de producción sirvió para recolectar información de los eventos de seguridad de la base de datos SQL Server 2016 Standard como se evidencia en la Figura 7 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 su estructura en las tablas como se muestra en la Figura 8.

2.5.4. Mitigación de ataques a bases de datos con un SIEM

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

En la Tabla 6 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 Cancillería.

La Tabla 7 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.

2.5.5. Situación propuesta de controles de EGSI V2.0 en el MREMH con un SIEM

Luego de la instalación y configuración del SIEM Eventlog Analyzer, 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, correlacionador 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 8, 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 el MREMH.

En la Tabla 9 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 funcionado 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.

CONCLUSIONES

El SIEM estudiado fue Eventlog Analyzer instalado en un servidor virtual con Windows Server 2016 Standard, la base de datos a la que se analizó fue SQL Server 2016 Standard, se identificaron las vulnerabilidades y como la herramienta puede detectar y mitigar los ataques a los datos críticos del MREMH, el SEIM posee dashboards de fácil interpretación, estos ayudan a los operadores a identificar los ataques que se presentan, se tiene además alertas que son enviadas por correo electrónico que permiten una intervención inmediata para detener los ataques que se están presentando, además, 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, como estás 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, esto se dio gracias a los módulos que la herramienta maneja, alguno 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 que controles del EGSI V2.0 se relacionan con un SIEM y como ayudaría a mejorar la seguridad de las bases de datos SQL Server, se describió los problemas que se presentan en el MREMH en la actualidad sin utilizar el correlacionador de eventos y se muestra el fortalecimiento de los hitos después del estudio.

Se evidencio que el SIEM estudiado, ofrece varias características válidas para mitigar ataques a las bases de datos y también entrega informes detallados para el cumplimiento del EGSI V2.0.

Del estudio 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 que aporta al cumplimiento del ODS sugerido en este artículo.

RECOMENDACIONES

Después de realizar el trabajo investigativo donde se evidencia que un SIEM para base de datos SQL Server 2016 Standard ayuda a detectar vulnerabilidades y detener ataques, es recomendable que se implemente para todos los motores de base de datos que maneja el MREMH como son: Oracle, PostgreSQL, Sybase, Mysql, etc.

Es recomendable el despliegue del SIEM para los demás dispositivos que puedan generar logs de seguridad que maneja el MREMH (Firewall, IPS, IDS, Router, etc.), esto permitirá tener una visión general para la detección y mitigación de ciberataques.

Después de la integración de los dispositivos al SIEM se debe analizar todos los controles del EGSI V2.0, e identificar qué hitos adicionales pueden ser fortificados con el uso de la herramienta, de igual manera se deben definir las políticas y procedimientos que aún no han sido redactadas.

Se sugiere realizar la actualización periódica del software de base de datos, al ser datos críticos es recomendable realizar pruebas en ambientes controlados y certificar que los parches de seguridad aplicados no afecten la funcionalidad de los sistemas.

Se debe establecer los roles que van a realizar los operadores del SIEM y de base de datos, esto ayudará a definir y direccionar las alarmas cuando se sufra una violación de seguridad.

Es recomendable que se tengan actualizadas las reglas del SIEM para detectar nuevas amenazas.

Se debe considerar el espacio que el SIEM utilizará para almacenaje de logs, según lo dispuesto por la ley ecuatoriana es siete años, dicho espacio podría ser utilizado en la nube, con esto se descentraliza la arquitectura de la herramienta.

BIBLIOGRAFÍA

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

Arango, J. D. (2016). *Implementacion de un Gestor de Seguridad de la Informacion y Gestion de Eventos (SIEM)* [Especialización en Seguridad Informática, Universidad de San Buenaventura]. https://bit.ly/3A22ftx

Auditoría de bases de datos | *Software de auditoría de bases de datos—ManageEngine EventLog Analyzer*. (s. f.). Recuperado 22 de junio de 2022, de https://bit.ly/3SWFfVx

Bartolomé, M., & Monteiro, 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

Basantes, A. C. (2021, julio 22). Te explicamos lo que pasó con el ataque a CNT. *GK*. https://gk.city/2021/07/22/ataque-cnt-informatico/

Bonilla, C. A. (2017). *Elaboración de una metodología de detección y mitigación de vulnerabilidades de base de datos y su incidencia en la seguridad de la información de la empresa Automekano Cía. Ltda., de la ciudad de Ambato* [Magíster en Gestión de Bases de Datos, Universidad Técnica de Ambato]. https://bit.ly/3w2NHZC

