GESTOR DE EVENTOS DE SEGURIDAD PARA MONITOREO DE LOS SERVIDORES WINDOWS DE LA EMPRESA MAZARS COLOMBIA SAS

JHON ALEXANDER LOPEZ NARANJO
EDWIN RICARDO SALAMANCA GUERRERO

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE POSTGRADOS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2021

GESTOR DE EVENTOS DE SEGURIDAD PARA MONITOREO DE LOS SERVIDORES WINDOWS DE LA EMPRESA MAZARS COLOMBIA SAS

JHON ALEXANDER LOPEZ NARANJO
EDWIN RICARDO SALAMANCA GUERRERO

Trabajo de grado como requisito parcial para optar el título de Especialista en Seguridad Informática

Asesor
INGENIERO ÁLVARO ESCOBAR ESCOBAR
Director Especialización en Seguridad Informática

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE POSTGRADOS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2021

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Bogotá D.C., agosto de 2021

Dedicamos este trabajo de grado a nuestros padres quienes nos apoyaron en todo momento. A nuestras familias que nos alentaron para continuar cuando parecía que nos rendiríamos. A los maestros de quienes nos enseñaron, sin importar las deficiencias en conocimiento que teníamos. Y a todos aquellos que depositaron su esperanza en nosotros. Para ellos es dedicado este trabajo de grado, ya que a ellos debemos su apoyo incondicional

AGRADECIMIENTOS

Le agradecemos a Dios por sabernos guiar y por acompañarnos en el transcurso de la especialización, por ser quien nos pudo dar la fortaleza necesaria en los momentos más débiles y frustrantes que tuvimos, por brindarnos el poder de aprender y progresar paso a paso, por poder disfrutar de las experiencias vividas y la felicidad que nos acompañó en el transcurso de este tiempo. También le agradecemos a nuestros padres por brindarnos la oportunidad de recibir una buena educación, y sobre todo por ser nuestro ejemplo a seguir.

CONTENIDO

	pág.
INTRODUCCIÓN	15
1. FORMULACIÓN DEL PROBLEMA	16
1.1 PLANTEAMIENTO – DESCRIPCIÓN GENERAL	16
1.2 FORMULACIÓN – PREGUNTA	16
2. OBJETIVOS	17
2.1 OBJETIVO GENERAL	17
2.2 OBJETIVOS ESPECÍFICOS	17
3. TIPO DE INVESTIGACIÓN	18
4. HIPÓTESIS	19
5. VARIABLES	20
6. MARCO TEORICO	21
6.1 ¿QUÉ ES UN SIEM?	21
6.2 MANEJO DE INCIDENTES	22
6.2.1 Preparación	23
6.2.1.1 Preparación para manejar incidentes	23
6.2.1.2 Prevención de incidentes	23
6.2.2 Detección y análisis de incidentes	24
6.2.2.1 Signos de un incidente	25
6.2.3 Análisis de incidentes	26
7. MARCO DE REFERENCIA	28
7.1 DOCUMENTACIÓN DE INFRAESTRUCTURA	29
7.1.1 Topología de red	29
7.1.2 Aplicaciones/servicios del negocio	29
7.1.3 Estado actual de la organización frente a la seguridad informática	31
8. DESARROLLO	33
8.1 CLASIFICACIÓN DE SERVIDORES CRÍTICOS	33
8.2 ANÁLISIS Y CLASIFICACIÓN DE INCIDENTES	33
8.3 CLASIFICACIÓN DE INCIDENTES	34
8.3.1 Criterios de evaluación	35
8.4 EVENTOS DE WINDOWS SERVER	38
8.5 SELECCIÓN DEL SIEM DE LICENCIAMIENTO LIBRE	39
8.6 INSTALACIÓN Y CONFIGURACIÓN DEL SIEM	42
8.6.1 Requerimientos de Hardware	42

8.6.2 Instalación del SIEM 42
8.7 VERIFICACIÓN DE RESULTADOS 46
8.7.1 Pruebas de verificación 47
8.7.2 Resultados Mitre ATT&CK 49

9. CONCLUSIONES 50

BIBLIOGRAFIA 51

ANEXOS 54

LISTA DE FIGURAS

pág.

Figura 1. Topología de Red Mazars Colombia 29
Figura 2. Criterios de evaluación 36
Figura 3. Diagrama de arquitectura de implementación de Wazuh 42
Figura 4. Versión sistema operativo 43
Figura 5. Servicio Elasticsearch 43
Figura 6. Servicio Logstash 43
Figura 7. Servicio Wazuh 44
Figura 8. Servicio Filebeat 44
Figura 9. Servicio Kibana 45
Figura 10. Modulos wazuh 45
Figura 11. Agente de instalación para clientes 45
Figura 12. Módulo de eventos de seguridad 46
Figura 13. Módulo de Agentes 47
Figura 14. Login Erróneo 47
Figura 15. Visor de Eventos Windows 48
Figura 16. Visor de eventos wazuh 48
Figura 17. Modulo Mitre ATT&CK 49

LISTA DE CUADROS

pág.

Cuadro 1. Desglose de la Matriz de Riesgo (consultar Anexo B) 34
Cuadro 2. Criterios de evaluación 36
Cuadro 3. Categoría de Incidentes 37
Cuadro 4. ID Eventos 38
Cuadro 5. Comparación SIEM Libre 39
Cuadro 6. Calificación de SIEM 40

LISTA DE ANEXOS

pág.

Anexo A. Matriz de Riesgos Mazars Colombia SAS 54
Anexo B. Perfil de los Sistemas 57
Anexo C. Carta de Cumplimiento 67
Anexo D. NDA Mazars Colombia 68

GLOSARIO

ACCESO NO AUTORIZADO: es un incidente que involucra a una persona, sistema o código malicioso que obtiene acceso lógico o físico sin autorización adecuada del dueño a un sistema, aplicación, información o un activo de información.

ACTIVO: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.[1]

AMENAZA: causa potencial de un incidente no deseado que puede provocar daños a un sistema o a la organización.[2]

ATAQUE: intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.[3]

CONFIDENCIALIDAD: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.[4]

CONTROL DE ACCESO: garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad[5]

DISPONIBILIDAD: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada[6]

EVENTO: un evento es cualquier ocurrencia observable en un sistema o red. Los eventos incluyen un usuario que se conecta a un archivo compartir, un servidor que recibe una solicitud de una página web, un usuario que envía un correo electrónico y un firewall que bloquea un intento de conexión. Los eventos adversos son eventos con consecuencias negativas, como fallas del sistema, inundaciones de paquetes, uso no autorizado de privilegios del sistema, acceso no autorizado a datos confidenciales y ejecución de malware que destruye datos.[7]

---

[1] ISO. Organización Internacional de Normalización. ISO/IEC 27000. Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Descripción general y vocabulario [en línea]. Ginebra: ISO [citado 24, abril, 2021]. Disponible en Internet: < URL: https://www.iso27000.es/glosario.html>

[2] Ibid., p.2.

[3] Ibid., p.2.

[4] Ibid., p.3.

[5] Ibid., p.2.

[6] Ibid., p.2.

[7] NIST. National Institute of Standards and Technology. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Information secuity. [en línea]. Ginebra: ISO [citado 24, abril, 2021]. Disponible en Internet: < URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.[8]
GDPR: ley de protección de datos de la unión europea (Reglamento General de Protección de Datos).[9]

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información[10]

INCIDENTE: es una violación o amenaza inminente de violación 1 de las políticas de seguridad informática, políticas de uso aceptable o prácticas de seguridad estándar.[11]

INTEGRIDAD: propiedad de la información relativa a su exactitud y completitud. [12]

INVENTARIO DE ACTIVOS: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.[13]

MITRE ATT&CK: es una base de conocimientos a nivel mundial accesible de las tácticas del adversario y técnicas basadas en observaciones del mundo real. La base de conocimientos de ATT & CK se utiliza como base para el desarrollo de modelos y metodologías de amenazas específicas en el sector privado, en el gobierno y en la comunidad de productos y servicios de ciberseguridad.[14]

MODIFICACIÓN DE RECURSOS NO AUTORIZADO: un incidente que involucra a una persona, sistema o código malicioso que afecta la integridad de la información o de un sistema de procesamiento.

MONITOREO: determinar el estado de un sistema, un proceso o una actividad. Para determinar el estado, puede ser necesario verificar, supervisar u observar

---

[8] ISO. Organización Internacional de Normalización. ISO/IEC 27000, Op. cit., p.2.
[9] PARLAMENTO EUROPEO Y DEL CONSEJO. Reglamento (UE) 2016/679. [en línea]. España: La entidad [citado 24, abril, 2021]. Disponible en Internet: < URL: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN>
[10] ISO. Organización Internacional de Normalización. ISO/IEC 27000, Op. cit., p.2.
[11] NIST. National Institute of Standards and Technology. Op. cit., p.2.
[12] ISO. Organización Internacional de Normalización. ISO/IEC 27000, Op. cit., p.2.
[13] Ibid., p.2.
[14] MITRE ATT y CK. Base de conocimientos. [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://attack.mitre.org/>

críticamente[15]

NIST 800-53: esta publicación proporciona un catálogo de controles de seguridad y privacidad para los sistemas de información y las organizaciones para proteger las operaciones y los activos de la organización, las personas, otras organizaciones y la Nación de un conjunto diverso de amenazas y riesgos, incluidos ataques hostiles, errores humanos, desastres naturales, fallas, entidades de inteligencia extranjeras y riesgos de privacidad.[16]

NO DISPONIBILIDAD DE LOS RECURSOS: un incidente que involucra a una persona, sistema o código malicioso que impide el uso autorizado de un activo de información.

PCI DSS: las Normas de seguridad de datos de la industria de tarjetas de pago (PCI DSS) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar la adopción de medidas de seguridad uniformes a nivel mundial.[17]

PLUGIN: un complemento o plugin es una aplicación (o programa informático) que se relaciona con otra para agregarle una función nueva y generalmente muy específica.

SERVIDOR: dispositivo físico o programa informático capaz de ofrecer a los clientes determinados servicios (páginas web, correo electrónico, contenidos multimedia en streaming, etc.)[18]

SIEM: las herramientas SIEM son un tipo de software de registro centralizado que puede facilitar la agregación y consolidación de registros de múltiples componentes del sistema de información. Las herramientas SIEM también pueden facilitar la correlación de registros de auditoría y análisis. La correlación de la información del registro de auditoría con la información de escaneo de vulnerabilidades es importante para determinar la veracidad de los análisis de vulnerabilidades y correlacionar la detección de ataques eventos con resultados de escaneo[19]

---

[15] ISO. Organización Internacional de Normalización. ISO/IEC 27000, Op. cit., p.2.
[16] NIST. National Institute of Standards and Technology. Controles de seguridad y privacidad para organizaciones y sistemas de información. [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
[17] PCI. Security Stanards Council. PCI (industria de tarjetas de pago) Normas de seguridad de datos. [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3-2-1-ES-LA.PDF>
[18] RAE. Real Academia Española. Definiciones. [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://dpej.rae.es/lema/servidor>
[19] Ibid., p.2.

SOFTWARE LIBRE: es el software que respeta la libertad de los usuarios y la comunidad. A grandes rasgos, significa que los usuarios tienen la libertad de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software[20]

USO INAPROPIADO: cualquier incidente que resulte de la violación de las políticas de uso aceptable de una organización por parte de un usuario autorizado[21]

VULNERABILIDAD: Debilidad de un activo o control que puede ser explotada por una o más amenazas.[22]

[20] GNU. ¿Qué es el Software Libre? [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://www.gnu.org/philosophy/free-sw.es.html#mission-statement>

[21] NIST. National Institute of Standards and Technology. Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

[22] ISO. Organización Internacional de Normalización. ISO/IEC 27000, Op. cit., p.2.

INTRODUCCIÓN

La seguridad informática ha venido tomando importancia a nivel mundial, es por ello por lo que las organizaciones empiezan a ver la necesidad de proteger los activos de información de su entidad; en este sentido, para la ISO/IEC 27001 un activo de información es: “algo que una organización valora y por lo tanto debe proteger”[23]

Para la elaboración de este proyecto de investigación se cuenta con el aval de Mazars Colombia SAS, esta es una firma internacional que se especializa en auditoria, contabilidad, consultoría, impuestos y servicios legales prestados a diferentes tipos de empresas y clientes; este trabajo nace por la necesidad urgente de la firma en monitorear sus servidores, ya que a través de su casa matriz está impartiendo instrucciones donde se deben correlacionar los eventos de seguridad de la información que reposa en los servidores de la compañía.

Es por lo anterior, que se planea implementar un gestor de eventos de seguridad en la empresa Mazars Colombia SAS, a fin de realizar el monitoreo a los servidores críticos, donde se envíen alertas al correo electrónico cuando se presenten eventos, como accesos no autorizados, creación, modificación y eliminación de la información que está alojada en los servidores.

Adicional a esto, se pretende realizar un análisis de la infraestructura de la empresa, para que de este modo se puedan clasificar los eventos y a su vez se definan las alertas. El presente proyecto estará dividido en tres fases con tareas como el análisis de la información, implementación y pruebas de funcionalidad.

[23] ISO. Organización Internacional de Normalización. ISO/IEC 27001. Sistemas de Gestión la Seguridad de la Información. ISO. Ginebra – Suiza. 2013.p.2.

1. FORMULACIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO – DESCRIPCIÓN GENERAL

Para Mazars Colombia SAS su activo más importante es la información, es por ello la importancia de protegerla; por tal motivo se hace necesario que la información que se encuentra en los servidores siempre esté disponible y sea confiable.

Actualmente el área de tecnología no tiene un monitoreo sobre estos servidores, por lo tanto, no se tiene una atención oportuna a posibles incidentes de seguridad, a partir de esto se debe emplear un tiempo considerable en la revisión de logs y en el análisis de manera detallada de los eventos hasta encontrar la causa raíz de la posible amenaza; para el área se ha vuelto inmanejable monitorear e interpretar de una manera correcta cada evento o log de los servidores de la compañía.

1.2 FORMULACIÓN – PREGUNTA

¿Cómo puede Mazars Colombia SAS monitorear los eventos de seguridad de los servidores críticos?

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Implementar un gestor de eventos de seguridad de la información (SIEM) de licenciamiento libre que permita alertar posibles incidentes de seguridad en tiempo real que afecten los servidores críticos en la empresa Mazars Colombia SAS.

2.2 OBJETIVOS ESPECÍFICOS

- Clasificar los servidores críticos de la empresa.
- Analizar y clasificar los incidentes de los servidores críticos.
- Seleccionar un gestor de eventos de licenciamiento libre.
- Instalar el SIEM en servidor proporcionado por la empresa.
- Verificar los resultados de las pruebas del software y ajustes que se requieran.

3. TIPO DE INVESTIGACIÓN

Para el presente proyecto el tipo de investigación que se adapta es la descriptiva, ya que el tema principal es la recolección de eventos de seguridad y el envió de alertas cuando los servidores críticos se vean afectados.

4. HIPÓTESIS

HI: La implementación de un Gestión de Eventos e Información de Seguridad por sus siglas en ingles *Security Information and Event Management* (SIEM), ayudará a interpretar y alertar cualquier intrusión a los servidores Windows donde se almacena información valiosa para Mazars Colombia SAS y sus clientes.

HO: La no implementación de un SIEM no ayudará a interpretar ni a alertar cualquier intrusión a los servidores Windows donde se almacena información valiosa para Mazars Colombia SAS y sus clientes.

5. VARIABLES

Dependientes
- SIEM
- Servidores

Independientes
- Eventos
- Plugins

6. MARCO TEORICO

6.1 ¿QUÉ ES UN SIEM?

Un sistema SIEM (*Security Information and Event Management*) o sistema de gestión de eventos e información de seguridad, es una herramienta utilizada para el almacenamiento centralizado y la interpretación de los datos relevantes de seguridad. Un sistema SIEM es la combinación de los sistemas SEM y SIM:

- SEM (Security Event Management) o gestión de eventos de seguridad, otorga la capacidad de monitorización en tiempo real, correlación de eventos, notificaciones y visualizaciones de la consola.

- SIM (Security Information Management) o gestión de la información de seguridad, comprende el conjunto de capacidades para el almacenamiento a largo plazo, análisis y presentación de la información de registro.

El SIEM es la principal herramienta utilizada en los centros de operaciones de seguridad o SOC (*Security Operations Center*) para la detección y respuesta a incidentes.

Las principales capacidades de un SIEM son:

- **Agregación de datos:** capacidad para administrar la información recibida de múltiples fuentes.

- **Correlación:** procesamiento de los datos recibidos para transformar dichos datos en información.

- **Alerta:** análisis de los eventos correlacionados, de manera que se generen avisos de seguridad que se envían a un administrador.

- **Cuadros de mando:** un SIEM posee las herramientas necesarias para transformar la información en tablas y gráficas.

- **Cumplimiento:** gracias a un SIEM se puede automatizar la recopilación de la información necesaria para la elaboración de informes sobre normativas existentes.

- **Retención:** un SIEM posee la capacidad de almacenamiento de datos a largo plazo, una característica que es vital para un correcto desempeño de funciones de análisis forense.

- **Redundancia:** para evitar la pérdida de datos, la base de datos de un SIEM suele estar redundada.

- **Escalabilidad:** un SIEM puede ser configurado jerárquicamente para aumentar o disminuir, en función de las necesidades del momento.

Ventajas del despliegue de un SIEM. El despliegue de un SIEM va a aportar una serie de ventajas a nivel de seguridad:

- **Detección temprana de un incidente**: gracias al análisis en tiempo real, el uso de un SIEM permite detectar un incidente que esté ocurriendo en la red, permitiendo incluso llevar a cabo las acciones necesarias para bloquear dicho incidente antes de que ocasione daños reales a la producción.

- **Análisis forense**: otro punto a favor de un SIEM es que, gracias a su capacidad para almacenar y poder consultar eventos de seguridad antiguos, facilita la tarea de análisis forense en caso de querer identificar cómo se produjo un incidente.

- **Centralización de la información**: gracias a la recopilación de eventos de los equipos de red y otros elementos de seguridad en un SIEM, éste permite una gestión centralizada de toda esa información recogida.

- **Ahorro de recursos:** al realizarse la recopilación de información de manera centralizada y automática, se consigue un ahorro significativo en cuanto a recursos.

- **Identificación de anomalías:** gracias a que las redes industriales son comúnmente estables, un punto a favor a la hora de desplegar un SIEM es que nos va a permitir identificar fácilmente, tras un periodo de aprendizaje, anomalías en el comportamiento de los equipos, pudiendo detectar problemas en el funcionamiento o incluso un incidente.

6.2 MANEJO DE INCIDENTES

El proceso de respuesta a incidentes tiene varias fases. La fase inicial implica establecer y capacitar a un equipo de respuesta a incidentes y adquirir las herramientas y los recursos necesarios. Durante la preparación y la organización también intenta limitar el número de incidentes que ocurrirán mediante la selección e implementación de un conjunto de controles basados en los resultados de las evaluaciones de riesgos. Sin embargo, el riesgo residual inevitablemente persistirá después de que se implementen los controles; por lo tanto, la detección de brechas de seguridad es necesaria para alertar a la organización cada vez que ocurren incidentes; en ese sentido, de acuerdo con la gravedad del incidente, la organización puede mitigar el impacto de éste conteniéndolo y finalmente recuperándose de él. Durante esta fase, la actividad suele volver a la detección y el análisis, por ejemplo, para ver si otros hosts están infectados por malware mientras se erradica un incidente de malware. Una vez que el incidente se maneja adecuadamente, la organización emite un informe que detalla la causa y el costo

del incidente y los pasos que la organización debe tomar para prevenir los futuros[24]

Esta sección describe las principales fases del proceso de respuesta a incidentes: preparación, detección y análisis.

6.2.1 Preparación. Las metodologías de respuesta a incidentes generalmente enfatizan la preparación, no solo estableciendo una capacidad de respuesta a incidentes para que la organización esté lista para responder a éstos, sino también previniéndolos al garantizar que los sistemas, redes y aplicaciones sean lo suficientemente seguros.[25]

6.2.1.1 Preparación para manejar incidentes. Las listas que se presentan a continuación proporcionan ejemplos de herramientas y recursos disponibles que pueden ser valiosos durante el manejo de incidentes. Estas listas están destinadas a ser un punto de partida para las discusiones sobre qué herramientas y recursos necesitan los "administradores de incidentes" de una organización.

Lista de recursos para el análisis de incidentes:

- Listas de puertos, incluidos los puertos de uso común y los puertos de caballo de Troya.

- Documentación para sistemas operativos, aplicaciones, protocolos y productos antivirus y de detección de intrusos.

- Diagramas de red y listas de activos críticos, como servidores de bases de datos.

- Línea base actual de la actividad esperada de la red, el sistema y las aplicaciones.

- Hashes criptográficos de archivos críticos para acelerar el análisis, la verificación y la erradicación de incidentes.[26]

6.2.1.2 Prevención de incidentes. Mantener el número de incidentes razonablemente bajo es muy importante para proteger los procesos comerciales de la organización. Si los controles de seguridad son insuficientes pueden ocurrir mayores volúmenes de incidentes, abrumadores al equipo de "respuesta a incidentes". Esto puede llevar a respuestas lentas e incompletas que se traducen en un mayor impacto comercial negativo (por ejemplo, daños más extensos,

[24] NIST. National Institute of Standards and Technology. Computer Security Incident Handling Guide, Op. cit., p.2.
[25] Ibid., p.2.
[26] Ibid., p.2.

períodos de servicio más prolongados y falta de disponibilidad de datos).[27]

6.2.2 Detección y análisis de incidentes. Los incidentes pueden ocurrir de innumerables formas, por lo que no es factible desarrollar instrucciones paso a paso para manejar cada uno de ellos. Las organizaciones deben estar generalmente preparadas para manejar cualquiera de ellos, pero deben enfocarse en estar preparadas para manejar los que utilizan vectores de ataque comunes. Los diferentes tipos de incidentes merecen estrategias de respuesta.

Los vectores de ataque que se enumeran a continuación no están destinados a proporcionar una clasificación definitiva de los incidentes; más bien, simplemente enumeran los métodos comunes de ataque que pueden usarse como base para definir procedimientos de manejo más específicos.

- **Medios externos/extraíbles:** un ataque ejecutado desde un medio extraíble o un dispositivo periférico, por ejemplo, un código malicioso que se propaga a un sistema desde una unidad flash USB infectada.

- **Desgaste:** un ataque que emplea métodos de fuerza bruta para comprometer, degradar o destruir sistemas, redes o servicios (por ejemplo, un DDoS destinado a impedir o denegar el acceso a un servicio o aplicación; un ataque de fuerza bruta contra un mecanismo de autenticación, como contraseñas, CAPTCHAS o firmas digitales).

- **Web:** un ataque ejecutado desde un sitio web o una aplicación basada en la web; por ejemplo, un ataque de secuencias de comandos entre sitios que se utiliza para robar credenciales o una redirección a un sitio que aprovecha una vulnerabilidad del navegador e instala malware.

- **Correo electrónico:** un ataque ejecutado a través de un mensaje de correo electrónico o un archivo adjunto; por ejemplo, código de explotación disfrazado como un documento adjunto o un enlace a un sitio web malicioso en el cuerpo de un mensaje de correo electrónico.

- **Suplantación de identidad:** un ataque que implica la sustitución de algo benigno por algo malicioso. Por ejemplo, suplantación de identidad, ataques de intermediario, puntos de acceso inalámbricos no autorizados e inyección de SQLen donde todos los ataques implican suplantación de identidad.

- **Uso inapropiado:** cualquier incidente que resulte de la violación del uso aceptable de una organización, políticas de un usuario autorizado, excluyendo las categorías anteriores; por ejemplo, un usuario instala el uso compartido de archivos

[27] Ibid., p.2.

software que conduce a la pérdida de datos sensibles; o un usuario realiza actividades ilegales en un sistema.

- **Pérdida o robo de equipo:** la pérdida o robo de un dispositivo o medio informático utilizado por la organización como una computadora portátil, un teléfono inteligente o un token de autenticación.[28]

6.2.2.1 Signos de un incidente. Los signos de un incidente se dividen en dos categorías: precursores e indicadores. Un precursor es una señal de que un incidente puede ocurrir en el futuro y un indicador es una señal de que un incidente puede haber ocurrido o puede estar ocurriendo ahora.

La mayoría de los ataques no tienen precursores identificables o detectables desde la perspectiva del objetivo. Si se detectan precursores, la organización puede tener la oportunidad de prevenir el incidente modificando su postura de seguridad para salvar a un objetivo de un ataque. Como mínimo, la organización podría monitorear la actividad involucrando al objetivo más de cerca.

Ejemplos de precursores son:

- Entradas de registro del servidor web que muestran el uso de un escáner de vulnerabilidades.

- Un anuncio de un nuevo exploit que apunta a una vulnerabilidad del servidor de correo de la organización.

- Una amenaza de un grupo que indica que el grupo atacará a la organización.

Tipos de indicadores:

- Un sensor de detección de intrusiones en la red alerta cuando se produce un intento de desbordamiento de búfer en una base de datos servidor.

- El software antivirus alerta cuando detecta que un host está infectado con malware.

- Un administrador del sistema ve un nombre de archivo con caracteres inusuales.

- Un host registra un cambio de configuración de auditoría en su registro.

- Una aplicación registra varios intentos fallidos de inicio de sesión desde un sistema remoto desconocido.

[28] Ibid., p.2.

- Un administrador de correo electrónico ve una gran cantidad de correos electrónicos devueltos con contenido sospechoso.

- Un administrador de red nota una desviación inusual de los flujos de tráfico de red típicos.[29]

6.2.3 Análisis de incidentes. La detección y el análisis de incidentes serían fáciles si se garantizara la precisión de todos los precursores o indicadores; sin embargo, este no es el caso. Por ejemplo, los indicadores proporcionados por el usuario, como una queja de un servidor que no está disponible suelen ser incorrectos. Los sistemas de detección de intrusos pueden producir indicadores incorrectos de falsos positivos. Estos ejemplos demuestran que dificulta la detección y el análisis de incidentes: idealmente, cada indicador debería evaluarse para determinar si es legítimo. Para empeorar las cosas, el número total de indicadores puede ser de miles o millones al día. Encontrar los incidentes de seguridad reales que ocurrieron entre todos los indicadores puede ser una tarea abrumadora. [30]

A continuación, se mencionan algunas recomendaciones para hacer que el análisis de incidentes sea más fácil y efectivo

- **Perfiles de redes y sistemas:** la elaboración de perfiles mide las características de la actividad esperada para que los cambios en él se pueden identificar más fácilmente. Algunos ejemplos de creación de perfiles son la ejecución de la comprobación de integridad de archivos software en hosts para derivar sumas de verificación para archivos críticos y monitorear el uso del ancho de banda de la red para que determine cuáles son los niveles de uso promedio y pico en varios días y horarios. En la práctica, es difícil detectar incidentes con precisión utilizando la mayoría de las técnicas de elaboración de perfiles, es por ello que las organizaciones deben usar la elaboración de perfiles como una de las diversas técnicas de detección y análisis.

- **Creación de una política de retención de registros:** la información relativa a un incidente puede registrarse en varios lugares, como firewall, IDPS (*Intrusion Detection and Prevention Systems*) y registros de aplicaciones. Crear e implementar una política de retención de registros que especifica cuánto tiempo se deben mantener los datos de registro puede ser extremadamente útil en el análisis porque las entradas de registro pueden mostrar actividad de reconocimiento o instancias anteriores de ataques similares. Otra razón para retener registros es que los incidentes no se pueden descubrir hasta días, semanas o incluso meses después. La cantidad de tiempo para mantener los datos de registro depende de varios factores, incluidos los datos de la organización políticas de retención y el volumen de datos.

[29] Ibid., p.2.
[30] Ibid., p.2.

- **Realizar correlación de eventos:** la evidencia de un incidente puede capturarse en varios registros, cada uno de los cuales contiene diferentes tipos de datos: un registro de firewall puede tener la dirección IP de origen que se utilizó, mientras que un registro de aplicación puede contener un nombre de usuario. Un IDPS (*Intrusion Detection and Prevention Systems)* de la red puede detectar que se lanzó un ataque contra un host en particular, pero es posible que no sepa si el ataque fue exitoso. Es posible que el analista deba examinar los registros del host para determinar esa información. La correlación de eventos entre múltiples fuentes de indicadores puede ser invaluable para validar si ocurrió un incidente en particular.

- **Mantener todos los relojes del host sincronizados:** protocolo de tiempo de red NTP (*Network Time Protocol*) sincroniza relojes entre hosts. La correlación de eventos será más complicada si los dispositivos que informan los eventos tienen configuraciones de reloj inconsistentes.

- **Filtrar los datos:** sencillamente, no hay tiempo suficiente para revisar y analizar todos los indicadores; como mínimo, hay que investigar la actividad más sospechosa. Una estrategia eficaz es filtrar las categorías de indicadores que tienden a ser insignificantes. Otra estrategia de filtrado consiste en mostrar sólo las categorías de indicadores que son de mayor importancia; sin embargo, este enfoque conlleva un riesgo sustancial porque la nueva actividad maliciosa puede no caer en una de las categorías de indicadores elegidas.[31]

[31] Ibid., p.2.

7. MARCO DE REFERENCIA

Mazars es una firma integrada globalmente, especializada en servicios de auditoría, contabilidad, asesoría, impuestos y legal. Operando en 91 países y territorios en todo el mundo, recurre a la experiencia de 40.400 profesionales - 24.400 en la sociedad integrada de Mazars y 16.000 a través de Mazars North America Alliance - para ayudar a clientes de todos los tamaños en cada etapa de su desarrollo.[32]

En la actualidad Mazars Colombia tiene presencia en Bogotá, Cali, Medellín, Cartagena, Barranquilla, Cúcuta, Ibagué, ya que sus clientes locales están presentes en estas ciudades; desde luego Mazars Colombia tiene clientes internacionales que tienen presencia en Colombia.

Mazars Colombia SAS pretende establecerse como una compañía líder en servicios de auditoría, contabilidad, asesoría, impuestos y legal; para lograr esto Mazars Colombia está en la búsqueda de fortalecer la seguridad de sus sistemas informáticos monitoreando, previniendo y neutralizando cualquier tipo de amenaza y/o vulnerabilidades externas y/o internas que puedan atentar contra los tres pilares de la seguridad informática (integridad, confidencialidad, disponibilidad).

Uno de los propósitos fundamentales para la compañía es certificarse en la norma ISO 27001, ya que para participar en varias licitaciones nacionales se solicita tener alguna norma de la ISO como la ISO 27000 o la norma ISO 9001, además se elige la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) ya que con este sistema también pretende mantener seguro los datos de los clientes que tiene la compañía. Para que Mazars Colombia SAS logre certificarse es necesario cumplir cada control de la norma ISO 27001 apoyados en el anexo A de la misma y la ISO 27002.

En este sentido, el presente documento ayudará a dar cumplimiento al control 12.4.1 - registro de eventos de la norma ISO 27002.

A nivel tecnológico Mazars Colombia cuenta un cuarto de comunicaciones en las oficinas principales en la ciudad de Bogotá, este cuarto cuenta con cuatro servidores físicos y cuatro servidores virtuales, cada servidor tiene habilitado la auditoria de sus carpetas donde se encuentra alojada la información y programas que se utilizan a nivel general. Los eventos que genera la auditoria en estas carpetas no son revisados con frecuencia por el equipo de tecnología de la compañía. Es importante monitorear estos eventos ya que pueden revelar un posible incidente de seguridad y a su vez este incidente puede llegar a generar la indisponibilidad de los servicios e información que se prestan a los clientes. A continuación, se ampliará un poco más la información.

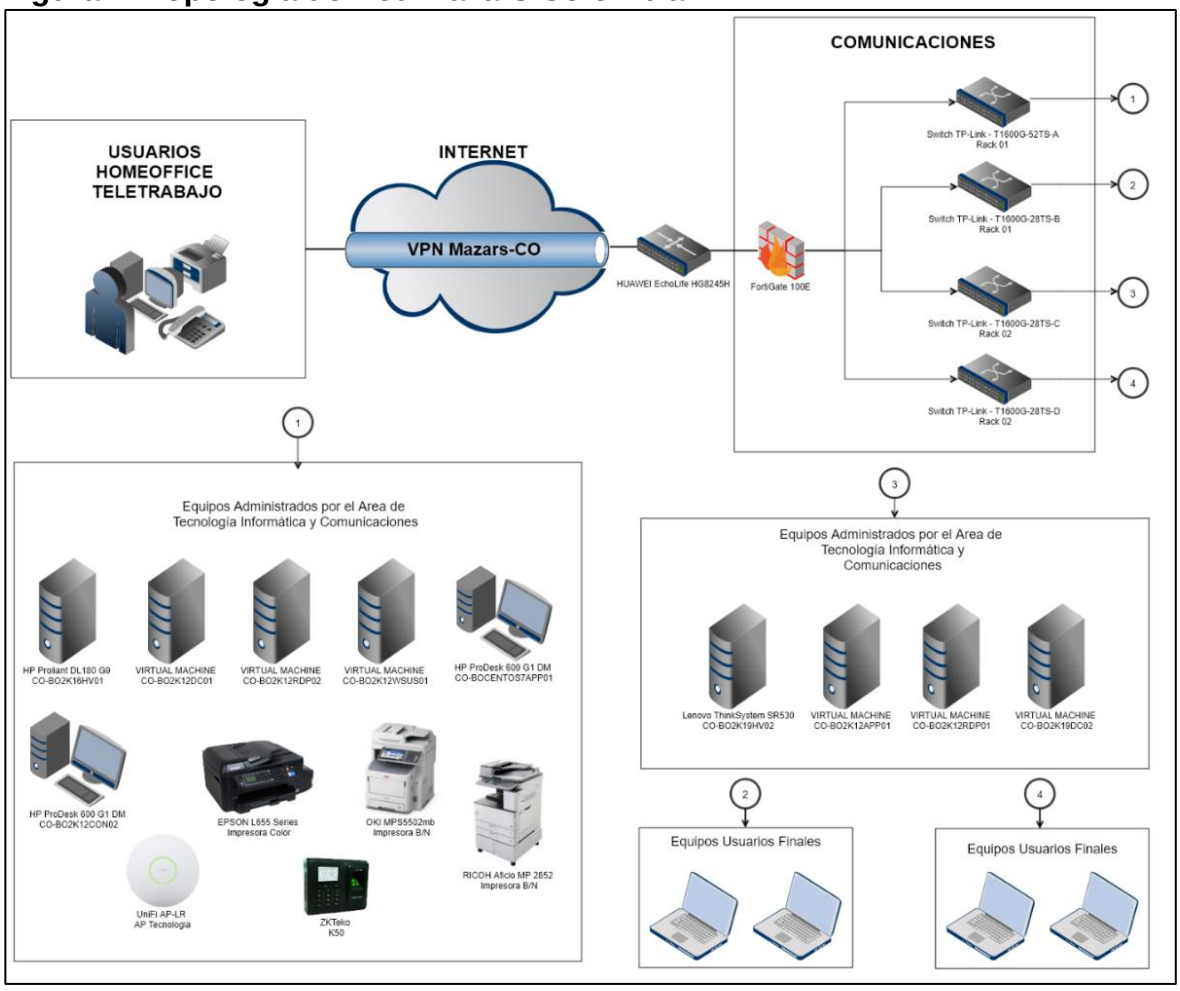
[32] MAZARS. Mazars en Colombia. [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://www.mazars.com.co/Pagina-inicial/Acerca-de-nosotros/Mazars-en-Colombia2>

7.1 DOCUMENTACIÓN DE INFRAESTRUCTURA

En este apartado se da a conocer la infraestructura con la que cuenta Mazars Colombia SAS.

7.1.1 Topología de red. Mazars Colombia SAS comparte el mapa de su infraestructura, como se evidencia la figura 1

Figura 1. Topología de Red Mazars Colombia



Fuente: MAZARS. Mazars en Colombia. [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://www.mazars.com.co/Pagina-inicial/Acerca-de-nosotros/Mazars-en-Colombia2>

7.1.2 Aplicaciones/servicios del negocio. Actualmente Mazars Colombia SAS cuenta con un inventario de aplicaciones y servicios prestado por el área de tecnología para el apoyo de sus actividades diarias:

- **Servicio de directorio activo (CO-BO2K12DC01 – CO-BO2K12DC02):** método para almacenar datos de directorio y hacer que estos permanezcan

disponibles para los usuarios y administradores de la red. Almacena información acerca de las cuentas de usuario, como nombres, contraseñas, números de teléfono, etc., y permite que otros usuarios autorizados de la misma red tengan acceso a dicha información[33], A través de este servicio se realiza el login a las aplicaciones de Mazars Grupo.

- **Servicio de escritorio remoto (CO-BO2K12RDP01 – CO-BO2K12RDP02):** este servicio es usado por los Usuarios de Mazars Colombia como usuarios de los clientes que para sus labores necesitan conexión hacia el software contable Helisa NIIF y el software de nómina Recurso Humano 4.

- **Servicio de impresión (CO-BO2K12APP01):** con este servicio, se comparten recursos de impresión en toda la red (Mazars-CO), de modo que clientes/Usuarios de una gran variedad de equipos y sistemas operativos podrán enviar trabajos de impresión a impresoras conectadas localmente a un servidor de impresión.

- **Servidor de archivos (CO-BO2K16HV01 – CO-BO2K19HV02):** en este servicio todos los colaboradores (auditoría, contabilidad, asesoría, impuestos y legal) alojan todos los papeles de trabajo de los clientes. Cada usuario solo tiene acceso a las carpetas que corresponden al área al que pertenece a menos que se solicite el ingreso a otras carpetas.

- **Helisa NIIF (CO-BO2K12CON02):** software contable donde se lleva la contabilidad de cada uno de los clientes y la contabilidad interna de la compañía[34] ; este sistema contable maneja una base interna para el manejo de los usuarios y contraseñas.

- **Recurso Humano 4 (CO-BO2K12CON02):** software donde se lleva la nómina de cada uno de los clientes[35]; este sistema contable cuenta con una base interna para el manejo de los usuarios y contraseñas

- **Microsoft 365 Empresa Estándar (Servicio Cloud Mensual):** es un servicio de suscripción que le permite ejecutar su organización en la nube mientras Microsoft se encarga de usted, de administrar dispositivos, de protegerse contra amenazas del mundo real y de ofrecer a su organización lo último en software empresarial[36];

---

[33] MICROSOFT. Introducción a Active Directory Domain Services. [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>

[34] HELISA. NIIF. [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://helisa.com/productos/administrador/>

[35] HELISA. Nomina. [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://helisa.com/productos/nomina/>

[36] MICROSOFT 365. Business Premium. [en línea]. El sitio [citado 29, abril, 2021]. Disponible en Internet: < URL: https://support.microsoft.com/es-es/office/%C2%BFqu%C3%A9-es-microsoft-365-business-premium-901e2522-c2cf-4b8c-894e-f482cda3347a>

los usuarios y contraseñas de esta plataforma se manejan con una conexión hacia el directorio activo local.

- **Acronis BaaS (Servicio Cloud Mensual):** servicio de copia de seguridad como servicio para pymes[37]; en este servicio solo se maneja un único usuario, la gestión del servicio es apoyado con el proveedor y el administrador de la infraestructura de la compañía.

- **GLPI (CO-BOCENTOS7APP01):** GLPI es una herramienta que ayuda a la compañía a gestionar el inventario de los equipos, también se utiliza para gestión de casos (ticket) ofrece a los usuarios un servicio de declaración de incidencias y requerimientos.[38]

- **KIMAI (CO-BOCENTOS7APP01):** Aplicación web gratuita y de fuente abierta para medir el tiempo invertido en las diferentes tareas de un proyecto.[39]

7.1.3 Estado actual de la organización frente a la seguridad informática. La firma cuenta con las siguientes herramientas de seguridad informática que ayudan a proteger la información de los clientes y la propia:

- **Política de seguridad de la información:** es la declaración general que Mazars Colombia SAS tiene con respecto a la protección de los activos de información.

- **Firewall Fortinet 100E:** hardware de seguridad perimetral que protege el acceso no autorizado a la red[40], este dispositivo es dirigido por el administrador de la infraestructura de Mazars Colombia SAS.

- **Kaspersky Endpoint Security Cloud Plus:** software de antivirus que proporciona seguridad en diferentes capas a los equipos y servidores de la compañía

- **Kaspersky Security for Microsoft Office 365:** servicio contratado por la firma que detiene la propagación de software malicioso, phishing, spam, ransomware a través de los mensajes de correo electrónico.[41]

---

[37] ACRONIS BAAS. Copia de seguridad en el cloud fácil de gestionar, fiable y sin infraestructura para pymes. [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://www.acronis.com/es-es/business/backup/cloud-deployment/>

[38] GLPI. Maneja la TI – Con el Poder de la Libertad. [en línea]. El sitio [citado 8, noviembre, 2020]. Disponible en Internet: < URL: https://glpi-project.org/es/>

[39] KIMAI. Time-Tracker. [en línea]. El sitio [citado 8, noviembre, 2020]. Disponible en Internet: < URL: https://www.kimai.org/about/>

[40] FORTINET. Recursos e información. [en línea]. El sitio [citado 2, noviembre, 2021]. Disponible en Internet: < URL: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_100E_Series.pdf>

[41] KASPERSKY. Security for Microsoft office 365. [en línea]. El sitio [citado 2, noviembre, 2021].

- **Nagios Core:** aplicación web que sirve como programador de eventos básico, donde se pueden planear diferentes alertas que validan el uso del procesador, memoria RAM, procesos del sistema entre otros[42].

- La compañía realiza la entrega de una matriz de riesgos (Anexo A) para que a través de esta se realice el análisis de los servidores críticos de la firma. Este matriz se encuentra como anexo del presente documento.

Disponible en Internet: < URL:https://latam.kaspersky.com/small-to-medium-business-security/microsoft-office-365-security

[42] NAGIOS CORE. [en línea]. El sitio [citado 2, noviembre, 2021]. Disponible en Internet: < URL: https://www.nagios.org/projects/nagios-core/>

8. DESARROLLO

8.1 CLASIFICACIÓN DE SERVIDORES CRÍTICOS

Según la matriz del Anexo B se consideran servidores críticos quienes en la recomendación de tratamiento de la matriz de riegos tienen como ítem SIEM.

8.2 ANÁLISIS Y CLASIFICACIÓN DE INCIDENTES

Lista para el análisis de incidentes:

- **Elaboración de perfiles de sistemas** (Anexo B): la elaboración de perfiles mide las características de la actividad esperada para que los cambios en él se pueden identificar más fácilmente. Ejemplos de creación de perfiles son la ejecución de la comprobación de integridad de archivos software en hosts para derivar sumas de verificación para archivos críticos y monitorear el uso del ancho de banda de la red para determinar cuáles son los niveles de uso promedio y pico en varios días y horarios. En la práctica, es difícil de detectar incidentes con precisión utilizando la mayoría de las técnicas de elaboración de perfiles; las organizaciones deben usar la elaboración de perfiles como una de las diversas técnicas de detección y análisis[43].

- **Mantener todos los relojes de los hosts sincronizados NTP**: según el control 12.4.4 de la ISO27002 refiere que los relojes de los servidores dentro de una red deben estar sincronizados con una única fuente; los servidores críticos de la compañía se sincronizan a través de un software SymmTime sugerido por el Instituto Nacional de Meteorología de Colombia[44], ya que éste regula la hora del territorio colombiano.

- **Realizar correlación de eventos**: la evidencia de un incidente se puede capturar en varios registros que cada contienen diferentes tipos de datos: un registro de firewall puede tener la dirección IP de origen que se utilizó, mientras que un registro de la aplicación puede contener un nombre de usuario. Un IDPS de la red puede detectar que se lanzó un ataque contra un host en particular, pero es posible que no sepa si el ataque fue exitoso. El analista puede necesitar examinar los registros del host para determinar esa información. Correlacionar eventos entre múltiples indicadores y las fuentes pueden ser invaluables para validar si ocurrió un incidente

[43] NIST. National Institute of Standards and Technology. Perfiles de sistema. [en línea]. El sitio [citado 2, noviembre, 2021]. Disponible en Internet: < URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

[44] INM. Instituto Nacional de Metrología de Colombia. Configuración para conexión de la hora legal colombiana. [en línea]. El sitio [citado 8, noviembre, 2020]. Disponible en Internet: < URL: http://www.inm.gov.co/nueva/wp-content/uploads/2019/10/InstructivoHoraLegalColombiaMayo2017.pdf>

en particular[45].

- **Recursos para el análisis de incidentes** (Anexo B): Documentación de sistema operativos, protocolos y productos antivirus de protección de intrusos[46].

- **Diagramas de red y listas de activos críticos** ver Anexo B y figura 2

8.3 CLASIFICACIÓN DE INCIDENTES

En el cuadro 1 se realiza un desglose de la Matriz de riesgo de la compañía, esto con el fin de saber las vulnerabilidades y amenazas que tienen los servidores.

Cuadro 1. Desglose de la Matriz de Riesgo (consultar Anexo B)

ID de Riesgo	Vulnerabilidad existente	Amenaza	Descripción del escenario	Probabilidad (A/M/B)	Impacto (A/M/B)	Prioridad (1-9)
HV01-01	Control de acceso inadecuado	Uso de software por usuarios no Autorizados	Ejecución de aplicaciones no autorizadas en los servidores de producción	Media	Media	5
HV01-04	Conexión de equipo no autorizado	Uso de Instalaciones de Red en Forma no Autorizada	Conexión a interfaces de red no autorizadas en los servidores físicos	Alta	Media	2
HV01-07	Control de acceso inadecuado	Ataque Malicioso - Manipulación de Equipo Informático	Manipulación del equipo para ingresar a datos sensibles de la organización	Media	Media	5
DC01-02	Administración de configuración inadecuada	Uso de Software por Usuarios no Autorizados	Ingreso no autorizado al servidor virtual	Media	Media	5
WSUS01-02	Administración de configuración inadecuada	Uso de Software por Usuarios no Autorizados	Ingreso no autorizado al servidor virtual	Media	Media	5
HV02-01	Control de acceso inadecuado	Uso de software por usuarios no Autorizados	Ejecución de aplicaciones no autorizadas en los servidores de producción	Media	Media	5
HV02-04	Conexión de equipo no autorizado	Uso de Instalaciones de Red en Forma no Autorizada	Conexión a interfaces de red no autorizadas en los servidores físicos	Alta	Media	2

[45] NIST. National Institute of Standards and Technology. Computer Security Incident, Op., cit, p.31.
[46] Ibid., p.32.

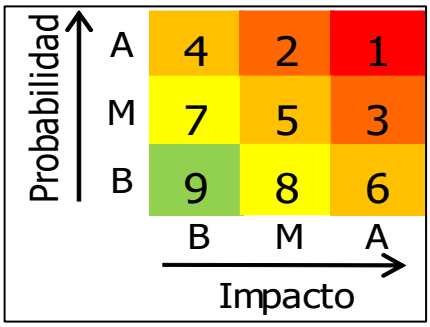
Cuadro 1 (continuación)

ID de Riesgo	Vulnerabilidad existente	Amenaza	Descripción del escenario	Probabilidad (A/M/B)	Impacto (A/M/B)	Prioridad (1-9)
HV02-07	Control de acceso inadecuado	Ataque Malicioso - Manipulación de Equipo Informático	manipulación del equipo para ingresar a datos sensibles de la organización	Media	Media	5
DC02-02	Administración de configuración inadecuada	Uso de Software por Usuarios no Autorizados	Ingreso no autorizado al servidor virtual	Media	Media	5
RDP01-02	Administración de configuración inadecuada	Uso de Software por Usuarios no Autorizados	Ingreso no autorizado al servidor de escritorio remoto	Media	Media	5
APP01-02	Administración de configuración inadecuada	Uso de Software por Usuarios no Autorizados	Ingreso no autorizado al servidor virtual de Wifi (Ubiquiti)	Media	Media	5
CON02-01	Control de acceso inadecuado	Uso de software por usuarios no Autorizados	Ejecución de aplicaciones no autorizadas en los servidores de producción	Media	Media	5
CON02-04	Conexión de equipo no autorizado	Uso de Instalaciones de Red en Forma no Autorizada	Conexión a interfaces de red no autorizadas en los servidores físicos	Alta	Media	2
CON02-07	Control de acceso inadecuado	Ataque Malicioso - Manipulación de Equipo Informático	Manipulación del equipo para ingresar a datos sensibles de la organización	Media	Media	5
RDP02-02	Administración de configuración inadecuada	Uso de Software por Usuarios no Autorizados	Ingreso no autorizado al servidor de escritorio remoto	Media	Media	5

Fuente: Elaboración propia de acuerdo con datos de MAZARS. Mazars en Colombia. Matriz de riesgos. Bogotá, 2021

8.3.1 Criterios de evaluación. En la figura 2, se presentan los criterios de evaluación de la matriz de riegos de la compañía Mazars Colombia.

Figura 2. Criterios de evaluación



Fuente: Elaboración propia de acuerdo con datos de MAZARS. Mazars en Colombia. Matriz de riesgos. Bogotá, 2021

En el cuadro 2 y 3, se mostrará los criterios de evaluación de la figura 2.

Cuadro 2. Criterios de evaluación

Impacto	
A	Muy Alto. La explotación de la vulnerabilidad puede resultar en: (1) Altos costos por pérdida de activos o recursos tangibles (2) Violencia significativa, daño o impedimento del logro de los objetivos de la organización, reputación o intereses (3) Pérdida de vidas humanas o daños serios a la salud.
M	Medio. Pérdida financiera significativa, amenaza con pérdida de imagen de la Organización.
B	Menor. La explotación de la vulnerabilidad puede resultar en: (1) Daños menores a los activos o recursos tangibles o (2) afectación mínima de la misión, objetivos o intereses de la organización.

Probabilidad	
A	Muy Frecuente: Sucede casi siempre cuando falla el control
M	Moderado: Puede suceder y ya ha ocurrido ocasionalmente
B	Rara vez: Concebible solo en condiciones extremas

Fuente: Elaboración propia de acuerdo con datos de MAZARS. Mazars en Colombia. Matriz de riesgos. Bogotá, 2021

De acuerdo con la matriz de riesgo de la compañía Mazars Colombia se puede concluir que los servidores críticos son los siguientes:

- CO-BO2K16HV01
- CO-BO2K12DC01
- CO-BO2K12WSUS01
- CO-BO2K19HV02
- CO-BO2K12DC02

- CO-BO2K12APP01
- CO-BO2K12CON01
- CO-BO2K12RDP01

En el Anexo B están los perfiles de cada uno de los servidores mencionados anteriormente.

Para la clasificación de los incidentes es necesario realizar el análisis de la matriz de riesgo de la compañía donde se pueden evidenciar las amenazas; según la ISO-27035 en su Anexo C donde presenta el cuadro de categorías de incidentes de la seguridad de la información y de acuerdo con las amenazas es pertinente hacer la clasificación evidenciada en el cuadro 3

Cuadro 3. Categoría de Incidentes

Vulnerabilidad existente	Amenaza	descripción del escenario	Categoría
Administración de configuración inadecuada	Uso de Software por Usuarios no Autorizados	Ingreso no autorizado al servidor virtual	Incidente de ataque técnico/Incidente de violación de reglas
Conexión de equipo no autorizado	Uso de Instalaciones de Red en Forma no Autorizada	Conexión a interfaces de red no autorizadas en los servidores físicos	Incidente de ataque técnico
Control de acceso inadecuado	Uso de software por usuarios no Autorizados	Ejecución de aplicaciones no autorizadas en los servidores de producción	Incidente de Malware/Incidente de ataque técnico
Control de acceso inadecuado	Ataque Malicioso - Manipulación de Equipo Informático	Manipulación del equipo para ingresar a datos sensibles de la organización	Incidente de Malware

Fuente: Los autores

Incidente de ataque técnico: la pérdida de seguridad de la información es causada por el ataque de sistemas de información, a través de redes u otros medios técnicos, ya sea mediante el aprovechamiento de las vulnerabilidades de los sistemas de información en cuanto a configuraciones, protocolos o programas, o por la fuerza, lo que da como resultado un estado anormal de los sistemas de información, o daño potencial a las operaciones precedentes del sistema.

Incidente de Malware: la pérdida de seguridad de la información es causada por programas maliciosos creados y divulgados en forma deliberada. Un programa malicioso se inserta en los sistemas de información para afectar la confidencialidad, la integridad o disponibilidad de los datos, las aplicaciones o sistemas operativos, y/o afectar la operación normal de los sistemas de información.

Incidente de violación de reglas: la pérdida de la seguridad de la información es causada por violación de las reglas en forma accidental o deliberada[47]**.**

8.4 EVENTOS DE WINDOWS SERVER

A través del visor de eventos se puede realizar la recolección y consolidación de los eventos de los servidores críticos de la compañía.

Los eventos se colocan en diferentes categorías, cada una de las cuales está relacionada con un registro que Windows mantiene en los eventos relacionados con esa categoría. Si bien hay muchas categorías, la gran cantidad de solución de problemas que podría querer hacer se relaciona con tres de ellas:

Aplicación: el registro de la aplicación registra eventos relacionados con los componentes del sistema de Windows, como los controladores y el built-in elementos de la interfaz.

Sistema: el registro del sistema registra eventos relacionados con programas instalados en el sistema.

Seguridad: cuando el registro de seguridad está habilitado (está desactivado por defecto en Windows), este registro registra eventos relacionado con la seguridad, como intentos de inicio de sesión y acceso a recursos.

Microsoft en su página[48] tiene todos los ID de eventos que genera sus sistemas operativos, de acuerdo con este cuadro y el análisis realizado de la categoría de incidentes se puede dar mayor relevancia a los siguientes eventos de los servidores, tal como se evidencia en el cuadro 4:

Cuadro 4. ID Eventos

ID. de evento de Windows actual	ID. de evento de Windows heredado	Importancia crítica potencial	Resumen del evento
4907	N/D	Media	Se cambió la configuración de auditoría del objeto
4656	560	Bajo	Se solicitó un identificador para un objeto.
4658	562	Bajo	Se cerró un identificador para un objeto.
4660	564	Bajo	Se eliminó un objeto.
4663	567	Bajo	se ha intentado obtener acceso a un objeto.

[47] ICONTEC INTERNACIONAL. Cross Border Technology, Compendio seguridad de la información, segunda edición. Bogotá: Contacto Grafico.2015, p.25.
[48] MICROSOFT. Anexo L: eventos para supervisar. [en línea]. El sitio [citado 8, noviembre, 2020]. Disponible en Internet: < URL: https://acortar.link/QEccfl>

Cuadro 4 (continuación)

ID. de evento de Windows actual	ID. de evento de Windows heredado	Importancia crítica potencia	Resumen del evento
4670	N/D	Bajo	Se cambiaron los permisos de un objeto.
4690	594	Bajo	Se intentó duplicar un identificador en un objeto.
5152	N/D	Bajo	La Plataforma de filtrado de Windows bloqueó un paquete
5156	N/D	Bajo	La Plataforma de filtrado de Windows permitió una conexión
5157	N/D	Bajo	La Plataforma de filtrado de Windows bloqueó una conexión
5447	N/D	Bajo	Se cambió un filtro de la Plataforma de filtrado de Windows.

Fuente: Los autores

8.5 SELECCIÓN DEL SIEM DE LICENCIAMIENTO LIBRE

Para la elección del SIEM de licenciamiento libre se hizo un comparativo donde se tomaron en cuenta diferentes compañías del mercado, tal como se aprecia en el cuadro 5

Cuadro 5. Comparación SIEM Libre

Software	Descripción	Características
Ossim AlienVault	Ofrece un modelo servidor-agente y sin servidor, con análisis de registros para servidores de correo, bases de datos, etc.	Descubrimiento de activos
		Evaluación de vulnerabilidad
		detección de intrusos
		Monitoreo de comportamiento
		Correlación de eventos
		Análisis de registros en tiempo real
		Configuración compleja
Sagan	Herramienta de correlación y análisis de registros en tiempo real que es compatible con consolas gráficas como Snorby y Eve Box	Ejecución de scripts en la detección de eventos
		Análisis de registros en tiempo real
		Correlación de eventos
		Alertas en tiempo real
		Uso difícil
		Configuración compleja
Splung Free	Versión gratuita de la herramienta Splunk que le permite indexar hasta 500 MB diarios para indexación de datos y alertas en tiempo real	Monitoreo en tiempo real.
		Detectar la ultimas amenazas más avanzadas.
		Mitigar el comportamiento y las transacciones fraudulentas
		Automatiza la recopilación, indexación y alerta de datos.
		indexar hasta 500 MB

Cuadro 5 (continuación)

Software	Descripción	Características
Snort	Analiza el tráfico de la red en tiempo real, pero las características lo hacen más adecuado para profesionales de TI con experiencia.	Solución gratuita de detección de intrusiones
		Análisis de tráfico de la red en tiempo real
		Análisis de registros
Mozdef	Una herramienta basada en microservicios que puede integrarse con plataformas de terceros para obtener información de seguridad sencilla	Aceptar eventos / registros de una variedad de sistemas.
		Almacenamiento de eventos / registros.
		Facilitar búsquedas.
		Facilitar la alerta.
		Facilitar la gestión de registros (archivo, restauración).
EKL Stack	Combina Elasticsearch con herramientas como Kibana, Beats y Logstash para obtener una solución SIEM más completa	Elasticsearch, es el motor de análisis y búsqueda distribuido basado en JSON.
		Kibana, es una ventana al Elastic Stack.
		Beats, engente que envía los datos desde host cliente
		Logstash, es el canal de recopilación de datos
Wazuh	Es una solución de monitoreo de seguridad gratuita, de código abierto y lista para la empresa para la detección de amenazas, monitoreo de integridad, respuesta a incidentes y cumplimiento.	Sistema de detección de intrusiones basado en host (HIDS)
		Wazuh proporciona los controles de seguridad necesarios, requeridos por estándares como PCI DSS, HIPAA, GDPR
		Wazuh se utiliza para recopilar, analizar y correlacionar datos, con la capacidad de brindar detección de amenazas, gestión de cumplimiento y capacidades de respuesta a incidentes.

Fuente: Los autores

Para escoger el SIEM libre para la compañía se realiza la evaluación según los objetivos del documento tal como se muestra en el cuadro 6

Cuadro 6. Calificación de SIEM

Preguntas de evaluación	Mozdef	Ossim AlienVault	Wazuh	Splunk
¿Software de Licenciamiento Libre?	Si	Si	Si	Si
Capacidad de Almacenamiento	Si	Si	Si	No
¿Tiene Procesamiento de logs?	Si	Si	Si	Si
Dashboard personalizables	Si	No	No	Si
¿Alerta y/o notifica posibles incidentes?	Si	Si	Si	Si
¿Se Integración con servidores Windows?	Si	Si	Si	Si

Cuadro 6 (continuación)

Preguntas de evaluación	Mozdef	Ossim AlienVault	Wazuh	Splunk
¿Tiene correlación de Eventos?	Si	Si	Si	Si
Experiencia en el mercado	2014	2003	2015	2003
Cuenta con sitio web de foros	Si	Si	Si	Si
Cuenta con comunidad para soporte	Si	Si	Si	Si
Fuente de Investigación	https://mozdef.readthedocs.io/en/latest/overview.html	https://cybersecurity.att.com/products/ossim	https://wazuh.com/	https://docs.splunk.com/Documentation/Splunk/7.2.6/Admin/MoreaboutSplunkFree

Fuente: Los autores

Según la calificación realiza el SIEM a implementar en la compañía Mazars Colombia SAS es WAZUH ya que cumple con los objetivos tratados con la compañía en este documento.

Wazuh es una plataforma gratuita y de código abierto que se utiliza para la prevención, detección y respuesta de amenazas, protege las cargas de trabajo en entornos locales, virtualizados, en contenedores y basados en la nube.

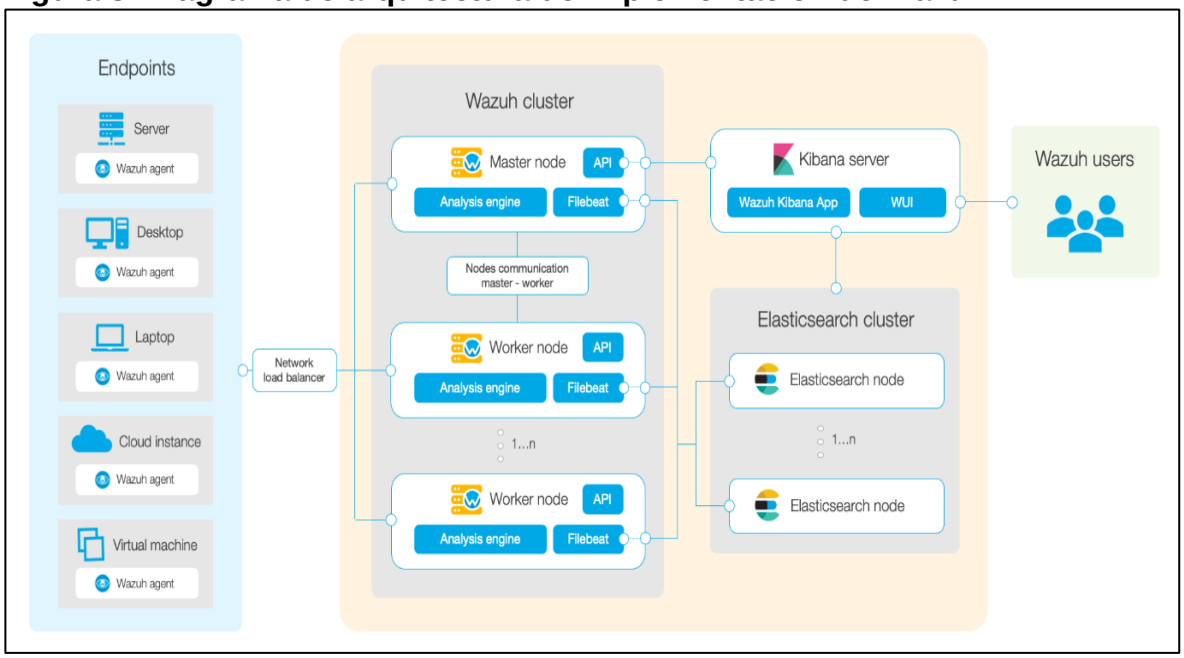
Wazuh tiene una de las comunidades de seguridad de código abierto más grandes del mundo. Se puede formar parte de él para aprender de otros usuarios, participar en discusiones, hablar con el equipo de desarrollo y contribuir al proyecto. Los siguientes recursos están fácilmente disponibles:

- Canal de Slack
- Grupo de Google
- Repositorios de GitHub[49]

La arquitectura de Wazuh se basa en agentes que se ejecutan en los puntos finales supervisados que envían datos de seguridad a un servidor central. Además, los dispositivos sin agentes (como firewalls, conmutadores, enrutadores, puntos de acceso, etc.) son compatibles y pueden enviar datos de registro de forma activa a través de Syslog, SSH o utilizando su propia API. El servidor central decodifica y analiza la información entrante y pasa los resultados a un clúster de Elasticsearch para su indexación y almacenamiento, tal como se muestra en la figura 3.

[49] WAZUH. Empezando. [en línea]. El sitio [citado 8, noviembre, 2020]. Disponible en Internet: < URL:https://documentation.wazuh.com/current/getting-started/index.html>

Figura 3. Diagrama de arquitectura de implementación de Wazuh



Fuente: WAZUH. Arquitectura. [en línea]. El sitio [citado 11, febrero, 2021]. Disponible en Internet: < URL: https://documentation.wazuh.com/current/getting-started/architecture.html>

Los requisitos mínimos para la implementación del SIEM Wazuh es de 4 GB de RAM y 2 núcleos de CPU, y los recomendados son 16 GB de RAM y 8 núcleos de CPU.[50]

8.6 INSTALACIÓN Y CONFIGURACIÓN DEL SIEM

En este apartado se verá reflejado todos los requerimientos técnicos para la instalación del SIEM.

8.6.1 Requerimientos de Hardware. Mazars Colombia brinda un equipo con las características recomendadas como 8 GB de RAM y un procesador Core i3 4130T a 2,90 Ghz con un disco duro mecánico de 1 Terabyte para la instalación del SIEM.

8.6.2 Instalación del SIEM. La instalación del SIEM se realizó bajo el sistema operativo Centos7, ya que es de licenciamiento libre, tal como se evidencia en la figura 4

[50] WAZUH. Requisitos [en línea]. El sitio [citado 11, febrero, 2021]. Disponible en Internet: < URL: https://documentation.wazuh.com/current/installation-guide/requirements.html>

Figura 4. Versión sistema operativo

```
[root@co-bocentos7siem01 ~]# cat /etc/redhat-release
CentOS Linux release 7.9.2009 (Core)
```

Fuente: Los autores

Luego de actualizar el sistema operativo, este queda listo para los siguientes pasos de la instalación del SIEM; el primero de estos es realizar la instalación de Elasticsearch como se muestra en la figura 5

Figura 5. Servicio Elasticsearch

```
[root@co-bocentos7siem01 data]# curl -XGET https://localhost:9200 -uelastic:                    -k
{
  "name" : "node-1",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "gxw_83CrRHmIVeNrVIWcFw",
  "version" : {
    "number" : "7.10.2",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "747e1cc71def077253878a59143c1f785afa92b9",
    "build_date" : "2021-01-13T00:42:12.435326Z",
    "build_snapshot" : false,
    "lucene_version" : "8.7.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
[root@co-bocentos7siem01 data]# systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: disabled)
   Active: active (running) since mar 2021-04-06 21:50:21 -05; 5 days ago
     Docs: https://www.elastic.co
 Main PID: 22522 (java)
   CGroup: /system.slice/elasticsearch.service
           ├─22522 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60 -Des.networkaddress...
           └─22711 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

abr 06 21:50:04 co-bocentos7siem01 systemd[1]: Starting Elasticsearch...
abr 06 21:50:21 co-bocentos7siem01 systemd[1]: Started Elasticsearch.
```

Fuente: Los autores

Inmediatamente que el servicio de Elasticsearch este activo e iniciado, a continuación, se procede con la instalación de Logstash como se visualiza en la figura 6

Figura 6. Servicio Logstash

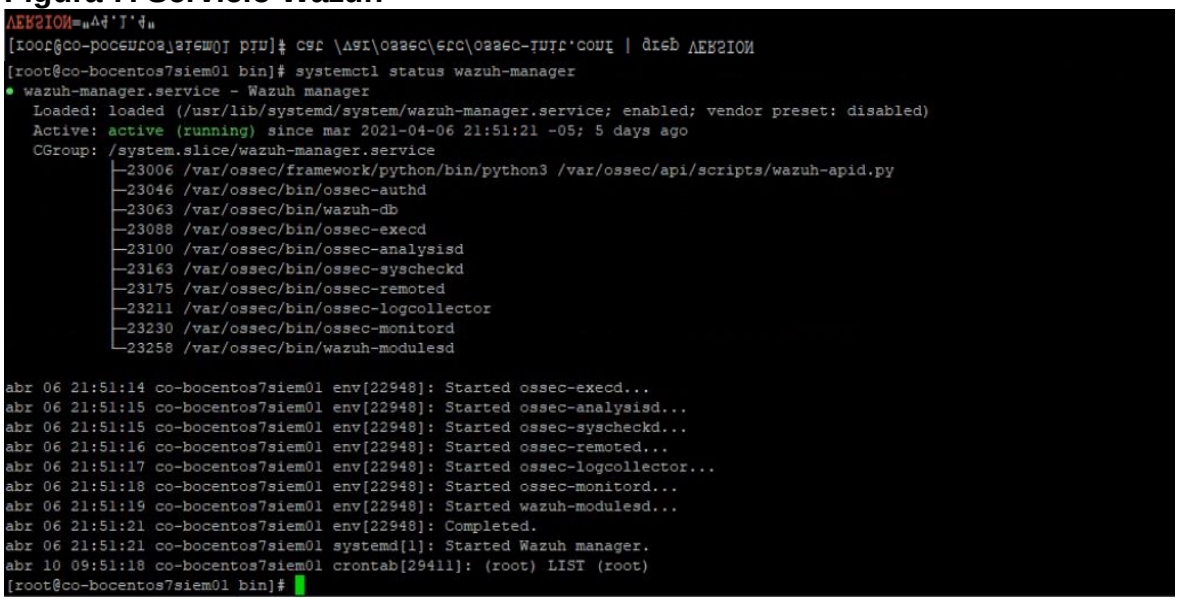
```
[root@co-bocentos7siem01 bin]# ./logstash --version
Using bundled JDK: /usr/share/logstash/jdk
logstash 7.11.0
[root@co-bocentos7siem01 bin]# systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: disabled)
   Active: active (running) since mar 2021-04-06 21:44:55 -05; 5 days ago
 Main PID: 22051 (java)
   CGroup: /system.slice/logstash.service
           └─22051 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFracti...

abr 12 19:25:43 co-bocentos7siem01 logstash[22051]: [2021-04-12T19:25:43,673][WARN ][logstash.outputs.elasticsearch][main]...
abr 12 19:25:48 co-bocentos7siem01 logstash[22051]: [2021-04-12T19:25:48,676][WARN ][logstash.outputs.elasticsearch][main]...
abr 12 19:25:53 co-bocentos7siem01 logstash[22051]: [2021-04-12T19:25:53,681][WARN ][logstash.outputs.elasticsearch][main]...
abr 12 19:25:58 co-bocentos7siem01 logstash[22051]: [2021-04-12T19:25:58,684][WARN ][logstash.outputs.elasticsearch][main]...
abr 12 19:26:03 co-bocentos7siem01 logstash[22051]: [2021-04-12T19:26:03,687][WARN ][logstash.outputs.elasticsearch][main]...
abr 12 19:26:08 co-bocentos7siem01 logstash[22051]: [2021-04-12T19:26:08,690][WARN ][logstash.outputs.elasticsearch][main]...
abr 12 19:26:13 co-bocentos7siem01 logstash[22051]: [2021-04-12T19:26:13,692][WARN ][logstash.outputs.elasticsearch][main]...
abr 12 19:26:18 co-bocentos7siem01 logstash[22051]: [2021-04-12T19:26:18,696][WARN ][logstash.outputs.elasticsearch][main]...
abr 12 19:26:23 co-bocentos7siem01 logstash[22051]: [2021-04-12T19:26:23,699][WARN ][logstash.outputs.elasticsearch][main]...
abr 12 19:26:28 co-bocentos7siem01 logstash[22051]: [2021-04-12T19:26:28,703][WARN ][logstash.outputs.elasticsearch][main]...
Hint: Some lines were ellipsized, use -l to show in full.
```

Fuente: Los autores

Cuando el servicio de Logstash este iniciado, seguidamente se realiza la instalación de Wazuh Server como se observa en la figura 7

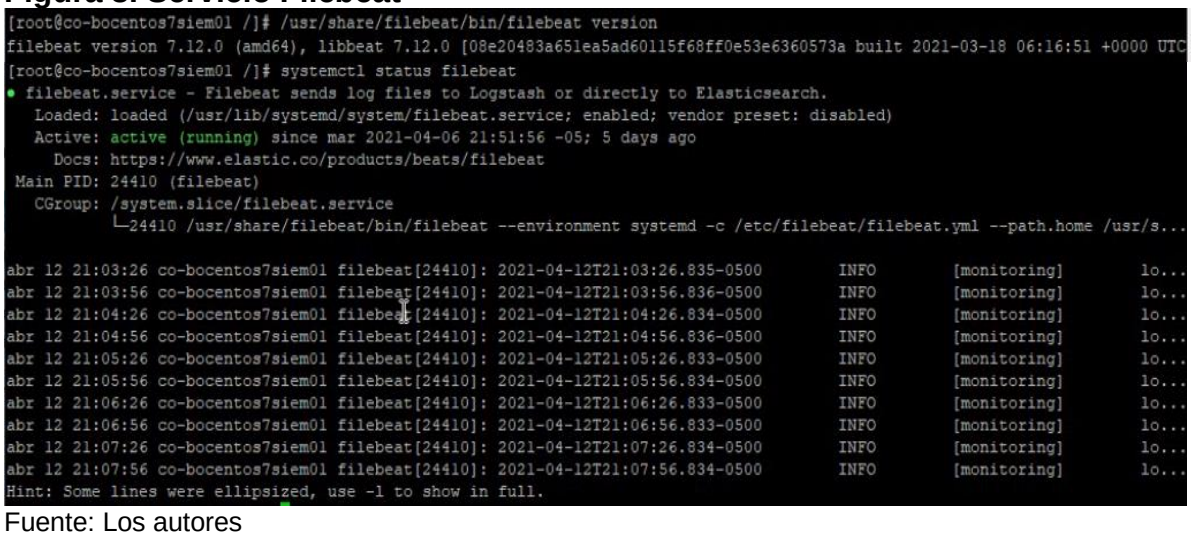
Figura 7. Servicio Wazuh



Fuente: Los autores

La figura 8 muestra que luego de tener instalado el wazuh server, se realiza la instalación de Filebeat, quien ayudará en todo el tema de alertas de Wazuh

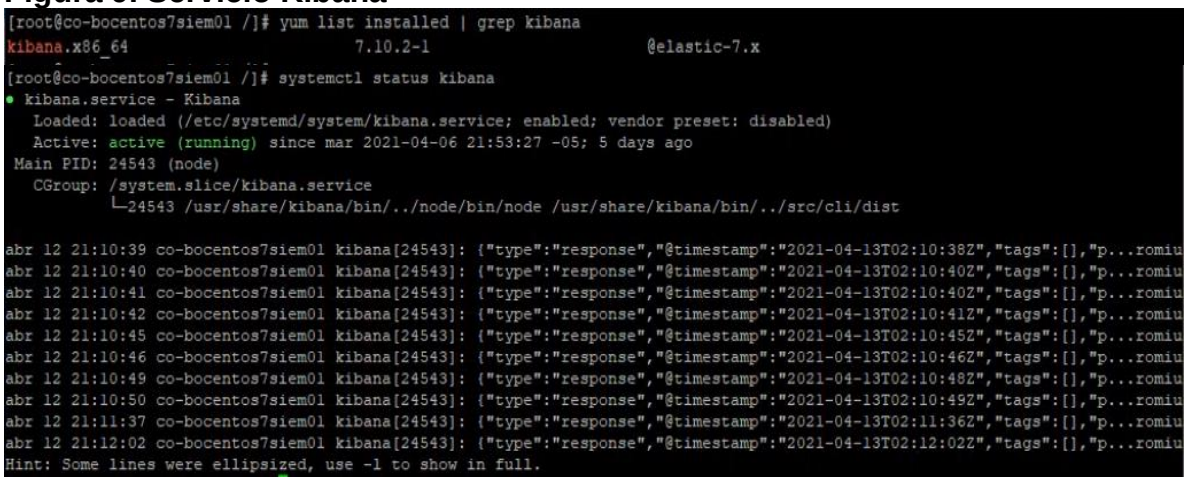
Figura 8. Servicio Filebeat



Fuente: Los autores

Inmediatamente que el servicio de Filebeat este activo he iniciado, a continuación, se procede con la instalación de Kibana , tal como se explica en la figura 9

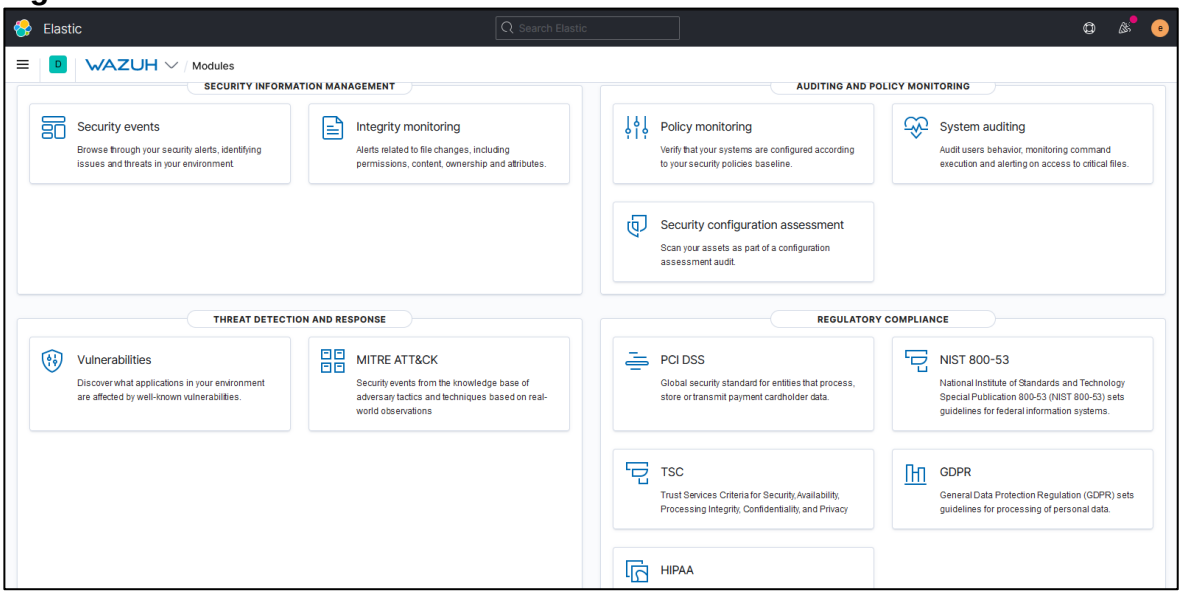
Figura 9. Servicio Kibana



Fuente: Los autores

En este punto ya se realizó la instalación de Wazuh, en la figura 10 se evidencia los módulos del SIEM los cuales están disponibles y son de libre uso.

Figura 10. Modulos wazuh



Fuente: Los autores

Para realizar la instalación del agente en cada uno de los servidores Windows se debe instalar con el comando mostrado en la figura 11

Figura 11. Agente de instalación para clientes

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.1.4-1.msi -OutFile wazuh-agent.msi;
./wazuh-agent.msi /q WAZUH_MANAGER='10.57.0.14' WAZUH_REGISTRATION_SERVER='10.57.0.14' WAZUH_AGENT_GROUP='Mazars-CO'
```

Fuente: Los autores

El símbolo del sistema debe ejecutarse como administrador para que el comando no presente inconvenientes.

Toda la instalación del SIEM se realizó con apoyo de los manuales de instalación.[51]

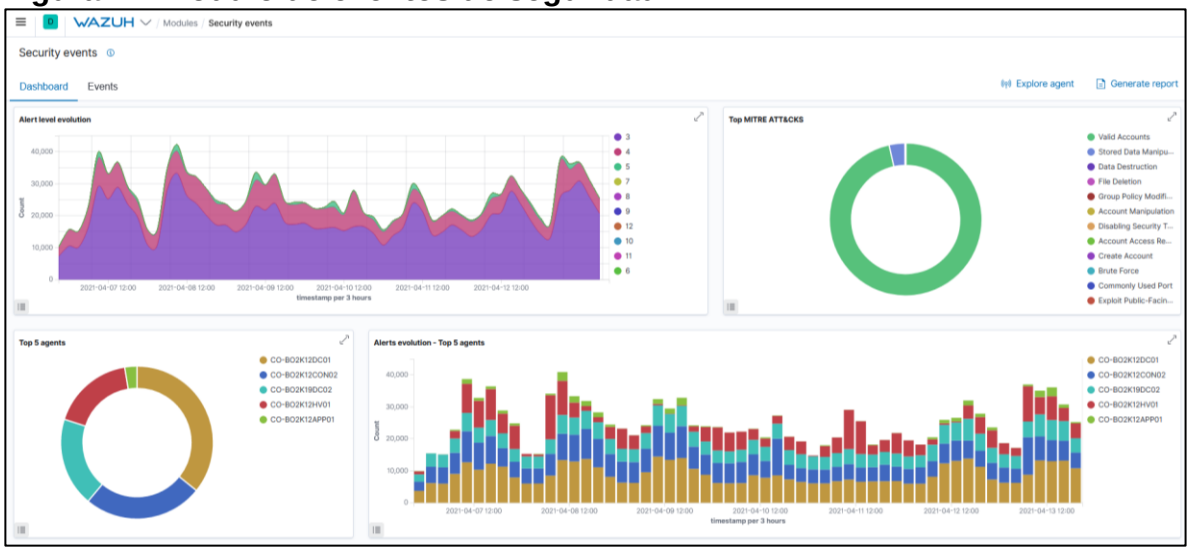
8.7 VERIFICACIÓN DE RESULTADOS

Después de la implementación y configuración del SIEM Wazuh se puede evidenciar que el sistema esta funcional y que Wazuh está recibiendo la información de los servidores.

En el Dashboard principal de los eventos de seguridad se puede tomar evidencia de cuatro gráficas comprendidas como se muestra en la figura 12

- Nivel de Evolución de Alertas
- Top Mitre Att&ck
- Top 5 de agentes
- Evolución de alertas por agentes.

Figura 12. Módulo de eventos de seguridad

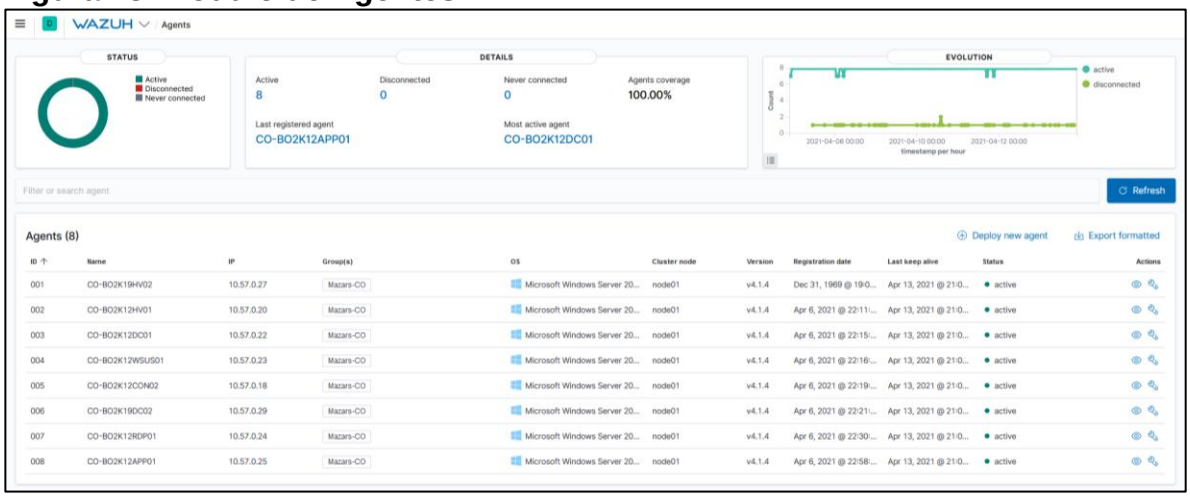


Fuente: Los autores

Teniendo en cuenta la configuración del agente donde se evidencia que los ID Event de Windows están configurados se valida que estos eventos estén reportando hacia el SIEM Wazuh como se ve en la figura 13

[51] WAZUH. Instalación paso a paso [en línea]. El sitio [citado 11, febrero, 2021]. Disponible en Internet: < URL: https://documentation.wazuh.com/current/installation-guide/open-distro/all-in-one-deployment/all_in_one.html>

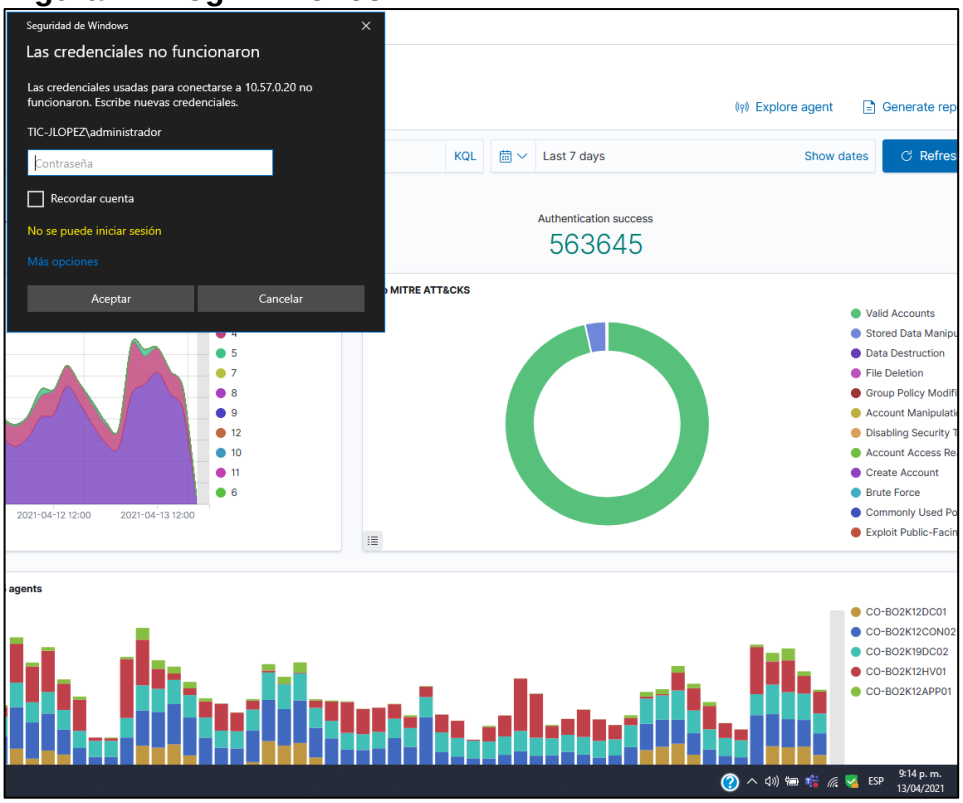
Figura 13. Módulo de Agentes



Fuente: Los autores

8.7.1 Pruebas de verificación. Para estas pruebas se realiza un login con el usuario administrador del servidor fallido intencionalmente para que este sea reportado al SIEM como se evidencia en la figura 14

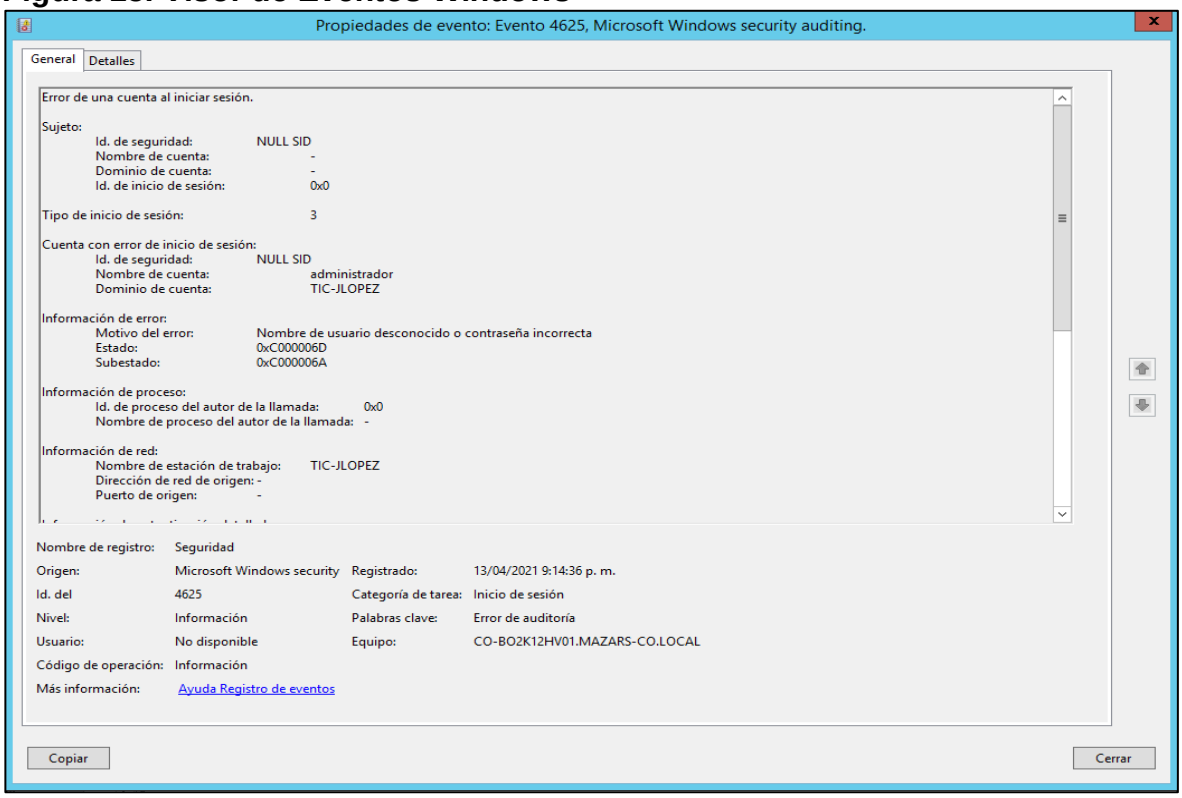
Figura 14. Login Erróneo



Fuente: Los autores

Luego de realizar el login se valida que haya sido reportado en el visor de eventos del sistema operativo para hacer la comparación con el SIEM, tal como se aprecia en la figura 15

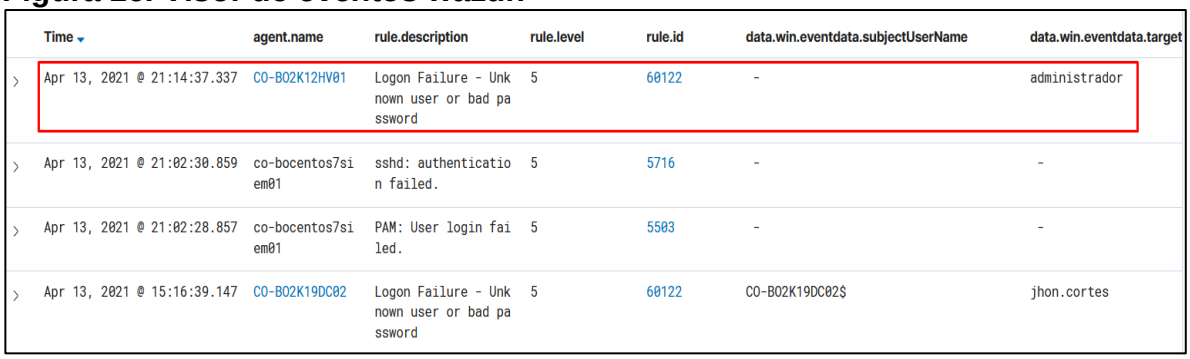
Figura 15. Visor de Eventos Windows



Fuente: Los autores

Después de ver que se reportó el evento en el visor de eventos del sistema operativo, se puede evidenciar que en el SIEM wazuh se evidencia el evento reportado por el visor de eventos del sistema operativo, tal como se aprecia en la figura 16

Figura 16. Visor de eventos wazuh



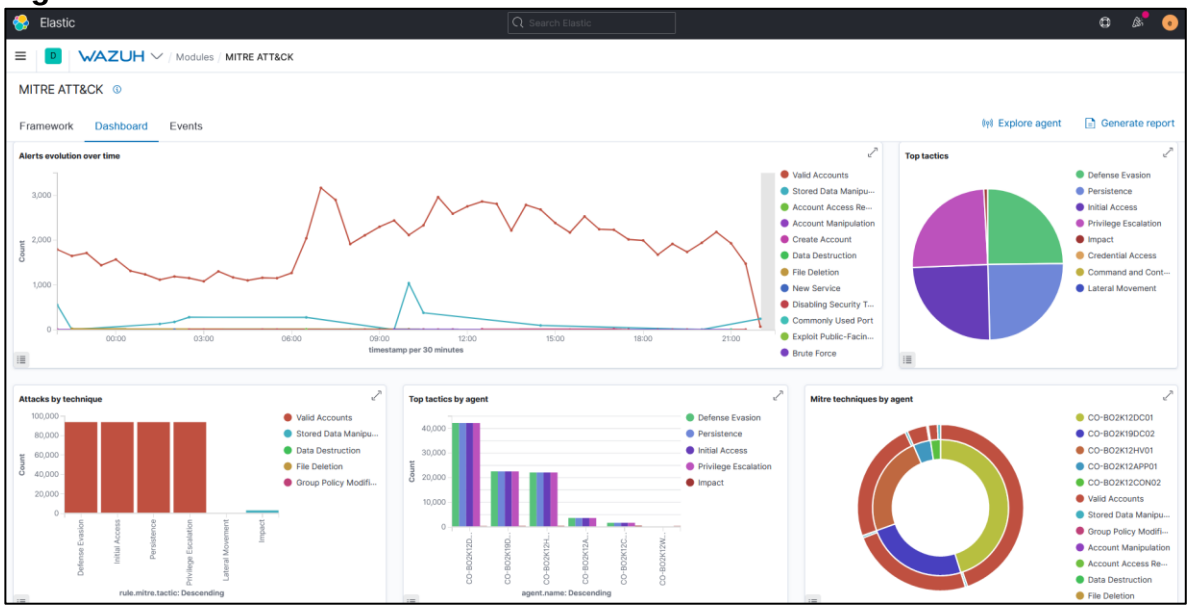
	Time	agent.name	rule.description	rule.level	rule.id	data.win.eventdata.subjectUserName	data.win.eventdata.target
›	Apr 13, 2021 @ 21:14:37.337	CO-BO2K12HV01	Logon Failure - Unknown user or bad password	5	60122	-	administrador
›	Apr 13, 2021 @ 21:02:30.859	co-bocentos7siem01	sshd: authentication failed.	5	5716	-	-
›	Apr 13, 2021 @ 21:02:28.857	co-bocentos7siem01	PAM: User login failed.	5	5503	-	-
›	Apr 13, 2021 @ 15:16:39.147	CO-BO2K19DC02	Logon Failure - Unknown user or bad password	5	60122	CO-BO2K19DC02$	jhon.cortes

Fuente: Los autores

8.7.2 Resultados Mitre ATT&CK. Wazuh se apoya en la base de datos de Mitre ATT&CK para tipificar la información que envían los agentes hacia el SIEM, esto es relevante ya que agrega una característica adicional al SIEM y detectar los posibles ataques.

En el dashboard de Mitre ATT&CK del SIEM se puede evidenciar cuales son los eventos de seguridad más significativos tal como se muestra en la figura 17

Figura 17. Modulo Mitre ATT&CK



Fuente: Los autores

9. CONCLUSIONES

Un SIEM es una herramienta de apoyo para los oficiales y analistas de seguridad ya que ayuda a centralizar los de eventos y logs de los servidores, es cierto que esta herramienta brinda un panorama completo del estado de la seguridad de la información en la compañía.

Se realizó la implementación de un SIEM Open Source, que tiene distintas características que dan valor agregado al área de tecnología para monitorear los eventos de seguridad y detectar diferentes ataques a los servidores Windows de la empresa Mazars Colombia, adicional a esto en el SIEM implementado se pueden encontrar módulos de gran importancia de cumplimiento normativo como la NIST 800-53, GDPR, PCI DSS entre otros; también tiene como apoyo un módulo de detección y respuesta a las amenazas donde se encuentra una base de conocimiento como Mitre ATT&CK.

BIBLIOGRAFIA

ACRONIS BAAS. Copia de seguridad en el cloud fácil de gestionar, fiable y sin infraestructura para pymes. [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://www.acronis.com/es-es/business/backup/cloud-deployment/>

FORTINET. Recursos e información. [en línea]. El sitio [citado 2, noviembre, 2021]. Disponible en Internet: < URL: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_100E_Series.pdf>

GLPI. Maneja la TI – Con el Poder de la Libertad. [en línea]. El sitio [citado 8, novimbre, 2020]. Disponible en Internet: < URL: https://glpi-project.org/es/>

GNU. ¿Qué es el Software Libre? [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://www.gnu.org/philosophy/free-sw.es.html#mission-statement>

HELISA. NIIF. [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://helisa.com/productos/administrador/>

_ _ _ _ _ _ _ _. Nomina. [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://helisa.com/productos/nomina/>

ICONTEC INTERNACIONAL. Cross Border Technology, Compendio seguridad de la información, segunda edición. Bogotá: Contacto Grafico.2015, p.25.

INM. Instituto Nacional de Metrología de Colombia. Configuración para conexión de la hora legal colombiana. [en línea]. El sitio [citado 8, noviembre, 2020]. Disponible en Internet: < URL: http://www.inm.gov.co/nueva/wp-content/uploads/2019/10/InstructivoHoraLegalColombiaMayo2017.pdf>

ISO. Organización Internacional de Normalización. ISO/IEC 27000. Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Descripción general y vocabulario [en línea]. Ginebra: ISO [citado 24, abril, 2021]. Disponible en Internet: < URL: https://www.iso27000.es/glosario.html>

_ _ _ _ _ _ _ _. Organización Internacional de Normalización. ISO/IEC 27001. Sistemas de Gestión la Seguridad de la Información. ISO. Ginebra – Suiza. 2013.p.2.

KASPERSKY. Security for Microsoft office 365. [en línea]. El sitio [citado 2, noviembre, 2021]. Disponible en Internet: < URL:https://latam.kaspersky.com/small-to-medium-business-security/microsoft-office-365-security>

KIMAI. Time-Tracker. [en línea]. El sitio [citado 8, noviembre, 2020]. Disponible en Internet: < URL:https://www.kimai.org/about/>

MAZARS. Mazars en Colombia. [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://www.mazars.com.co/Pagina-inicial/Acerca-de-nosotros/Mazars-en-Colombia2>

MICROSOFT 365. Business Premium. [en línea]. El sitio [citado 29, abril, 2021]. Disponible en Internet: < URL: https://support.microsoft.com/es-es/office/%C2%BFqu%C3%A9-es-microsoft-365-business-premium-901e2522-c2cf-4b8c-894e-f482cda3347a>

_ _ _ _ _ _ _ _. Anexo L: eventos para supervisar. [en línea]. El sitio [citado 8, noviembre, 2020]. Disponible en Internet: < URL:https://acortar.link/QEccfl>

_ _ _ _ _ _ _ _. Introducción a Active Directory Domain Services. [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>

MITRE ATT y CK. Base de conocimientos. [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://attack.mitre.org/>

NAGIOS CORE. [en línea]. El sitio [citado 2, noviembre, 2021]. Disponible en Internet: < URL: https://www.nagios.org/projects/nagios-core/>

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Information secuity. [en línea]. Ginebra: ISO [citado 24, abril, 2021]. Disponible en Internet: < URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

NIST. National Institute of Standards and Technology. Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

_ _ _ _ _ _ _ _. National Institute of Standards and Technology. Controles de seguridad y privacidad para organizaciones y sistemas de información. [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>

_ _ _ _ _ _ _ _. National Institute of Standards and Technology. Perfiles de sistema. [en línea]. El sitio [citado 2, noviembre, 2021]. Disponible en Internet: < URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

PARLAMENTO EUROPEO Y DEL CONSEJO. Reglamento (UE) 2016/679. [en línea]. España: La entidad [citado 24, abril, 2021]. Disponible en Internet: < URL: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN>

PCI. Security Stanards Council. PCI (industria de tarjetas de pago) Normas de seguridad de datos. [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3-2-1-ES-LA.PDF>

RAE. Real Academia Española.Definiciones. [en línea]. El sitio [citado 27, abril, 2021]. Disponible en Internet: < URL: https://dpej.rae.es/lema/servidor>

WAZUH. Arquitectura. [en línea]. El sitio [citado 8, noviembre, 2020]. Disponible en Internet: < URL: https://documentation.wazuh.com/current/getting-started/architecture.html>

_ _ _ _ _ _ _ _. Empezando. [en línea]. El sitio [citado 8, noviembre, 2020]. Disponible en Internet: < URL:https://documentation.wazuh.com/current/getting-started/index.html>

_ _ _ _ _ _ _ _. Instalación paso a paso [en línea]. El sitio [citado 11, febrero, 2021]. Disponible en Internet: < URL: https://documentation.wazuh.com/current/installation-guide/open-distro/all-in-one-deployment/all_in_one.html>

_ _ _ _ _ _ _ _. Requisitos [en línea]. El sitio [citado 11, febrero, 2021]. Disponible en Internet: < URL: https://documentation.wazuh.com/current/installation-guide/requirements.html>

ANEXOS

ANEXO A

MATRIZ DE RIESGOS MAZARS COLOMBIA SAS

MAZARS	MATRIZ DE RIESGOS	CÓDIGO:
		Versión: 1.0
		Fecha de Emisión: 09/08/2020
Tipo de proceso: Infraestructura Mazars-CO	Proceso: Infraestructura Mazars-CO - Analisis integral de Riesgos	Responsable: Jhon Alexander Lopez Naranjo	Clasificación:

TIPO DE ACTIVO	NOMBRE DEL ACTIVO IMPACTADO	ID de Riesgo	VULNERABILIDAD EXISTENTE	AMENAZA	DESCRIPCIÓN DEL ESCENARIO	PRINCIPIO DE SEGURIDAD IMPACTADO			PROBABILIDAD (A/M/B)	IMPACTO (A/M/B)	PRIORIDAD (1-9)	RECOMENDACIONES PARA EL TRATAMIENTO
						Confidencialidad	Integridad	Disponibilidad				
Hardware	Firewall Fortinet 100D	FW-01	10.57.0.15	Falla/Degradación de Sistema de Comunicaciones	Perdida de paquetes TCP, causa fallos en los servicios de la plataforma			×	Baja	Media	8	Validar que las conexiones fisicas esten en optimas condiciones
		FW-02	Falla	Sobrecarga de Tráfico	Saturacion de la capacidad de procesamiento de los paquetes en la plataforma			×	Media	Media	5	Evaluacion del performace del hardaware
		FW-03	Control de configuración inadecuado	Negación de Servicio	Cambios autorizados en la configuracion del firewall que causan denegacion del servicio de la plataforma.			×	Media	Media	5	Copias de Seguridad Recurrentes
		FW-04	Suministro eléctrico	Falla de Suministro de Energía	Apagado o desconfiguracion de los equipos por fallas en el fluido electrico			×	Baja	Alta	6	UPS - Planta Electrica
Hardware	CO-BO2K16HV01	HV01-01	Control de acceso inadecuado	Uso de software por usuarios no Autorizados	Ejecucion de aplicaciones no autorizadas en los servidores de produccion	×	×	×	Media	Media	5	SIEM
		HV01-02	Suministro eléctrico	Subidas de Voltaje / Fluctuaciones	Daño en los equipos físicos: Board, Memoria, Procesador que causan fallos en los servidores físicos		×	×	Media	Alta	3	Supresor de Picos
		HV01-03	Falla	Pérdida de Disponibilidad a Usuarios Autorizados	Falla física del hardware que genera fallas en los servicios prestados			×	Media	Media	5	Copias de Seguridad Recurrentes
		HV01-04	Conexión de equipo no autorizado	Uso de Instalaciones de Red en Forma no Autorizada	Conexión a interfaces de red no autorizadas en los servidores físicos	×	×		Alta	Media	2	SIEM
		HV01-05	Desastre natural	Falla de Suministro de Energía	Apagado de todos los servidores por fallas en el fluido electrico	×	×	×	Media	Alta	3	UPS - Planta Electrica
		HV01-06	Locación del sitio	Daño Accidental - Incendio	Incendio de las instalaciones del Datacenter			×	Media	Alta	3	BCP y DRP
		HV01-07	Control de acceso inadecuado	Ataque Malicioso - Manipulación de Equipo Informático	Manipulacion del equipo para ingresar a datos sensibles de la organización	×			Media	Media	5	SIEM
Software	Servidor Virtual CO-BO2K12DC01	DC01-01	Especificación inadecuada incompleta	Degradación en Tiempo de Respuesta	Cambio autorizado que genera problemas y/o fallos en los tiempos de respuesta en la aplicación de monitoreo			×	Baja	Media	8	Evaluacion del performace del hardaware
		DC01-02	Administración de configuración inadecuada	Uso de Software por Usuarios no Autorizados	Ingreso no autorizado al servidor virtual	×	×	×	Media	Media	5	SIEM
		DC01-03	Testeo inadecuado insuficiente	Degradación de Disponibilidad	Degradacion del servicio del Servidor por actualizacion del sistema operativo/aplicación sin el suficiente testeo para detectar problemas y/o fallos.			×	Media	Media	5	Copias de Seguridad Recurrentes
		DC01-04	Control de descarga inadecuado	Descarga no Controlada de Software	Actualizacion de aplicaciones no autorizadas o programadas en horario de alto trafico			×	Media	Media	5	Cronograma de Actualizaciones
		DC01-05	Suministro eléctrico	Subidas de Voltaje / Fluctuaciones	Daño en los equipos físicos: Board, Memoria, Procesador que causan fallos en los servidores físicos		×	×	Media	Alta	3	UPS - Planta Electrica
Software	Servidor Virtual CO-BO2K12WSUS01	WSUS01-01	Especificación inadecuada incompleta	Degradación en Tiempo de Respuesta	Cambio autorizado que genera problemas y/o fallos en los tiempos de respuesta en la aplicación de monitoreo			×	Baja	Media	8	Evaluacion del performace del hardaware
		WSUS01-02	Administración de configuración inadecuada	Uso de Software por Usuarios no Autorizados	Ingreso no autorizado al servidor virtual	×	×	×	Media	Media	5	SIEM
		WSUS01-03	Testeo inadecuado insuficiente	Degradación de Disponibilidad	Degradacion del servicio del Servidor por actualizacion del sistema operativo/aplicación sin el suficiente testeo para detectar problemas y/o fallos.			×	Media	Media	5	Cronograma de Actualizaciones
		WSUS01-04	Control de descarga inadecuado	Descarga no Controlada de Software	Actualizacion de aplicaciones no autorizadas o programadas en horario de alto trafico			×	Media	Media	5	Cronograma de Actualizaciones
		WSUS01-05	Suministro eléctrico	Subidas de Voltaje / Fluctuaciones	Daño en los equipos físicos: Board, Memoria, Procesador que causan fallos en los servidores físicos		×	×	Media	Alta	3	UPS - Planta Electrica
Hardware	CO-BO2K19HV02	HV02-01	Control de acceso inadecuado	Uso de software por usuarios no Autorizados	Ejecucion de aplicaciones no autorizadas en los servidores de produccion	×	×	×	Media	Media	5	SIEM
		HV02-02	Suministro eléctrico	Subidas de Voltaje / Fluctuaciones	Daño en los equipos físicos: Board, Memoria, Procesador que causan fallos en los servidores físicos		×	×	Media	Alta	3	UPS - Planta Electrica
		HV02-03	Falla	Pérdida de Disponibilidad a Usuarios Autorizados	Falla física del hardware que genera fallas en los servicios prestados			×	Media	Media	5	Copias de Seguridad Recurrentes
		HV02-04	Conexión de equipo no autorizado	Uso de Instalaciones de Red en Forma no Autorizada	Conexión a interfaces de red no autorizadas en los servidores físicos	×	×		Alta	Media	2	SIEM
		HV02-05	Desastre natural	Falla de Suministro de Energía	Apagado de todos los servidores por fallas en el fluido electrico	×	×	×	Media	Alta	3	UPS - Planta Electrica
		HV02-06	Locación del sitio	Daño Accidental - Incendio	Incendio de las instalaciones del Datacenter			×	Media	Alta	3	BCP y DRP
		HV02-07	Control de acceso inadecuado	Ataque Malicioso - Manipulación de Equipo Informático	Manipulacion del equipo para ingresar a datos sensibles de la organización	×			Media	Media	5	SIEM
Software	Servidor Virtual CO-BO2K12DC02	DC02-01	Especificación inadecuada incompleta	Degradación en Tiempo de Respuesta	Cambio autorizado que genera problemas y/o fallos en los tiempos de respuesta en la aplicación de monitoreo			×	Baja	Media	8	Evaluacion del performace del hardaware
		DC02-02	Administración de configuración inadecuada	Uso de Software por Usuarios no Autorizados	Ingreso no autorizado al servidor virtual	×	×	×	Media	Media	5	SIEM
		DC02-03	Testeo inadecuado insuficiente	Degradación de Disponibilidad	Degradacion del servicio del Servidor por actualizacion del sistema operativo/aplicación sin el suficiente testeo para detectar problemas y/o fallos.			×	Media	Media	5	Copias de Seguridad Recurrentes
		DC02-04	Control de descarga inadecuado	Descarga no Controlada de Software	Actualizacion de aplicaciones no autorizadas o programadas en horario de alto trafico			×	Media	Media	5	Cronograma de Actualizaciones
		DC02-05	Suministro eléctrico	Subidas de Voltaje / Fluctuaciones	Daño en los equipos físicos: Board, Memoria, Procesador que causan fallos en los servidores físicos		×	×	Media	Alta	3	UPS - Planta Electrica

Software	Servidor Virtual CO-BO2K12RDP01	RDP01-01	Especificación inadecuada incompleta	Degradación en Tiempo de Respuesta	Cambio autorizado que genera problemas y/o fallos en los tiempos de respuesta en la aplicación de escritorio remoto			X	Baja	Media	8	Evaluacion del performace del hardaware
		RDP01-02	Administración de configuración inadecuada	Uso de Software por Usuarios no Autorizados	Ingreso no autorizado al servidor de escritorio remoto	X	X	X	Media	Media	5	SIEM
		RDP01-03	Testeo inadecuado insuficiente	Degradación de Disponibilidad	Degradacion del servicio del servidor por actualizacion del sistema operativo/aplicación sin el suficiente testeo para detectar problemas y/o fallos.			X	Media	Media	5	Copias de Seguridad Recurrentes
		RDP01-04	Control de descarga inadecuado	Descarga no Controlada de Software	Actualizacion de aplicaciones no autorizadas o programadas en horario de alto trafico			X	Media	Media	5	Cronograma de Actualizaciones
		RDP01-05	Suministro eléctrico	Subidas de Voltaje / Fluctuaciones	Daño en los equipos fisicos: Board, Memoria, Procesador que causan fallos en los servidores fisicos		X	X	Media	Alta	3	UPS - Planta Electrica
Software	Servidor Virtual CO-BO2K12APP01	APP01-01	Especificación inadecuada incompleta	Degradación en Tiempo de Respuesta	Cambio autorizado que genera problemas y/o fallos en los tiempos de respuesta en la aplicación Wifi (Ubiquiti)			X	Baja	Media	8	Evaluacion del performace del hardaware
		APP01-02	Administración de configuración inadecuada	Uso de Software por Usuarios no Autorizados	Ingreso no autorizado al servidor virtual de Wifi (Ubiquiti)	X	X	X	Media	Media	5	SIEM
		APP01-03	Testeo inadecuado insuficiente	Degradación de Disponibilidad	Degradacion del servicio del Host por actualizacion del sistema operativo/aplicación sin el suficiente testeo para detectar problemas y/o fallos.			X	Media	Media	5	Copias de Seguridad Recurrentes
		APP01-04	Control de descarga inadecuado	Descarga no Controlada de Software	Actualizacion de aplicaciones no autorizadas o programadas en horario de alto trafico			X	Media	Media	5	Cronograma de Actualizaciones
		APP01-05	Suministro eléctrico	Subidas de Voltaje / Fluctuaciones	Daño en los equipos fisicos: Board, Memoria, Procesador que causan fallos en los servidores fisicos		X	X	Media	Alta	3	UPS - Planta Electrica
Hardware	CO-BO2K12CON02	CON02-01	Control de acceso inadecuado	Uso de software por usuarios no Autorizados	Ejecucion de aplicaciones no autorizadas en los servidores de produccion	X	X	X	Media	Media	5	SIEM
		CON02-02	Suministro eléctrico	Subidas de Voltaje / Fluctuaciones	Daño en los equipos fisicos: Board, Memoria, Procesador que causan fallos en los servidores fisicos		X	X	Media	Alta	3	Supresor de Picos
		CON02-03	Falla	Pérdida de Disponibilidad a Usuarios Autorizados	Falla fisica del hardware que genera fallas en los servicios prestados			X	Media	Media	5	Copias de Seguridad Recurrentes
		CON02-04	Conexión de equipo no autorizado	Uso de Instalaciones de Red en Forma no Autorizada	Conexión a interfaces de red no autorizadas en los servidores fisicos	X	X		Alta	Media	2	SIEM
		CON02-05	Desastre natural	Falla de Suministro de Energía	Apagado de todos los servidores por fallas en el fluido electrico	X	X	X	Media	Alta	3	UPS - Planta Electrica
		CON02-06	Locación del sitio	Daño Accidental - Incendio	Incendio de las instalaciones del Datacenter			X	Media	Alta	3	BCP y DRP
		CON02-07	Control de acceso inadecuado	Ataque Malicioso - Manipulación de Equipo Informático	Manipulacion del equipo para ingresar a datos sensibles de la organización	X			Media	Media	5	SIEM
Hardware	CO-BO2K12RDP02	RDP02-01	Especificación inadecuada incompleta	Degradación en Tiempo de Respuesta	Cambio autorizado que genera problemas y/o fallos en los tiempos de respuesta en la aplicación de escritorio remoto			X	Baja	Media	8	Evaluacion del performace del hardaware
		RDP02-02	Administración de configuración inadecuada	Uso de Software por Usuarios no Autorizados	Ingreso no autorizado al servidor de escritorio remoto	X	X	X	Media	Media	5	SIEM
		RDP02-03	Testeo inadecuado insuficiente	Degradación de Disponibilidad	Degradacion del servicio del servidor por actualizacion del sistema operativo/aplicación sin el suficiente testeo para detectar problemas y/o fallos.			X	Media	Media	5	Copias de Seguridad Recurrentes
		RDP02-04	Control de descarga inadecuado	Descarga no Controlada de Software	Actualizacion de aplicaciones no autorizadas o programadas en horario de alto trafico			X	Media	Media	5	Cronograma de Actualizaciones
		RDP02-05	Suministro eléctrico	Subidas de Voltaje / Fluctuaciones	Daño en los equipos fisicos: Board, Memoria, Procesador que causan fallos en los servidores fisicos		X	X	Media	Alta	3	UPS - Planta Electrica
Software	Servidor Virtual CENTOS	CENTOS-01	Especificación inadecuada incompleta	Degradación en Tiempo de Respuesta	Cambio autorizado que genera problemas y/o fallos en los tiempos de respuesta en la aplicación GLPI			X	Baja	Media	8	Evaluacion del performace del hardaware
		CENTOS-02	Administración de configuración inadecuada	Uso de Software por Usuarios no Autorizados	Ingreso no autorizado al servidor virtual GLPI	X	X	X	Media	Media	5	SIEM
		CENTOS-03	Testeo inadecuado insuficiente	Degradación de Disponibilidad	Degradacion del servicio del Host por actualizacion del sistema operativo/aplicación sin el suficiente testeo para detectar problemas y/o fallos.			X	Media	Media	5	Copias de Seguridad Recurrentes
		CENTOS-04	Control de descarga inadecuado	Descarga no Controlada de Software	Actualizacion de aplicaciones no autorizadas o programadas en horario de alto trafico			X	Media	Media	5	Cronograma de Actualizaciones
		CENTOS-05	Suministro eléctrico	Subidas de Voltaje / Fluctuaciones	Daño en los equipos fisicos: Board, Memoria, Procesador que causan fallos en los servidores fisicos		X	X	Media	Alta	3	UPS - Planta Electrica
Personal	Auxiliar de TI&C	AUXTI-01	Ausentismo	Déficit de Personal	Renuncia del personal a cargo del soporte de la operación			X	Alta	Media	2	Plan Carrera - Salario Emocional
		AUXTI-02	Excesiva autoridad control	Uso no Autorizado de Sistemas Informáticos	Intento de ingreso no autorizado a servidores, equipos de red	X	X		Media	Media	5	Plan de estudios - Evaluacion de Desmepeño
		AUXTI-03	Falta de políticas normas procedimientos	Acceso no Autorizado al Edificio	Ingreso al datacenter luego de revocar los permisos de acceso	X	X	X	Baja	Media	8	Evaluacion politica de acceso
		AUXTI-04	Empleado molesto	Ataque Malicioso - Manipulación de Datos o Software	Intento de manipulacion de la plataforma luego de terminacion del contrato	X	X	X	Baja	Media	8	Baja de usuario y credenciales

Personal	Coordinador TI&C	CIO-01	Excesiva autoridad control	Pérdida de Confidencialidad	Credenciales de acceso comprometidas o robadas por un tercero dentro o fuera de la Organización	X	X		Media	Media	5	Cambio recurrente de Contraseñas - Segundo factor de autenticacion
		CIO-02	Ausentismo	Degradación en Tiempo de Respuesta	Retardos en los tiempos de respuesta del manejo y atencion de fallas e indicentes en la plataforma			X	Alta	Media	2	Plan Carrera - Salario Emocional
		CIO-03	Revocación de derechos de acceso	Uso de Software por Usuarios no Autorizados	Intento de ingreso a activos no autorizados	X	X		Media	Media	5	Evaluacion politica de acceso
		CIO-04	Excesiva autoridad control	Uso no Autorizado de Sistemas Informáticos	Intento de ingreso no autorizado a servidores, equipos de red	X	X		Media	Media	5	Plan de estudios - Evaluacion de Desmepeño
Información	Backup maquinas virutales servidores hyperv	BK-01	Locación almacenamiento no protegido	Pérdida de Confidencialidad	Acceso a copias de maquinas virtuales sin autorizacion	X	X		Media	Media	5	Politica de copias de seguridad - Control de acceso a copias de seguridad
		BK-02	Falta de validación	Corrupción de Datos	Modificacion no autorizada del backup almacenado	X	X		Media	Media	5	Politica de seguridad - Bitacora de copias de seguridad
		BK-03	Disponibilidad de datos respaldados	No-Disponibilidad de Respaldos	Copias de seguridad corruptas o no probadas			X	Baja	Alta	6	Prubas de recurrentes de restauracion de copias de seguridad
		BK-04	Copyright	Uso de Software por Usuarios no Autorizados	Restaurar los backups en un entorno diferente a produccion	X	X		Media	Media	5	Validacion trimestral de la configuracion de restauracion de copias de seguridad

Fuente: Mazars Colombia, 2020

ANEXO B

PERFIL DE LOS SISTEMAS

Servidor					
Ubicación	**Elementos**	**Descripción**			
RACK PRINCIPAL	Nombre:	**CO-BO2K16HV01**			
	Marca:	HP			
	Modelo:	ProLiant DL180 Gen9			
	Procesador:	Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz (16 CPUs), ~2.1GHz			
	Memoria RAM:	32 GB			
	Discos Duros:	4(2 TB) - Raid5 (5588,94 GB)			
	Tarjeta de Red:	Intel(R) I350 Gigabit Network Connection			
	Volúmenes de Disco:	Vol. C	Vol. I		
	Espacio Total:	250 MB	5338,40 GB		
	Espacio Disponible:	181,40 GB	1297,30 GB		
	Tolerancia a Fallos:	No			
	Modem / Dial Up:	SI: NO:X			
	Software				
	Sistema Operativo:	Windows Server 2016 Standard (Español)			
	Service Pack:	1			
	Windows Update	Si			
	Función:	File Server - Virtualizacion (Hyper-V) - Backup			
	Servicios Instalados:	File Server / Hyper-V / Copias de Seguridad			
	Versión IE:	11			
	Imagen de S.O.	SI: NO: X			
	Fecha de Creación				
	Red				
	Dominio y/o Árbol:	Mazars-CO.local	N/A		
	Protocolos:	TCP/IP	N/A		
	MAC Address	98-F2-B3-F2-E3-EF	N/A		
	Dirección IP:	10.57.0.20	N/A		
	Subnet Mask:	255.255.255.0	N/A		
	Gateway:	10.57.0.254	N/A		
	DNS1:	10.57.0.22	N/A		
	DNS2:	N/A	N/A		
	WINS:	N/A	N/A		
	Comportamiento				
	Hora de disponibilidad	7x24x360			
	Frecuencia de Actualizaciones	Segundo Jueves habil de cada mes			
	Criticidad:				
	Servidor de documentos - Servidor de Virtualizacion - Servidor de Backups				

Servidor					
Ubicación	**Elementos**	**Descripción**			
RACK PRINCIPAL	Nombre:	**CO-BO2K12DC01**			
	Marca:	Microsoft Corporation			
	Modelo:	Virtual Machine			
	Procesador:	Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz, ~2.1GHz			
	Memoria RAM:	4 GB			
	Discos Duros:	Virtual de 127 GB			
	Tarjeta de Red:	Adaptador de red de Microsoft Hyper-V			
	Volúmenes de Disco:	Vol. C			
	Espacio Total:	127 GB			
	Espacio Disponible:	108 GB			
	Tolerancia a Fallos:	No			
	Modem / Dial Up:	SI: NO:X			
	Software				
	Sistema Operativo:	Microsoft Windows Server 2012 R2 Standard			
	Service Pack:	1			
	Windows Update	Si			
	Función:	Controlador de Dominio			
	Servicios Instalados:	AD - DHCP - DNS			
	Versión IE:	11			
	Imagen de S.O.	SI: NO: X			
	Fecha de Creación				
	Red				
	Dominio y/o Árbol:	Mazars-CO.local	N/A		
	Protocolos:	TCP/IP	N/A		
	MAC Address	00-15-5D-32-14-09	N/A		
	Dirección IP:	10.57.0.22	N/A		
	Subnet Mask:	255.255.255.0	N/A		
	Gateway:	10.57.0.254	N/A		
	DNS1:	10.57.0.22	N/A		
	DNS2:	127.0.0.1	N/A		
	WINS:	N/A	N/A		
	Comportamiento				
	Hora de disponibilidad	7x24x360			
	Frecuencia de Actualizaciones	Segundo Jueves habil de cada mes			
	Criticidad:				
	Servidor Controlador de Dominio				

Servidor					
Ubicación	**Elementos**	**Descripción**			
RACK PRINCIPAL	Nombre:	**CO-BO2K12RDP02**			
	Marca:	Microsoft Corporation			
	Modelo:	Virtual Machine			
	Procesador:	Intel(R) Core(TM) i3-4130T CPU @ 2.90GHz (4 CPUs), ~2.9GHz			
	Memoria RAM:	8 GB			
	Discos Duros:	HHD 320 GB			
	Tarjeta de Red:	Intel(R) Ethernet Connection I217-LM			
	Volúmenes de Disco:	Vol. C			
	Espacio Total:	228.6 GB			
	Espacio Disponible:	194.8 GB			
	Tolerancia a Fallos:	No			
	Modem / Dial Up:	SI: NO:X			
	Software				
	Sistema Operativo:	Microsoft Windows Server 2012 R2 Standard			
	Service Pack:	1			
	Windows Update	Si			
	Función:	RDP Clientes - Conexión Remota Helisa Niif y Recurso Humano 4			
	Servicios Instalados:	Administrador Licencias Escritorio Remoto			
	Versión IE:	11			
	Imagen de S.O.	SI: NO: X			
	Fecha de Creación				
	Red				
	Dominio y/o Árbol:	Mazars-CO.local	N/A		
	Protocolos:	TCP/IP	N/A		
	MAC Address	00-15-5D-32-14-0A	N/A		
	Dirección IP:	10.57.0.19	N/A		
	Subnet Mask:	255.255.255.0	N/A		
	Gateway:	10.57.0.254	N/A		
	DNS1:	10.57.0.22	N/A		
	DNS2:	N/A	N/A		
	WINS:	N/A	N/A		
	Comportamiento				
	Hora de disponibilidad	7x24x360			
	Frecuencia de Actualizaciones	Segundo Jueves habil de cada mes			
	Criticidad:				
	Conexión Remota Helisa Niif y Recurso Humano 4				

Servidor					
Ubicación	**Elementos**	**Descripción**			
RACK PRINCIPAL	Nombre:	**CO-BO2K12WSUS01**			
	Marca:	Microsoft Corporation			
	Modelo:	Virtual Machine			
	Procesador:	Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz (2 CPUs), ~2.1GHz			
	Memoria RAM:	4 GB			
	Discos Duros:	Virtual de 127 GB			
	Tarjeta de Red:	Adaptador de red de Microsoft Hyper-V			
	Volúmenes de Disco:	Vol. C	Vol. D		
	Espacio Total:	127 GB	255 GB		
	Espacio Disponible:	90,40 GB	118 GB		
	Tolerancia a Fallos:	No			
	Modem / Dial Up:	SI: NO:X			
	Software				
	Sistema Operativo:	Microsoft Windows Server 2012 R2 Standard			
	Service Pack:	1			
	Windows Update	Si			
	Función:	Servidor de actualizaciones para servidores de Mazars-CO			
	Servicios Instalados:	Servicios de actualización de Windows Server			
	Versión IE:	11			
	Imagen de S.O.	SI: NO: X			
	Fecha de Creación				
	Red				
	Dominio y/o Árbol:	Mazars-CO.local	N/A		
	Protocolos:	TCP/IP	N/A		
	MAC Address	00-15-5D-32-14-07	N/A		
	Dirección IP:	10.57.0.23	N/A		
	Subnet Mask:	255.255.255.0	N/A		
	Gateway:	10.57.0.254	N/A		
	DNS1:	10.57.0.22	N/A		
	DNS2:	N/A	N/A		
	WINS:	N/A	N/A		
	Comportamiento				
	Hora de disponibilidad	5x12			
	Frecuencia de Actualizaciones	Segundo Jueves habil de cada mes			
	Criticidad:				
	Actualizacion de Servidores				

Servidor									
Ubicación	**Elementos**	**Descripción**							
RACK PRINCIPAL	Nombre:	**CO-BOCENTOS7APP01**							
	Marca:	HP							
	Modelo:	ProDesk 600 G1 DM							
	Procesador:	Intel(R) Core(TM) i3-4130T CPU @ 2.90GHz (4 CPUs), ~2.9GHz							
	Memoria RAM:	4 GB							
	Discos Duros:	Virtual de 250 GB							
	Tarjeta de Red:	Adaptador de red de Microsoft Hyper-V							
	Volúmenes de Disco:	/dev/mapper/centos-root (Montado en "/")	devtmpfs (Montado en "/dev")	tmpfs (Montado en "/dev/shm")	tmpfs (Montado en "/run")	tmpfs (Montado en "/sys/fs/cgroup")	/dev/sda1 (Montado en "/boot")	/dev/mapper/centos-home (Montado en "/home")	tmpfs (Montado en "/run/user/0")
	Espacio Total:	50 G	448 M	460 M	460 M	460 M	1014 M	74 G	92 M
	Espacio Disponible:	47 G	448 M	460 M	454 M	460 M	856 M	74 G	92 M
	Tolerancia a Fallos:	No							
	Modem / Dial Up:	SI: NO:X							
	Software								
	Sistema Operativo:	CentOS Linux 7 (Core)							
	Service Pack:	Linux 3.10.0-1160.2.2.el7.x86_64							
	Windows Update	Si							
	Función:	Kimai - GLPI							
	Servicios Instalados:	Apache - MariaDB - PHP							
	Versión IE:	N/A							
	Imagen de S.O.	SI: NO: X							
	Fecha de Creación								
	Red								
	Dominio y/o Árbol:	Mazars-CO.local				N/A			
	Protocolos:	TCP/IP				N/A			
	MAC Address	00-15-5D-32-14-0A				N/A			
	Dirección IP:	10.57.0.17				N/A			
	Subnet Mask:	255.255.255.0				N/A			
	Gateway:	10.57.0.254				N/A			
	DNS1:	10.57.0.22				N/A			
	DNS2:	N/A				N/A			
	WINS:	N/A				N/A			
	Criticidad:								
	Kimai - GLPI								

Servidor					
Ubicación	**Elementos**	**Descripción**			
RACK PRINCIPAL	Nombre:	**CO-BO2K12CON02**			
	Marca:	HP			
	Modelo:	ProDesk 600 G1 DM			
	Procesador:	Intel(R) Core(TM) i3-4130T CPU @ 2.90GHz (4 CPUs), ~2.9GHz			
	Memoria RAM:	4 GB			
	Discos Duros:	HHD 500 GB			
	Tarjeta de Red:	Intel(R) Ethernet Connection I217-LM			
	Volúmenes de Disco:	Vol. C			
	Espacio Total:	476.4 GB			
	Espacio Disponible:	385.1 GB			
	Tolerancia a Fallos:	No			
	Modem / Dial Up:	SI: NO:X			
	Software				
	Sistema Operativo:	Microsoft Windows Server 2012 R2 Standard			
	Service Pack:	1			
	Windows Update	Si			
	Función:	Servidor de Contabildiad y Nomina			
	Servicios Instalados:	Helisa Niif - Recurso Humano 4			
	Versión IE:	11			
	Imagen de S.O.	SI: NO: X			
	Fecha de Creación				
	Red				
	Dominio y/o Árbol:	Mazars-CO.local	N/A		
	Protocolos:	TCP/IP	N/A		
	MAC Address	00-15-5D-32-14-01	N/A		
	Dirección IP:	10.57.0.18	N/A		
	Subnet Mask:	255.255.255.0	N/A		
	Gateway:	10.57.0.254	N/A		
	DNS1:	10.57.0.22	N/A		
	DNS2:	N/A	N/A		
	WINS:	N/A	N/A		
	Comportamiento				
	Hora de disponibilidad	7x24x360			
	Frecuencia de Actualizaciones	Segundo Jueves habil de cada mes			
	Criticidad:				
	Servidor de Contabilidad				

Servidor					
Ubicación	**Elementos**	**Descripción**			
RACK PRINCIPAL	Nombre:	**CO-BO2K19HV02**			
	Marca:	Lenovo			
	Modelo:	ThinkSystem SR530			
	Procesador:	Intel(R) Xeon(R) Bronze 3106 CPU @ 1.70GHz (8 CPUs), ~1.7GHz			
	Memoria RAM:	64 GB			
	Discos Duros:	4(2 TB) - Raid5 (5588,94 GB)			
	Tarjeta de Red:	Intel(R) I350 Gigabit Network Connection			
	Volúmenes de Disco:	Vol. C	Vol. D		
	Espacio Total:	244,14 GB	5340,48 GB		
	Espacio Disponible:	150,16 GB	1386, 57 GB		
	Tolerancia a Fallos:	No			
	Modem / Dial Up:	SI: NO:X			
	Software				
	Sistema Operativo:	Windows Server 2019 Standard 64-bit			
	Service Pack:	1			
	Windows Update	Si			
	Función:	File Server - Virtualizacion (Hyper-V) - Backup			
	Servicios Instalados:	File Server / Hyper-V / Copias de Seguridad			
	Versión IE:	11			
	Imagen de S.O.	SI: NO: X			
	Fecha de Creación				
	Red				
	Dominio y/o Árbol:	Mazars-CO.local	N/A		
	Protocolos:	TCP/IP	N/A		
	MAC Address	98-F2-B3-F2-E3-EF	N/A		
	Dirección IP:	10.57.0.27	N/A		
	Subnet Mask:	255.255.255.0	N/A		
	Gateway:	10.57.0.254	N/A		
	DNS1:	10.57.0.22	N/A		
	DNS2:	N/A	N/A		
	WINS:	N/A	N/A		
	Comportamiento				
	Hora de disponibilidad	7x24x360			
	Frecuencia de Actualizaciones	Segundo Jueves habil de cada mes			
	Criticidad:				
	Servidor de documentos - Servidor de Virtualizacion - Servidor de Backups				

Servidor					
Ubicación	**Elementos**	**Descripción**			
RACK PRINCIPAL	Nombre:	**CO-BO2K12APP01**			
	Marca:	Microsoft Corporation			
	Modelo:	Virtual Machine			
	Procesador:	Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz (2 CPUs), ~2.1GHz			
	Memoria RAM:	3 GB			
	Discos Duros:	Virtual de 127 GB			
	Tarjeta de Red:	Adaptador de red de Microsoft Hyper-V			
	Volúmenes de Disco:	Vol. C			
	Espacio Total:	127 GB			
	Espacio Disponible:	90,40 GB			
	Tolerancia a Fallos:	No			
	Modem / Dial Up:	SI: NO:X			
	Software				
	Sistema Operativo:	Microsoft Windows Server 2012 R2 Standard			
	Service Pack:	1			
	Windows Update	Si			
	Función:				
	Servicios Instalados:	CJL Time - Ubiquiti UniFi - Print Server			
	Versión IE:	11			
	Imagen de S.O.	SI: NO: X			
	Fecha de Creación				
	Red				
	Dominio y/o Árbol:	Mazars-CO.local	N/A		
	Protocolos:	TCP/IP	N/A		
	MAC Address	00-15-5D-32-14-07	N/A		
	Dirección IP:	10.57.0.25	N/A		
	Subnet Mask:	255.255.255.0	N/A		
	Gateway:	10.57.0.254	N/A		
	DNS1:	10.57.0.22	N/A		
	DNS2:	N/A	N/A		
	WINS:	N/A	N/A		
	Comportamiento				
	Hora de disponibilidad	5x12			
	Frecuencia de Actualizaciones	Segundo Jueves habil de cada mes			
	Criticidad:				
	Print Server - CJL Time				

Servidor					
Ubicación	**Elementos**	**Descripción**			
RACK PRINCIPAL	Nombre:	**CO-BO2K12RDP01**			
	Marca:	Microsoft Corporation			
	Modelo:	Virtual Machine			
	Procesador:	Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz, ~2.1GHz			
	Memoria RAM:	4 GB			
	Discos Duros:	Virtual de 127 GB			
	Tarjeta de Red:	Adaptador de red de Microsoft Hyper-V			
	Volúmenes de Disco:	Vol. C			
	Espacio Total:	127 GB			
	Espacio Disponible:	113,6 GB			
	Tolerancia a Fallos:	No			
	Modem / Dial Up:	SI: NO:X			
	Software				
	Sistema Operativo:	Microsoft Windows Server 2012 R2 Standard			
	Service Pack:	1			
	Windows Update	Si			
	Función:	RDP Clientes - Conexión Remota Helisa Niif y Recurso Humano 4			
	Servicios Instalados:	Administrador Licencias Escritorio Remoto			
	Versión IE:	11			
	Imagen de S.O.	SI: NO: X			
	Fecha de Creación				
	Red				
	Dominio y/o Árbol:	Mazars-CO.local	N/A		
	Protocolos:	TCP/IP	N/A		
	MAC Address	00-15-5D-32-14-0A	N/A		
	Dirección IP:	10.57.0.24	N/A		
	Subnet Mask:	255.255.255.0	N/A		
	Gateway:	10.57.0.254	N/A		
	DNS1:	10.57.0.22	N/A		
	DNS2:	N/A	N/A		
	WINS:	N/A	N/A		
	Comportamiento				
	Hora de disponibilidad	7x24x360			
	Frecuencia de Actualizaciones	Segundo Jueves habil de cada mes			
	Criticidad:				
	Conexión Remota Helisa Niif y Recurso Humano 4				

Servidor					
Ubicación	**Elementos**	**Descripción**			
RACK PRINCIPAL	Nombre:	**CO-BO2K12DC02**			
	Marca:	Microsoft Corporation			
	Modelo:	Virtual Machine			
	Procesador:	Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz, ~2.1GHz			
	Memoria RAM:	4 GB			
	Discos Duros:	Virtual de 127 GB			
	Tarjeta de Red:	Adaptador de red de Microsoft Hyper-V			
	Volúmenes de Disco:	Vol. C			
	Espacio Total:	127 GB			
	Espacio Disponible:	108 GB			
	Tolerancia a Fallos:	No			
	Modem / Dial Up:	SI: NO:X			
	Software				
	Sistema Operativo:	Microsoft Windows Server 2012 R2 Standard			
	Service Pack:	1			
	Windows Update	Si			
	Función:	Controlador de Dominio			
	Servicios Instalados:	AD - DHCP - DNS			
	Versión IE:	11			
	Imagen de S.O.	SI: NO: X			
	Fecha de Creación				
	Red				
	Dominio y/o Árbol:	Mazars-CO.local	N/A		
	Protocolos:	TCP/IP	N/A		
	MAC Address	00-15-5D-32-14-09	N/A		
	Dirección IP:	10.57.0.22	N/A		
	Subnet Mask:	255.255.255.0	N/A		
	Gateway:	10.57.0.254	N/A		
	DNS1:	10.57.0.22	N/A		
	DNS2:	127.0.0.1	N/A		
	WINS:	N/A	N/A		
	Comportamiento				
	Hora de disponibilidad	7x24x360			
	Frecuencia de Actualizaciones	Segundo Jueves habil de cada mes			
	Criticidad:				
	Servidor Controlador de Dominio				

ANEXO C

CARTA DE CUMPLIMIENTO

mazars

Calle 93 No. 15 – 40 Piso 4
Bogotá, Colombia
Tel: +57 (1) 256 30 04
www.mazars.com.co

Bogotá, 19 de abril de 2021

Ingeniero Alvaro Escobar Escobar.
Coordinador posgrados TIC.
Universidad Piloto de Colombia.
Cr9 No 45 A – 44 Segundo piso.

Referencia: Entrega proyecto de grado SIEM

Los alumnos de la de la especialización de seguridad informática Jhon Alexander Lopez Naranjo con numero de cedula de ciudadanía 81.717.413 y Edwin Ricardo Salamanca con numero de cedula de ciudadanía 1.072.659.667 de Chía Cundinamarca, realizaron la entrega del trabajo de grado titulado "GESTOR DE EVENTOS DE SEGURIDAD PARA MONITOREO DE LOS SERVIDORES WINDOWS DE LA EMPRESA MAZARS COLOMBIA SAS.", cuya herramienta se recibió a total satisfacción, los estudiantes realizaron la entrega de toda la documentación de implementación de dicha herramienta junto con el manual de instalación, es de resaltar que esta herramienta a sido de gran ayuda y que no ha generado ningún costo para la compañía.

Atentamente,

Carlos Andres Molano
Carl Partner Mazars Colombia

Mazars Colombia SAS
NIT: 830.055.030 – 9

ANEXO D

NDA MAZARS COLOMBIA

mazars

Calle 93 No. 15 – 40 Piso 4
Bogotá, Colombia
Tel: +57 (1) 256 30 04
www.mazars.com.co

ACUERDO DE CONFIDENCIALIDAD

Jhon Alexander Lopez Naranjo identificado con cedula de ciudadanía número 81.717.413 de Bogotá, y **Edwin Ricardo Salamanca Guerrero** identificado con cedula de ciudadanía número 1.072.659.557 de Chia Cundinamarca.

y

MAZARS COLOMBIA S.A.S. con domicilio principal en la Calle 93 No. 15- 40 oficina 402, con número de identificación tributaria (NIT).: 830.055.030-9, representada por **CARLOS ANDRES MOLANO CAMELO**, identificado con cédula de ciudadanía N.º 80.066.533,

De aquí en adelante designadas conjuntamente las "Partes" e individualmente la "Parte", acuerdan:

CONSIDERANDO:

1. Que las Partes desean participar en la celebración de un acuerdo de confidencialidad para ejecutar el procesamiento y tareas que permitan adelantar e implementar un SIEM de software libre para Mazars Colombia SAS trabajo realizado para cumplir con el proyecto de grado por parte de la Especialización de Seguridad Informática del corte ESI-44, en el marco de que las partes, en beneficio mutuo, revelaran información de carácter físico, instalaciones, técnico, análisis, proyecciones, especificaciones, sistemas de información, programación, datos, prototipos, secretos industriales y otra información de negocios o técnica relativa o necesaria para evaluar la posibilidad de llevar a cabo la implementación de un SIEM en Mazars Colombia, toda vez que no afecte en ningún sentido la integridad, disponibilidad y confidencialidad de los activos de información de la firma ni la seguridad del personal.

2. En conexión con la Transacción, las Partes pretenden intercambiar Información Confidencial (conforme se define abajo) y desean asegurarse de que toda la Información Confidencial recibida por una Parte ("Parte Receptora") de la otra ("Parte Reveladora"), sea tratada como confidencial y sea utilizada exclusivamente en relación con la Transacción. En cumplimiento del objeto del Acuerdo y dependiendo las circunstancias del desarrollo del mismo, las Partes podrán adquirir la calidad de Parte Receptora o Parte Reveladora, por lo tanto, las obligaciones de confidencialidad de este Acuerdo recaerán en la Parte que reciba la Información Confidencial, es decir, la Parte Receptora.

Las Partes celebran el presente Acuerdo de Confidencialidad ("Acuerdo"), en conformidad a los siguientes términos y condiciones:

1. OBJETO

El objeto de este Acuerdo es establecer las condiciones que deben ser observadas por las Partes en el intercambio de Información Confidencial.

2. INFORMACIÓN CONFIDENCIAL

2.1. "Información Confidencial" es toda información recibida por la Parte Receptora de la Parte Reveladora y/o sus Afiliadas (como se define más abajo), directa o indirectamente: (i) en forma tangible, incluyendo, pero sin limitarse a, documentos escritos, gráficos, visuales o información virtual contenida en programas de computadora o mantenida en archivos de almacenamiento electrónico; o (ii) en virtud de acceso de la Parte Receptora a objetos tangibles, incluyendo, pero sin limitarse a, documentos, prototipos, muestras, proyectos, o equipos e información relacionada a patentes, aplicaciones de patentes, investigación, planes de negocios y/o productos, know-how, propuestas técnicas o comerciales, productos, desarrollos, invenciones, procesos, diseños, fórmulas, estudios de ingeniería y mercados, información regulatoria, datos y análisis, reactivos,

materiales biológicos, fórmulas químicas, contratos con terceros, servicios, consumidores, marketing o finanzas de la Parte Reveladora.

2.2. Para efectos del presente Acuerdo, el término "Afiliadas" significa las sociedades o asociaciones que, directa o indirectamente, controlan, son controladas o están bajo control común de una de las Partes. El término "control" significa la titularidad de al menos cincuenta por ciento (50%) del capital social y/o derechos de voto.

3. EXCLUSIONES

3.1. No será considerada como "Información Confidencial" la información que: a) era de dominio público en el momento de la divulgación para la Parte Receptora, o se convierta en dominio público, sin que para tal fin haya participado la Parte Receptora; b) estaba en posesión de la Parte Receptora en el momento de la revelación, como lo demuestre un documento escrito; c) ha sido legítimamente recibida por la Parte Receptora de un tercero, que, bajo el mejor conocimiento de la Parte Receptora, esté autorizado a revelar dicha información sin incumplir con obligación alguna de sigilo ante la Parte Reveladora; d) fue desarrollada independientemente por la Parte Receptora sin ninguna mención o referencia a la Información Confidencial, como lo demuestre un documento escrito; o; e) la Parte Reveladora haya autorizado previamente por escrito a la Parte Receptora a divulgar o revelar a terceros.

4. TRATAMIENTO DE LA INFORMACIÓN CONFIDENCIAL

4.1. La Parte Receptora se compromete a no revelar, total o parcialmente, la Información Confidencial a ninguna persona o entidad que no esté directamente involucrada en la Transacción, sin el consentimiento previo por escrito de la Parte Reveladora. Sin embargo, queda estipulado que la Parte Receptora podrá revelar dicha Información Confidencial, sin la necesidad del consentimiento de la Parte Reveladora si:

a) la divulgación es hecha hacia los empleados, socios, consultores, agentes, apoderados, directores, administradores o ejecutivos de la Parte Receptora ("Representantes"), o hacia las Afiliadas que necesitan conocer dicha Información Confidencial con el fin de evaluar o participar en las discusiones relacionadas con la Transacción; y

b) dichos Representantes han sido informados de las obligaciones de confidencialidad de la Parte Receptora, y a las cuales también están sujetos, debido a la obligación profesional de mantener como confidencial toda la información que les pueda ser revelada por la Parte Receptora, o tengan conocimiento de las obligaciones de confidencialidad de la Parte Receptora a través de documento que contenga restricciones sobre el uso y divulgación sustancialmente similares a las contenidas en este Acuerdo.

4.2. La Parte Receptora no deberá utilizar la Información Confidencial de la Parte Reveladora para cualquier otro propósito que no esté en conexión con la Transacción. La Parte Receptora no podrá, sin el previo consentimiento por escrito de la Parte Reveladora, utilizar la Información Confidencial de la Parte Reveladora para desarrollar sus propios negocios o para competir con la Parte Reveladora.

4.3. La Parte Receptora no podrá copiar, duplicar, reproducir o grabar de ninguna forma, ninguna Información Confidencial sin el consentimiento previo, por escrito, de la Parte Reveladora, excepto si esto es necesario para la circulación entre las personas que soliciten Información Confidencial, y que estén sujetas a un compromiso de confidencialidad.

4.4. Sin limitarse a cualquier otra obligación aquí contemplada, la Parte Receptora deberá tratar la Información Confidencial de la Parte Reveladora con el mismo grado de confidencialidad y celo con que manejaría su propia información. Se enfatiza que en ningún caso la Parte Receptora podrá dejar de adoptar criterios razonables de cuidado cuando esté utilizando la Información Confidencial de la Parte Reveladora. La Parte Receptora se compromete a asegurar el almacenamiento adecuado y seguro para todos los materiales confidenciales, escritos o electrónicos, que estén en su posesión.

Calle 93 No. 15 – 40 Piso 4
Bogotá, Colombia
Tel: +57 (1) 256 30 04
www.mazars.com.co

4.5. Cualquier uso o divulgación no autorizados de Información Confidencial (conforme a lo dispuesto en el presente Acuerdo) por parte de los Representantes o Afiliadas de la Parte Receptora se considerará violación de este Acuerdo, como si la propia Parte Receptora no hubiera cumplido directamente con los términos aquí previstos.

4.6. Salvo lo expresamente permitido en este Acuerdo, toda y cualquier Información Confidencial divulgada como resultado de este Acuerdo seguirá siendo de propiedad o de uso exclusivo de la Parte Reveladora.

5. DIVULGACIÓN.

5.1. Ninguna Parte podrá revelar los términos o la existencia del presente Acuerdo, ni de cualquier transacción u operación comercial eventualmente firmada entre las Partes, con relación a discusiones y negociaciones todavía en curso, sin el previo consentimiento de la otra Parte, siendo que dicho consentimiento no se podrá rechazar injustificadamente.

5.2. Si la Parte Receptora es obligada legalmente a proporcionar Información Confidencial en cumplimiento de una orden judicial, administrativa o arbitral, la Parte Reveladora deberá ser notificada, por escrito, como máximo 03 (tres) días hábiles posteriores a tener conocimiento de tal orden, con el fin de permitir que la Parte Reveladora tome todas las medidas legales que entienda necesarias. La Parte Receptora deberá, en cumplimiento de dicha orden judicial, administrativa o arbitral, proporcionar solamente la Información Confidencial que se solicite y debe realizar sus mejores esfuerzos para obtener un trato confidencial de la información divulgada.

6. DEVOLUCIÓN DE LA INFORMACIÓN CONFIDENCIAL

6.1. Mediante solicitud por escrito de la Parte Reveladora, en cualquier momento, durante la vigencia del presente Acuerdo, la Parte Receptora deberá, en un plazo de 30 (treinta) días contados a partir de la recepción de la solicitud, devolver a la Parte Reveladora o destruir toda la Información Confidencial, incluyendo informes, resúmenes, notas, copias o extractos de la Información Confidencial generada por la Parte Receptora. Mediante mencionada solicitud, la Parte Receptora deberá, a sus propias expensas, borrar de sus sistemas toda la Información Confidencial mantenida en medios electrónicos y descartar todos los materiales y muestras que no se utilicen, dándoles la finalidad determinada por la Parte Reveladora.

7. VIGENCIA

7.1. El presente Acuerdo entra en vigencia desde su firma y tendrá un término de duración igual al de las relaciones comerciales y de servicios entre las Partes y cinco (5) años más después de la terminación.

8. DISPOSICIONES GENERALES

8.1. Nada en este Acuerdo se entenderá como participación de las Partes en ninguna relación comercial entre sí o con terceros, ni tampoco como obligación de llevar a cabo negocios o celebrar cualquier otro acuerdo. Cualesquiera obligaciones en este sentido dependerán de las negociaciones específicas y de la firma de los contratos correspondientes.

8.2. Todas las notificaciones bajo este Acuerdo deberán enviarse a las direcciones indicadas en el preámbulo.

8.3. Todos los derechos y obligaciones aquí previstos no podrán ser cedidos o transferidos a ninguna persona, sin el previo consentimiento por escrito de la otra Parte.

8.4. El no ejercicio o atraso en el ejercicio de cualquier derecho, por cualquiera de las Partes, no se considerará como una renuncia a tales derechos, siendo que tal renuncia solamente se operará a través de nuevo instrumento firmado, por escrito, entre ambas Partes.

8.5. Si alguna de las disposiciones contenidas en el presente Acuerdo es, en algún momento, considerada como nula, ilegal o no ejecutable, las restantes disposiciones permanecerán en pleno vigor y efecto, quedando

obligadas las Partes, en este caso, a realizar sus mejores esfuerzos para subsituir la disposición inválida y no ejecutable por una nueva disposición válida y eficaz.

8.6. Este Acuerdo constituye la voluntad íntegra de las Partes en relación con el objeto aquí previsto y obliga a las Partes y a sus sucesores a cualquier y solo podrá ser modificado por documento escrito y es firmado por ambas Partes.

8.7. El incumplimiento del compromiso de confidencialidad establecido en este Acuerdo dará lugar a la responsabilidad de la Parte infractora de indemnizar los daños causados a la otra Parte sin exceder de 30 salarios mínimos legales mensuales vigentes. las Partes no serán responsables por lucros cesantes o daños indirectos en consecuencia del incumplimiento de este Acuerdo. La Parte infractora se compromete a practicar todos los actos necesarios para impedir o restringir la divulgación de la Información Confidencial.

9. LEY APLICABLE Y FORO

9.1. Este acuerdo se regirá e interpretará de conformidad con la legislación colombiana aplicable y cualquier disputa que surja de este Acuerdo o que guarde relación con éste será resuelta definitivamente de acuerdo con la jurisdicción de la ciudad de Bogotá D.C., Colombia.

10. NOTIFICACIONES

10.1 Todas las comunicaciones y/o notificaciones que deban surtirse en desarrollo o con ocasión al presente Contrato se entenderán válidamente efectuadas al correo electrónico de las Partes y/o a la dirección física que se indica a continuación:

Mazars

Dirección: Cra 93 # 15–40 piso 4 en la ciudad de Bogotá D.C.
Correo electrónico: carlos.molano@mazars.com.co

Estudiantes

Jhon Alexander Lopez Naranjo
Correo electrónico: jhonalex031@hotmail.com
Edwin Ricardo Salamanca
Correo electrónico: Ersg90z@gmail.com

Y, por estar justas y acordadas, las Partes firman el presente Acuerdo el 19/04/2021 en la ciudad de Bogotá D.C.

ESTUDIANTES

Jhon Alexander Lopez Naranjo
C.C No. 81.717.413

Edwin Ricardo Salamanca Guerrero
C.C No. 1.072.659.667

MAZARS COLOMBIA S.A.S

Carlos Andres Molano Camelo
C.C. No. 80.066.533
Representante legal