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

Cómbita, J. P. (2018). *Importancia de la gestión centralizada de registros en un correlacionador de eventos (SIEM) en una organización* [Especialista en Seguridad Informática, Universidad Piloto de Colombia]. https://bit.ly/3w8wkGK

Días, V. (2021, octubre 11). *Banco Pichincha confirma «incidente de ciberseguridad» en sus sistemas*. El Comercio. https://bit.ly/3bXPngc

Fernandez, E. (2019, abril 5). ¿Qué es un Firewall de next-generation? *Revista de Ciberseguridad y Seguridad de la Información para Empresas y Organismos Públicos.* https://bit.ly/3C62zdF

González, G., González, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors (Basel, Switzerland)*, *21*(14), 4759. https://doi.org/10.3390/s21144759

Hashim, H. B. (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

Keary, T. (2019, noviembre 28). IDS vs IPS - What's the Difference & Which do You Need? *Comparitech*. https://www.comparitech.com/net-admin/ids-vs-ips/

Ley Orgánica de la Contraloría General del Estado.- RO Suplemento 595, del 12 de junio del 2002; reformas RO No.31 del 07 de julio del 2017. https://bit.ly/3Arit13

Ley Orgánica de Protección de Datos Personales.- RO Suplemento 459, del 26 de mayo del 2021. https://bit.ly/3AqdT2M

Martínez, D. A., & Tejada, L. (2019). *Manual de bases de datos*. Universidad Abierta para Adultos (UAPA). https://elibro.net/es/ereader/uisrael/175897?page=15

Esquema Gubernamental de Seguridad de la Información, 025-2019 Acuerdo Ministerial 123 (2020). https://bit.ly/3QIeWAA

Política de Ciberseguridad, 006-2021 Acuerdo Ministerial 89 (2021). https://bit.ly/3JWprho

Naik, S. (2014). *Concepts of database management system*.

ODS de las Naciones Unidas. (2017, septiembre 25). *Desarrollo Sostenible*. https://bit.ly/2qk9f28

Pazmiño, C., & Pazmiño, J. (2018). *Implementación de un Correlacionador de Eventos basado en software libre para la detección de ataques informáticos en la Empresa Eléctrica* [Escuela Superior Politécnica de Chimborazo]. https://bit.ly/3Sd1uWA

Prado, J. P. (2021). Ingeniería social, un ejemplo práctico. *REVISTA ODIGOS*, *2*(3), 47-76. https://doi.org/10.35290/ro.v2n3.2021.493

Pulido, E., Escobar Dominguez, O., & Nuñez Perez, J. A. (2019). *Base de datos*. Grupo Editorial Patria. https://elibro.net/es/ereader/uisrael/121283

Ramírez, S. (2020, mayo 7). Inteligencia artificial y Machine learning. *ManageEngine Blog*. https://bit.ly/3pkA446

Švarc, L., & Strnad, P. (2021). Automated Computer Attacks Detection in University Environment. *Acta Informatica Pragensia*, *10*(1), 75-84. https://doi.org/10.18267/j.aip.147

Vance, J. (2022, marzo 23). *What is NAC and why is it important for network security?* Network World. https://bit.ly/3QqoAbi

Vielberth, M., & Pernul, G. (2018). *A Security Information and Event Management Pattern*. https://bit.ly/3C4T4v5

GLOSARIO DE TÉRMINOS

Malware: La palabra es la combinación de los términos “software” y “malicioso”, cubre todas las clases de aplicaciones malignas que pueden comprometer la seguridad de un dispositivo.

Ransomware: Es un tipo de malware que impide el acceso a la información, se exige un pago para devolver el acceso a los datos.

Spear Phsing: Es una estafa que se presenta por medio de correo electrónico, estas comunicaciones van dirigidas a personas o empresas, su objetivo es engañar para obtener datos de los usuarios para fines maliciosos, además, los ciberdelincuentes pueden instalar malware en computadores o servidores de sus víctimas.

ANEXOS

ANEXO 1

Memorando Nro. MREMH-CGTIC-2021-0664-M

Memorando Nro. MREMH-CGTIC-2021-0664-M

Quito, 21 de diciembre de 2021

PARA: Sr. Mgs. Fernando Esteban Bermeo Mancheno
Director Administrativo, Encargado

Srta. Dra. América Lourdes Pereira Sotomayor
Directora de Administración del Talento Humano

Sr. Emb. Francisco Augusto Riofrío Maldonado
Director de Gestión Documental y Archivo

Ing. Pablo Xavier Corrales Arauz
Director de Diseño e Implementación de T.I.

Sr. Mgs. Christian Roberto Ordóñez Orellana
Director de Infraestructura, Seguridad y Soporte de T.I.

Sr. Mgs. Jairo Vinicio Eras Nieto
Secretario del Comité de Seguridad de la Información del MREMH

ASUNTO: Remítese Informe de seguimiento de la implementación de hitos del EGSIv2 en el MREMH.

Mediante Memorando Nro. MREMH-CGTIC-2020-0596-M, de 18 de noviembre de 2021, esta Coordinación informó sobre la metodología de evaluación que utilizará MINTEL para la revisión de la documentación, verificables e implementación de los diferentes hitos del proyecto que contempla el EGSI v2, además, solicitó el nombre de los funcionarios delegados de las unidades administrativas a cargo de la implementación de los hitos del EGSI v2, con la finalidad de

coordinar con las áreas involucradas la revisión y preparación de la documentación, y disponer de tiempo para que el Comité de Seguridad designe al Oficial de Seguridad de la Información – OSI de la institución, quien deberá participar en todas las jornadas de evaluación que realizará MINTEL en consideración a que será el responsable de realizar el seguimiento de las recomendaciones sobre este proceso.

ANEXO 2

INFORME DE SEGUIMIENTO DE LA IMPLEMENTACIÓN DE HITOS DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN – (EGSI v2.0)

1. Objetivo

Conocer el cumplimiento de la implementación de los hitos del Esquema Gubernamental de Seguridad de la Información V2.0, en las distintas unidades administrativas que se encuentran a cargo de gestionar los hitos.

2. Antecedentes

Mediante Edición Especial No. 228 de 10 de enero de 2020 fue publicado en el Registro Oficial el Acuerdo Ministerial No. 025-2019 que contiene en su Anexo el Esquema Gubernamental de Seguridad de la Información (EGSI versión 2.0), el cual es de implementación obligatoria en las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva (APCID).

Mediante Acuerdo No. 25 - 2019, el Ministerio de Telecomunicaciones y de la Sociedad de la Información dispone, en su Art.1, la implementación obligatoria en las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el Esquema Gubernamental de Seguridad de la Información – EGSI.

Con fecha 17 de noviembre de 2021, la Dirección de Infraestructura, Interoperabilidad, Seguridad de la Información y Registro Civil de MINTEL, notificó a la Coordinación General de Tecnologías de la Información y Comunicación sobre el inicio del proceso de evaluación de la Implementación del Esquema Gubernamental de Seguridad de la Información (EGSI v2) del MREMH, y remitió el cronograma de evaluación con fechas tentativas de los días lunes 22, martes 23 y miércoles 24 de noviembre de 2021.

Se consideró el cronograma de evaluación de acuerdo a lo determinado por MINTEL, se evaluó si el hito contiene documentación como: política, procedimiento, manuales, bitácoras, checklist, informes y toda información que sustente la ejecución del hito. En el proceso de evaluación participaron los funcionarios de la DISSTI (Diego Montenegro, Julio Loachamin, Luis Clavijo, Carmen Azua y Eduardo Bolaños), y CGTIC (Ana María Paredes).

La evaluación que se realizó de manera interna a cada uno de los funcionaros responsables de gestionar los hitos en las unidades administrativas, la cual se basó en una serie de preguntas acorde a la ISO 27000 enfocadas en la gestión propia del hito, entrega de productos/verificables para la correcta implementación de cada hito. Se emitieron las debidas recomendaciones para fortalecer la ejecución y cumplimiento del hito acorde a cada pregunta evaluada.

Considerando que algunos hitos no contaban con los verificables que sustente su implementación, se solicitó la entrega de la información que demuestre el cumplimiento del hito, hasta el 30 de diciembre de 2021, dichos entregables deben ser remitidos a los compañeros encargados de revisar los hitos. (Carmen Azua y Julio Loachamin).

Se detectó que los funcionarios a cargo de los hitos no cumplen en su totalidad con la ejecución del hito, puesto que los procedimientos no se encuentran socializados a todas las unidades administrativas, además no se cuenta con bitácoras, repositorios centralizados para el manejo de la información propia del hito, y cierta información no se encuentra de manera organizada.

Como anexo se remite la matriz del *"Estado y Aplicabilidad de controles de Seguridad de la Información"*, en la cual se detalla por hitos las observaciones detectadas en el proceso de evaluación preliminar.

A continuación, se detalla el estado de la situación actual de cumplimiento de los hitos: