TRABAJO DE GRADO

PROPUESTA DE BUENAS PRACTICAS DE EVENTOS A MONITOREAR EN UN SIEM PARA COOPERATIVAS FINANCIERAS EN COLOMBIA DANDO CUMPLIMIENTO A LA CIRCULAR 007

JORGE FABIAN MARIÑO GARCIA

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2020

TRABAJO DE GRADO

PROPUESTA DE BUENAS PRACTICAS DE EVENTOS A MONITOREAR EN UN SIEM PARA COOPERATIVAS FINANCIERAS EN COLOMBIA DANDO CUMPLIMIENTO A LA CIRCULAR 007

JORGE FABIAN MARIÑO GARCIA

Trabajo de grado presentado para optar al título de Especialista en Seguridad de la Información

Docente

DIEGO OSORIO REINA
M.Sc.

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2020

TABLA DE CONTENIDO

Pág.

1. INTRODUCCIÓN

En la actualidad se detectado que el cibercrimen va en aumento y más con el crecimiento y desarrollo de la tecnología, el sector financiero es el principal vector de ataque ya que genera rentabilidad a los cibercriminales, este sector se ha tenido que ir equipando de herramientas de seguridad informática para lograr mitigar y no dejar materializar los graves daños económicos que se pueden generar, ya sea con un software de antivirus, un DLP (*Data Loss Prevention*), un IPS (*Intrusion Prevention System*), análisis de vulnerabilidades, firewall y actualizaciones en los sistemas, sin embargo el tener varias herramientas ha resultado insuficiente ya que se puede perder la visión general por tener que verificar diferentes consolas de administración, por lo que se hace necesario tener un centralizador de eventos o un SIEM (*Security Information and Event Manager*) en donde se pueda monitorear los eventos que están ocurriendo en la infraestructura tecnológica, además los SIEM ayudan a cumplir políticas de regulación y control impuestas por entes internacionales.

En Colombia, las entidades financieras por estar sometidas a inspección y vigilancia de la Superintendencia Financiera, están en el deber de cumplir con diferentes circulares y sus lineamientos expresamente señalados, se tiene como ejemplo la circular 007 de 2018 - requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad, donde estipula dentro de sus lineamientos que debe contar con la ya mencionada herramienta SIEM sobre la cual se desarrolla la propuesta de buenas prácticas a monitorear de diferentes sistemas de información enfocándose en las entidades del sector financiero, en especial en las cooperativas financieras que para el caso de Colombia son 181 las reguladas por la Superintendencia.

En la propuesta de buenas prácticas a monitorear se realizará una prueba de concepto de los resultados entregados en un ambiente de pruebas.

2. GENERALIDADES

1. LÍNEA DE INVESTIGACIÓN

De acuerdo con las necesidades planteadas, el proyecto, se enfoca en la línea de investigación "***Software Inteligente Y Convergencia Tecnológica***" avalada por la Universidad Católica de Colombia y el grupo de Investigación GISIC. Este trabajo busca proponer las buenas prácticas de eventos a monitorear en un SIEM para cooperativas financieras bajo políticas de la Superintendencia Financiera de Colombia enmarcadas en la circular 007 de 2018.

2. PLANTEAMIENTO DEL PROBLEMA

Teniendo en cuenta la Circular 007 de 2018, expedida por la Superfinanciera de Colombia, la cual consagra los requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad, se evidencia que esta no especifica como obligación de que activos, dispositivos o software de seguridad monitorear por medio de la plataforma SIEM; por el contrario, deja en manos de la Entidad Financiera la interpretación sobre el manejo que se debe llevar a cabo para el monitoreo de los ya mencionados conceptos.

2.2.1. ANTECEDENTES DEL PROBLEMA

El principal objetivo de los cibercriminales es el sector de servicios financieros por sus lucrativas ganancias que les puede dejar cada ataque informático que pueda llegar a ser satisfactorio.
Entre noviembre de 2017 y abril del 2019, las instituciones bancarias y financieras fueron el objetivo del ciberdelito, así lo confirma el Reporte de Seguridad: "El mercado de los ataques al sector financiero" de Akamai Technologies, presentado en Latinoamérica, este reporte registró 4 mil millones de ataques web en todos los sectores durante el periodo, algo más del 9 % que es igual a 411 millones de los ataques que afectó al sector de servicios financieros.

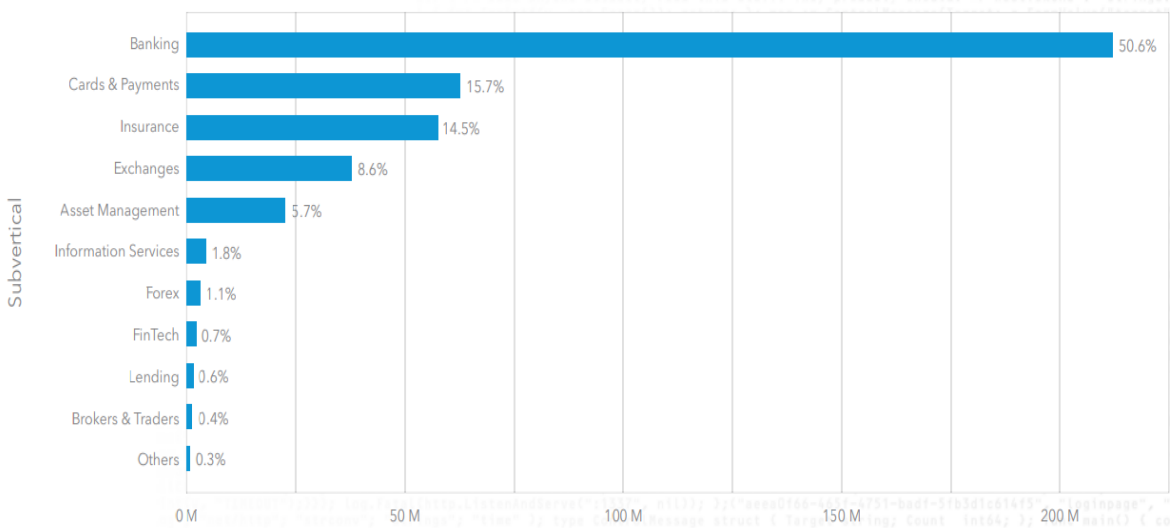


Figura 1. Subsectores vs ataques del sector financiero. Tomado de: Financial Services Attack Economy. Vol.5 pag.15

El estudio detectó más de 57 mil millones de intentos de inicio de sesión maliciosos, 3 mil millones fueron a instituciones bancarias. Estados Unidos, China, Malasia, Brasil y Alemania fueron los principales puntos de origen de estos ataques, pero tenían como destino países de América Latina. En la figura categorizada por países de América Latina, Colombia se encuentra en el puesto 26 siendo fuente de ataque de abusos de credenciales (Figura 2) y en el puesto 47 de fuentes de ataque de aplicaciones Web (Figura 3).[1]

Top 10 Source Countries – Americas

COUNTRY	MALICIOUS LOGINS	GLOBAL RANK
United States	18,542,844,141	01
Brazil	3,197,885,812	03
Canada	2,378,887,475	04
Colombia	368,068,555	26
Ecuador	315,523,060	27
Chile	315,318,808	28
Argentina	287,502,033	31
Mexico	242,785,728	33
Venezuela	146,584,731	43
Dominican Republic	63,667,312	61

Figura 2. Credential Abuse Attack Sources — Americas November 2017 – April 20191. Tomado de: Financial Services Attack Economy. Vol.5 pag.31

[1] Financial Services Attack Economy. Akamai Intelligent Security Starts at the Edge. Vol 5, Issue 4. On-line

Top 10 Source Countries – Americas

COUNTRY	MALICIOUS LOGINS	GLOBAL RANK
United States	1,045,462,552	01
Brazil	173,458,367	05
Canada	84,886,941	11
Belize	82,136,387	12
Panama	21,618,465	29
Mexico	18,129,828	33
Argentina	11,654,146	41
Colombia	8,271,724	47
Venezuela	6,139,547	56
Peru	5,474,860	62

Figura 3. Web Application Attack Sources — Americas November 2017 – April 20191. Tomado de: Financial Services Attack Economy. Vol.5 pag.34

2.2.2. PREGUNTA DE INVESTIGACIÓN

¿Qué eventos se deben tener en cuenta a monitorear con un SIEM para el cumplimiento de los lineamientos estipulados en la circular 007 de la Superintendencia Financiera de Colombia?

2.2.3. VARIABLES DEL PROBLEMA

Se determinaron las variables dependientes o independientes que puedan afectar el desarrollo de la investigación.

- Variable dependiente 1: Expedición de una nueva circular por parte de la superintendencia Financiera de Colombia que llegue a reemplazar o anular la circular 007.
- Variable dependiente 2: Modificaciones en el contenido de la circular que cambie el software solicitado para cumplimiento.
- Variable independiente: Creación de una guía de eventos a monitorear de un SIEM para cumplimiento de la circular 007.

3. JUSTIFICACIÓN

En Colombia los delitos informáticos los encabezan los ataques al sector financiero según Víctor Manuel Muñoz, Alto Consejero para la Transformación Digital (de la Presidencia de la República), durante el encuentro de equipos de respuesta a incidentes cibernéticos (CSIRTs) en el foro de Ciberseguridad dio detalles de la afectación que hay en Colombia por cuenta de los ataques cibernéticos.

Muñoz dio a conocer que los sectores económicos contra los que más arremeten son el Financiero y el de Telecomunicaciones, con un 39,6% y 25,5% de los ataques respectivamente, siguiendo el sector Gobierno con 15,4%; Industria, con 9,5%; Retail, con 6,4% y el Energético, con un 3,6% de los ataques[2]. (Grafico 1)

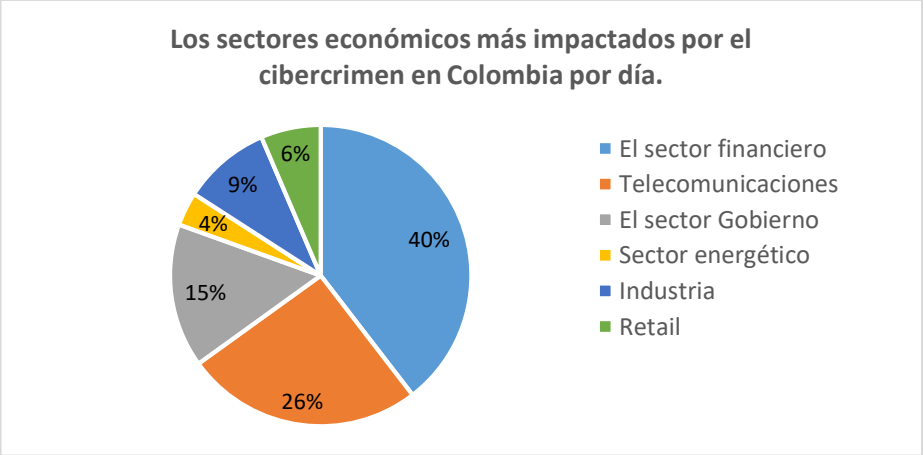


Gráfico 1. Sectores Afectados Por El Cibercrimen En Colombia

Según fuentes de la Fiscalía General de la Nación informa Asobancaria, durante 2018 se registraron en Colombia más de 20.000 denuncias por delitos informáticos a entidades bancarias. Dentro de las tipologías más usadas está el código malicioso o malware, la suplantación de identidad y la suplantación de sitios web para extraer información financiera (phishing). Durante el año 2018 el 58% del total de las operaciones, monetarias y no monetarias, se realizaron a través de canales digitales y en el país se registraron 11.524 incidentes cibernéticos con un incremento del 42% frente al 2017.

Datos como estos muestran lo rentable que puede ser el cibercrimen en Colombia si no se protegen las entidades frente a las constantes amenazas y que no basta solo tener una consola de antivirus para detectar el malware, o un DLP para

[2] MUÑOZ, Victor Manuel. Foro de Ciberseguridad y encuentro de equipos de respuesta a incidentes cibernéticos (CSIRTs). 2018.

detectar una fuga de datos o un firewall para generar bloqueos de red; si no que es necesario un equipo de respuesta a incidentes (CSIRT) que este en el monitoreo constante de nuestra infraestructura como servidores, equipos de redes, aplicaciones y servicios de T.I. Motivo por el cual la Superintendencia Financiera de Colombia publica la circular 007 de 2018 - requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad la cual es de cumplimiento obligatorio para entidades financieras y pasarelas de pago dentro de la cual se exponen los lineamientos para realizar una adecuada administración de riesgo de ciberseguridad y proteger la información de los consumidores del sistema financiero, por tal motivo se plantea esta propuesta de diseño de parametrización de un SIEM bajo el marco del cumplimiento de la circular 007[3].

Teniendo en cuenta que la circular 007 no menciona un gran detalle en cuanto a que activos, servicios o software se debe monitorear para realizar una adecuada parametrización, se ha basado en la recolección de logs de los dispositivos solicitados en la circular 042 de 2012 y adicional en los ataques más utilizados según Mitre Att&ck al sector bancario.

4. HIPÓTESIS

Teniendo en cuenta la experiencia en el área donde se ha tenido la oportunidad de trabajar con diferentes cooperativas financieras en Colombia se especula que algunas de ellas no tienen la suficiente fuerza económica o simplemente no le dan la importancia necesaria para contratar un servicio de SOC (Security Operation Center - Centro de Operaciones de Seguridad) que esté a cargo del monitoreo constante de la infraestructura tecnológica o tampoco con los dispositivos de última generación que estén a la vanguardia de las nuevas amenazas que surgen en el día a día, o lograr evidenciar los posibles ataques o fallos de seguridad de las entidades, algunos cuentan con un SIEM pero no conocen todas las ventajas que pueden tener con este software de seguridad o simplemente no lo tienen bien parametrizado para tener una visión general de lo que ocurre en la infraestructura, en las diferentes aplicaciones o software de seguridad que tenga la entidad, motivo por el que la superintendencia procede a implantar estos controles mencionando los requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad por medio de la circular 007.

[3] Asobancaria. Informe Internacional de Regulación- edición N° 31. Developer Increnta. COMUNICADO DE PRENSA 13 / 10 de mayo de 2019.

3. OBJETIVOS

1. OBJETIVO GENERAL

- Diseñar una propuesta de buenas prácticas de eventos a monitorear en un SIEM para las cooperativas financieras en Colombia dando cumplimiento a la circular 007.

2. OBJETIVOS ESPECÍFICOS

- Identificar fuentes de información y técnicas utilizadas por ciberdelincuentes.
- Interpretar los lineamientos de la circular 007 de la Superintendencia Financiera de Colombia.
- Diseñar la propuesta de eventos a monitorear según fuentes de información y técnicas de los ciberdelincuentes.
- Implementar en un ambiente de pruebas algunos de los eventos a monitorear propuestos.

4. MARCOS DE REFERENCIA

1. MARCO CONCEPTUAL

Este capítulo presenta los conceptos fundamentales necesarios para el diseño del esquema de parametrización de un SIEM para cooperativas financieras bajo políticas de la Superintendencia Financiera de Colombia partiendo de la definición de seguridad de la información, de sus 3 pilares y de las herramientas más utilizadas en entidades del sector financiero que ayudan a mitigar los riesgos que diario se pueden presentar.

4.1.1 SEGURIDAD DE LA INFORMACIÓN

Según Sánchez se entiende por seguridad de la información al "conjunto de sistemas y procedimientos que garantizan: la confidencialidad, la integridad y la disponibilidad de la información"[4].

.

La seguridad de la información es un factor indispensable para las empresas o entidades sin importar su fin o misión, ya que con los avances tecnológicos que se ven a diario es necesario cuidar tanto nuestros sistemas como concientizar al personal de cada área que día a día se ven comprometidos en los ataques o posibles amenazas[5].

.

4.1.2 PILARES DE LA SEGURIDAD DE LA INFORMACIÓN

Disponibilidad y accesibilidad de los sistemas y datos: Según Areitio en 2008 "Solo para uso autorizado, es un requisito necesario que garantiza que el sistema trabaje puntualmente, con prontitud y que no se deniegue el servicio a ningún usuario autorizado"[6].

Integridad: "Se encarga de garantizar que la información del sistema no haya sido alterada por usuarios no autorizados mientras se almacena, procesan o transmiten así evitando la perdida de consistencia" [6]

---

[4] SÁNCHEZ SOLÁ, A. P. 2013. Diseño de un sistema de gestión de la seguridad de la información para un comercio electrónico basado en la ISO 27001 para pequeñas y medianas empresas en la ciudad de Quito [on-line]. Tesis-Carrera de ingeniería de sistemas y computación. p. 15

[5] FERNÁNDEZ GRANADOS, J. E.; HERRERA KAIRUZ, J. H.; GARCÍA, J. C. Implementación de un security information and event management –siem– en el comando de la armada nacional [on-line]. Dirección de tecnologías de la información y las comunicaciones. Tesis - Especialización en Seguridad Informática. p. 18

[6] YAGUAL DEL VALLE, C.; CHILÁN RODRÍGUEZ, L. 2014. Análisis para la integración de un Sistema de Gestión de Seguridad de Información (SGSI) ISO-27001 Utilizando OSSIM para empresa Industrial [on-line]. Tesis- Ingeniería de sistemas con mención de Telemática. p. 7.

Confidencialidad de datos: “Es el requisito que intenta que la información privada o secreta no se revele a individuos no autorizados. La protección de la confidencialidad se aplica a los datos almacenados durante su procesamiento, mientras se transmiten y se encuentran en tránsito” [6].

4.2 CLASIFICACIÓN DE HERRAMIENTAS PARA GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN

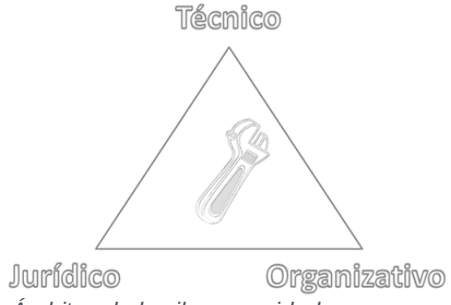


Figura 4. Ámbitos de la ciberseguridad en una empresa.

Para alcanzar un adecuado nivel de ciberseguridad en la empresa, se deberá de atender no solo el ámbito técnico de la seguridad, sino también el jurídico y el organizativo.

Técnico: se refiere a los sistemas, los dispositivos, el software y cualquier elemento, mecanismo o dispositivo, que permite implementar seguridad.

Jurídico: se refiere al cumplimiento de la legislación en materia de ciberseguridad, que afecta a las empresas, en función de su actividad, del sector al que pertenecen o de los datos que utilizan en sus procesos de negocio.

Organizativo: se refiere al cumplimiento de normativas relativas a seguridad, como normas ISO, PCI, políticas de seguridad impartidas por cada entidad o por entidades reguladoras, buenas prácticas, etc. Existe una gran interrelación entre estos ámbitos, en especial, entre el ámbito jurídico y organizativo, puesto que son muy similares y se complementan y a su vez se apoyan en el ámbito técnico[7].

[7] CHINE LÓPEZ, J. 2014. Tipos de herramientas básicas para garantizar la ciberseguridad en la empresa [on-line].

4.3 SOFTWARE O APLICACIONES PARA GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN

4.3.1. IPS (Intrusion Prevention System)

Es un software o hardware que protege redes de amenazas conocidas o no bloqueando ataques Estos dispositivos o software son encargados de revisar el tráfico de red con el propósito de detectar y responder a posibles ataques o intrusiones. Las acciones más usuales son descartar los paquetes de un ataque o la modificación para anular el objetivo malintencionado del atacante. Se podría decir que se clasifican en dispositivos proactivos, debido a que reaccionan de forma automática a situaciones anómalas.

4.3.2 Firewall

Son soluciones para organizaciones que desean proteger varios sistemas con el mismo mecanismo. Ofrecen servicios tales como bloqueo de paquetes y es posible utilizarlos como herramienta de análisis del comportamiento de sistema y la red, herramienta de análisis forense, defensa contra virus, gusanos y spam[8].

4.3.3 DLP – Data Loss Prevention

Tiene como objetivo evitar la fuga de información ya sea a través de puertos o dispositivos u otros canales de comunicación como Correo electrónico, mensajería instantánea, redes sociales o la nube. Las soluciones DLP, incluyen un conjunto de tecnologías que persiguen tres objetivos claves[9].

4.3.4 Antivirus

Es un software programado con el fin de realizar detecciones de otros software diseñados de manera malintencionada para dañar sistemas, también puede realizar tareas de borrado del virus para hacer una desinfección del equipo, es necesario siempre tener el antivirus actualizada ya que los virus siempre intentaran estar un paso más adelante y es posible que estos no sean detectados por el antivirus, cuando se conoce de la existencia de un nuevo virus los fabricantes se apresuran a sacar actualizaciones en sus bases de firmas para detectarlos.

---

[8] RAMÍREZ LUNA, H. E.; MEJIA MIRANDA, J. 2015. Propuesta de infraestructura técnica de seguridad para un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT) [on-line]. ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica. Vol. 4 N°1, p. 9.

[9] HEINERT VILLACIS, L. A. Implementación De Una Solución Data Loss Prevention (DLP) En Una Empresa Con Actividades De Servicios Alimenticios [on-line]. Tesis- Magister en seguridad informática aplicada. p. 3.

4.3.5 Hardening

La terminología fortalecimiento (Hardening) se refiere al proceso de asegurar un sistema mediante la reducción de vulnerabilidades al mínimo, esto se logra eliminado software, servicios, usuarios y así como cerrando puertos que no estén en uso, además de muchos otros métodos y técnica. Es importante mencionar que tales mecanismos de seguridad perimetral no protegen de ataques cuyo tráfico no pase por ellos, de copias ilegales de información en medios de almacenamiento físico, de ataques de ingeniería social, de virus informáticos en archivos o software y de fallos de seguridad de los servicios y protocolos cuyo tráfico no se esté analizado o esté permitido[10].

4.3.6 Servidores de Gestión de Roles y Accesos

Los servidores de gestión de accesos utilizan el protocolo LDAP, siglas de *Lightweight Directory Access Protocol*. LDAP es un protocolo a nivel de aplicación que permite el acceso a un Servicio de Directorio o DS. El DS es una aplicación que almacena y organiza la información de los usuarios de una red y sobre los recursos de red que permite a los administradores gestionar el acceso de usuarios a los recursos de esta.

LDAP almacena la información de autenticación, usuario y contraseña, y es utilizado para ello, aunque también es posible almacenar otra información como datos de usuario, permisos o certificados[11].

4.3.7 SIEM

Gestión de Eventos e Información de Seguridad (*Security Information and Event Management*) es una categoría de software informático que tiene como objetivo brindar a las organizaciones información útil sobre potenciales amenazas de seguridad, a través de la estandarización, correlación de datos y priorización de amenazas. Esto es posible mediante un análisis centralizado de datos (Logs), obtenidos desde múltiples sistemas, que incluyen aplicaciones antivirus, firewalls, bases de datos, diferentes sistemas operativos y soluciones de prevención de intrusiones.

Un SIEM trabaja con un sistema de correlación para que el CSIRT (*Computer Security Incident Response Team / equipo de respuesta a incidentes informáticos*)

[10] Grupo Smartekh. ¿Qué es Hardening? [on-line]. 2012.
[11] ARACIL ORDUÑA, E. 2019. Desarrollo y Despliegue de Servicios Web integrados mediante un Servidor de Autenticación único basado en Roles. Universidad Autónoma De Madrid. Escuela Politécnica Superior. Pag. 8.

pueda gestionar de forma proactiva las potenciales vulnerabilidades desde un SOC (*Security Operations Center / Centro de Operaciones se Seguridad*), protegiendo a las empresas de devastadoras filtraciones de datos o información. Piénselo como un lente que agudiza su visión sobre la situación general, para ayudarlo a enfocar los esfuerzos de su equipo hacia donde puedan tener mayor impacto.

Con esta última herramienta será el enfoque con el que se desarrollará la propuesta de diseño y con la que se cumplirá los puntos de la circular 007 de la superintendencia.

4.3.7.1 Arquitectura de los Sistemas SIEM

Se debe tener en cuenta aquellas características que deben tener las herramientas SIEM y que ayudan con las funciones de almacenamiento, análisis y eliminación de datos de logs, que no deben impactar de manera alguna los recursos tecnológicos ni la integridad de los datos, para que las investigaciones forenses basadas en los mismos no se vean afectadas. Entre estas características se encuentran, la recolección de datos y la conversión de datos. La recolección de datos consiste en obtener los registros de datos mediante un software denominado colector también conocido como agente, que se encuentra instalado en las fuentes de logs, se describen como todo aquel dispositivo, sistema operativo, aplicación o cualquier sistema de información que generen registros de datos (logs)[12].

[12] AVELLA CORONADO, J. D.; CALDERON BARRIOS, L. F.; MATEUS DÍAS, C. A. 2015. Guía Metodológica para la gestión centralizada de registros de seguridad a través de un siem [on-line]. Tesis- Especialista en Seguridad en Redes. p. 17.

Figura 5. Arquitectura de los sistemas SIEM12. Tomada de: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81267/6/ljasomarTFM0618memoria.pdf

- **Recolección y gestión de logs**. Los sistemas SIEM cuentan con la capacidad de adquirir datos de diversas fuentes y almacenarlos en una base de datos centralizada. Esta base de datos inicialmente realiza un análisis sintáctico del dato, normalizándolo, ya que los distintos sensores (elementos fuente) envían el dato en diferentes formatos. Hay que tener presente que estos sensores normalmente son de naturalezas muy diversas (equipos con diferentes sistemas operativos, sistemas de infraestructura de red como switches, routers, firewalls, sistemas de detección de intrusos, etc.). Seguidamente el SIEM, normalmente, almacena todos los datos normalizados, los organiza y les aplica una política de retención para satisfacer los requerimientos de la organización o regulaciones vigentes. Estos datos también son utilizados en tiempo real, para analizar la salud y seguridad de estos sensores y equipos que se encuentran en nuestra organización proporcionando datos al SIEM (Figura 5)[13].

- **Cumplimiento de las regulaciones vigentes de la seguridad de la información.** Todos los sucesos generados desde los sistemas que están siendo recolectados como logs, pueden ser analizados bajo filtros y reglas para auditar y validar el cumplimento de los requerimientos impuestos por la organización en su política de seguridad y satisfacer estos requisitos de seguridad exigibles y los asociados a las regulaciones vigentes[13].

- **Capacidad forense.** Posibilidad de analizar los datos y alertas para determinar

[13] JASO MARQUINA, L. M. & LOZANO MERINO, M. A. 2018. Ventajas e implementación de un sistema SIEM [on-line]. Tesis- Máster en Seguridad de las tecnologías de la información y de las telecomunicaciones.

el origen de las incidencias de seguridad y hacer frente a las mismas[13].

- **Agregación y correlación de eventos de seguridad en tiempo real.** El SIEM establece relaciones entre diferentes sucesos, estudiando la frecuencia de los sucesos, el horario de estos, etc., para establecer la veracidad del incidente (eliminar falsos positivos) y poder unir todos estos sucesos y verlos como un único incidente, lo cual ayuda a su tratamiento. El motor de correlación puede considerar otros eventos diferentes al investigado para proporcionar una fotografía más completa de la verdadera causa del problema[13].

- **Capacidad de respuesta. Acciones reactivas.** Una vez que el SIEM es capaz de identificar el incidente de seguridad tras recolectar y adecuar los logs y correlacionarlos para estar seguro de que el incidente es cierto, algunos SIEM cuentan con la capacidad de reaccionar automáticamente frente a dichos incidentes tratando de mitigar el problema. Por ejemplo, una vez confirmada la causa del problema podríamos apagar la boca del switch desde donde se genera el problema, si es posible y adecuado, o filtrar el acceso a esa IP determinada desde donde se origina el incidente, etc.

- **Seguridad en los equipos clientes.** Los sistemas SIEM tienen la capacidad de monitorizar la salud y el estado de un equipo final. Por ejemplo, pueden monitorizar el estado de los recursos del sistema de un servidor, desktop u otros, los procesos que se están ejecutando, escanear sus vulnerabilidades, monitorizar el estado de sus antivirus, etc., mediante la arquitectura HIDS (*Host-based intrusion detection system / Sistema de detección de intrusos basado en un host*).

- **Monitorización y alertas de seguridad.** Los sistemas SIEM tienen la capacidad de visualizar, monitorizar y administrar todos los eventos de seguridad. Son capaces de analizar automáticamente todos los eventos y solamente notificar de aquellos que realmente son más relevantes. Se debe tener presente la gran cantidad de datos que proporcionan los sensores al sistema SIEM y esta debe ser capaz de alertar solamente de aquellos que sean realmente significativos, se trata de “encontrar la aguja dentro del pajar”.

- **Presentación de Informes de seguridad**. Capacidad de presentación de informes ejecutivos y técnicos

2. MARCO TEÓRICO

La seguridad de la información es un factor indispensable en el día a día de las empresas, todos los días se presentan incidentes de seguridad en los diferentes sectores de la industria, los avances tecnológicos obligan a las empresas a implementar nuevos sistemas de seguridad y a mejorar los controles y así mitigar las inminentes amenazas. Toda información de cualquier tipo es valiosa para su propietario, por esto surge la necesidad de protegerla ante peligros potenciales. Actualmente la información debe cumplir con los 3 pilares de la información, debe estar siempre disponible, no modificada y salvaguardada de una manera segura.

Gracias a entidades de control y vigilancia en Colombia se puede disminuir los índices de daños por los cibercriminales y garantizar los 3 pilares de la seguridad de la información, estos grupos o entidades las conforma el grupo de respuesta a emergencias cibernéticas de Colombia (coICERT) del Ministerio de defensa Nacional, el comando conjunto cibernético (CCOC) del comando general de las fuerzas militares de Colombia, el centro cibernético policial (CCP) de la policía nacional de Colombia, el equipo de respuesta a incidentes de seguridad informática de la policía nacional (CSIRT PONAL), para el caso de las entidades del sector bancario están regidas a la superintendencia financiera de Colombia quien constantemente está en la implementación de controles, políticas y publicación de circulares de estricto cumplimiento.

3. MARCO JURÍDICO

Superintendencia Financiera de Colombia ha emitido circulares donde se da una serie de requisitos a seguir de carácter obligatorio para el cumplimiento de entidades financieras, dentro de las cuales se ha tomado como punto de referencia las siguientes:

4.3.1 CIRCULAR EXTERNA 007 DE 2018 - REQUERIMIENTOS MÍNIMOS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD

Se expidió teniendo en cuenta el auge de la digitalización de los servicios financieros, la mayor interconectividad de los agentes y la masificación en el uso de canales electrónicos, entre otros, y complementa las normas existentes con relación a la administración de los riesgos operativos y la seguridad de la información.

Así, la entidad vigilada deberá informar a los consumidores financieros sobre los incidentes cibernéticos que se hayan presentado y en los que se vieran afectadas

la confidencialidad o integridad de su información, al igual que las medidas adoptadas para solucionar la situación.

Dentro de los requerimientos que deberán cumplir las entidades vigiladas en materia de ciberseguridad también está la conformación de una unidad que gestione los riesgos de seguridad de la información y la ciberseguridad.

En este aspecto, es importante la actualización permanente y especializada sobre las nuevas modalidades de ciberataques que pudieran llegar a afectar a la entidad, por lo que deben realizar capacitaciones periódicas para los funcionarios en ciberseguridad.

Adicionalmente, las entidades vigiladas deberán establecer una estrategia de comunicación e información para el envío de reportes a las autoridades que hacen parte del modelo nacional de gestión de incidentes cibernéticos[14].

4.3.2 CIRCULAR EXTERNA 042 DE 2012 - REQUERIMIENTOS MÍNIMOS DE SEGURIDAD Y CALIDAD PARA LA REALIZACIÓN DE OPERACIONES

Donde se establecen una serie de medidas encaminadas a fortalecer la seguridad y la calidad en el manejo de la información de los clientes y usuarios de las entidades vigiladas por la Superintendencia Financiera de Colombia, bien sea que acudan directamente a las oficinas, a cualquiera de los medios (tarjetas débito y crédito) o de los canales a través de los cuales éstas prestan sus servicios. En esta menciona los requerimientos en cuanto a software, hardware o protocolos para garantizar el adecuado aseguramiento de la información en cuanto a la disponibilidad, integridad y confidencialidad

4. MARCO GEOGRÁFICO

El estudio se desarrolla en territorio colombiano donde tiene control la Superintendencia Financiera de Colombia sobre las entidades financieras en específico sobre las 181 cooperativas financieras (en color rojo) registradas legalmente según la Superintendencia de la economía Solidaria (SuperSolidaria), dentro de las más conocidas se encuentran Cotrafa, CFA, Coofinep, JFK y Confiar.

[14] Gestión de Riesgo. Circular externa 007 [on-linne]. 2018

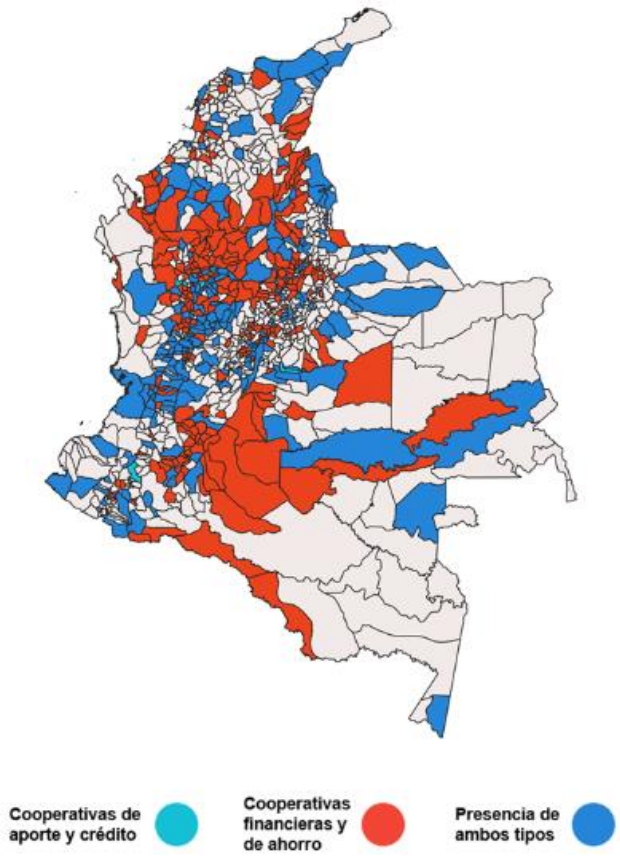


Figura 6. Mapa de Colombia con la ubicación geográfica de las cooperativas financieras y de aporte y crédito

5. MARCO DEMOGRÁFICO

En la investigación se tiene claridad que el estudio realizado va enfocado a las 181 cooperativas financieras en Colombia, estas se diferencian de las Cooperativas de ahorro y crédito en su capacidad legal para recibir depósitos de terceros, también su segunda característica es que son Vigiladas por Superfinanciera de Colombia.

5. METODOLOGÍA

En este capítulo se presentan cada una de las fases que se realizaron para el desarrollo del proyecto y obtener las buenas prácticas a monitorear con un SIEM teniendo en cuenta el levantamiento de información, análisis de los datos recolectados, la propuesta de buenas prácticas y por último una prueba de concepto.

1. FASES DEL TRABAJO DE GRADO

5.1.1 FASE 1 LEVANTAMIENTO DE INFORMACIÓN: En esta fase se realizó la búsqueda de información acerca de sistemas de información con los que cuentan las cooperativas financieras, para esta toma de datos se realizó una encuesta, adicionalmente se identificaron las principales técnicas utilizadas por grupos de ciberdelincuentes que atacan el sector financiero.

5.1.2 FASE 2 ANÁLISIS: Se realiza el análisis de los datos recopilados basándose en otras regulaciones que tiene el sector bancario como la circular 042 donde menciona los requerimientos mínimos de seguridad y calidad para la realización de operaciones los cuales serán los sistemas de información y generadores de logs que alimentarán al SIEM, también se realiza un detallado análisis de los numerales de la circular 007 identificando a cuáles apoyará el sistema SIEM.

5.1.3 FASE 3 EJECUCIÓN: En esta fase se buscó integrar los dispositivos identificados junto con el análisis realizado de la circular 007 y las técnicas más utilizadas por los cibercriminales al sector bancario unificándolo para obtener las buenas prácticas a monitorear con el SIEM, por último, se realiza una prueba de concepto en ambiente pruebas monitoreando algunos de los eventos presentados.

5.1.4 FASE 4 CIERRE: Una vez se terminen las anteriores fases del proyecto y el desarrollo de cada uno de los objetivos se realiza la sustentación del proyecto haciendo entrega del documento formal y los entregables adjuntos.

Gráfico 2. Fases del Trabajo de Grado

2. INSTRUMENTOS O HERRAMIENTAS UTILIZADAS

En el Mercado existen una gran variedad de sistemas SIEM, los más populares son de pago, solamente unos pocos son Open Source y con características limitadas, pero algunos de los más conocidos ofrecen versiones de prueba por un periodo de tiempo. En este caso el ingeniero a cargo labora en una compañía que es un reseller del fabricante Solarwinds quien cuenta un sistema SIEM llamado SEM por sus siglas “Security Event Manager” la cual se muestra en el cuadrante de Gartner para el año 2020, por tal motivo cuenta con licencias disponibles para utilizar el software para la prueba de concepto de las buenas prácticas propuestas anteriormente.

Figura 7. Cuadrante Mágico de Gartner para Security Information and Event Management
Tomado de: https://www.gartner.com/en/documents/3981040[15]

3. POBLACIÓN Y MUESTRA

La propuesta está enfocada en un nicho limitado del sector financiero, principalmente a las 181 cooperativas financieras registradas según la superintendencia de economía solidaria las cuales están regidas a supervisión y vigilancia de la superintendencia financiera de Colombia y que deben cumplir en

[15] KAVANAGH, K.; BUSSA, T.; SADOWSKI, G. 2020. Magic Quadrant for Security Information and Event Management. Gartner.

su totalidad los lineamientos expresos en la circular 007, esto basado en la experiencia que el ingeniero a cargo del proyecto ha tenido con estas entidades ya que los recursos son muy limitados, ya sea porque no tienen la suficiente fuerza económica o simplemente no le daban la importancia necesaria para implementar un sistema SIEM.

4. ALCANCES Y LIMITACIONES

Para el desarrollo del presente trabajo de grado se definen las buenas prácticas a monitorear de los activos o dispositivos y así configurar el sistema SIEM para dar cumplimiento de los lineamientos expresos en de la circular 007 para las cooperativas financieras de Colombia, entregando como resultado el análisis de la circular 007, la identificación de las fuentes y tipos de eventos a monitorear como buenas prácticas y una prueba de concepto.

Como limitaciones se aclara que no es una guía de instalación, no es una investigación de cual es mejor SIEM, no es una prueba exhaustiva del SIEM del del fabricante de Solarwinds.

6. PRODUCTOS A ENTREGAR

El presente trabajo contempla las buenas prácticas de eventos a monitorear de los sistemas de información con los que cuentan las cooperativas financieras en Colombia con el fin de dar cumplimiento a los lineamientos estipulados en la circular externa 007 de 2018 la cual menciona requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad expedida por la Superintendencia Financiera de Colombia.

PRODUCTOS ENTREGABLES

1. Encuesta A Cooperativas Financieras En Colombia.
2. Análisis De Los Sistemas Recomendados Por La Circular 042.
3. Principales APTs Y Técnicas De Ciberataques Al Sector Financiero.
4. Análisis Circular 007 De La Superfinanciera.
5. Eventos Por Monitorear Como Buenas Prácticas.
6. Prueba De Concepto.

7. ENTREGA DE RESULTADOS E IMPACTOS

1. ENCUESTA A COOPERATIVAS FINANCIERAS EN COLOMBIA.

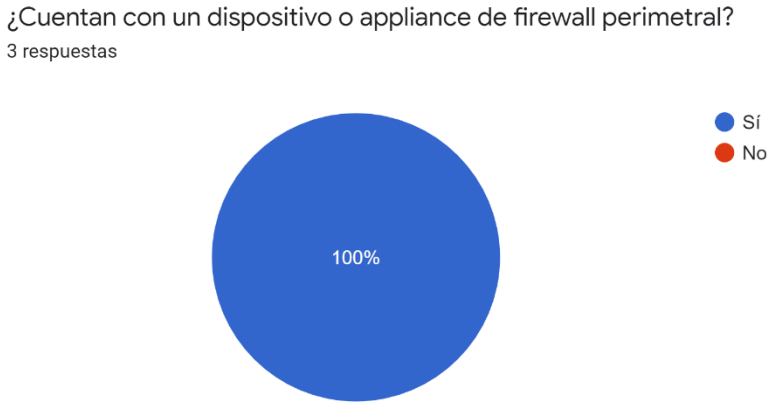
Teniendo en cuenta el sector financiero al que va dirigido la propuesta de eventos a monitorear en un SIEM, se realizó una encuesta solicitando información acerca de cuáles son los sistemas de información con los que cuentan en las entidades.

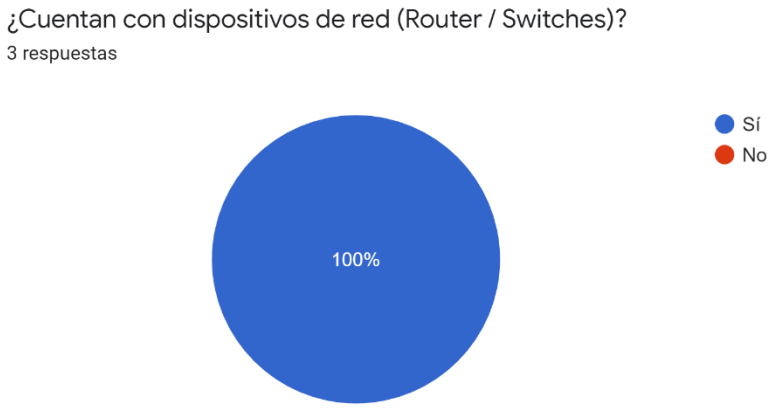
Figura 8. Portada de la Encuesta: Sistemas de información en las Cooperativas Financieras de Colombia

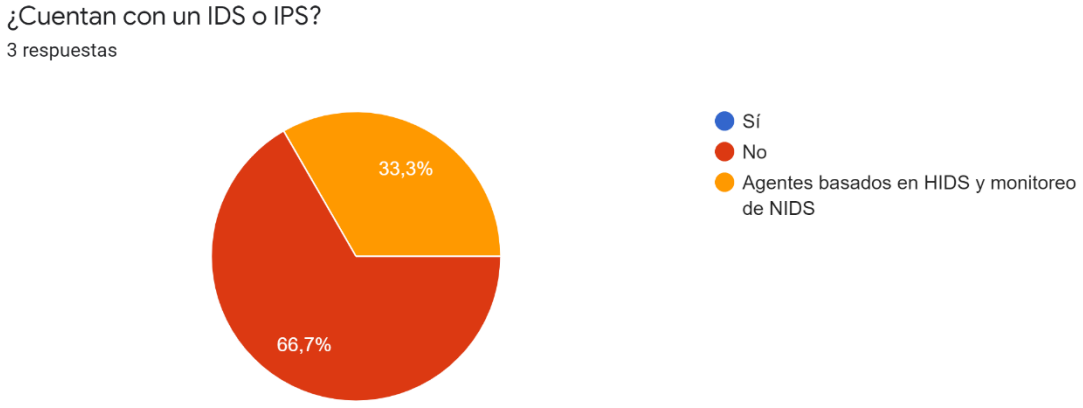
Conociendo el sector financiero al cual se le realiza la encuesta se identifica que estas respuestas pueden considerarse como información reservada para la entidad y que no cualquier persona debería conocer, por este motivo no se obtuvieron muchas respuestas acerca de los sistemas de información de las cooperativas financieras, estas respuestas fueron enviadas de manera anónima. Se seleccionó una muestra según los contactos de correo electrónico que se lograron conseguir de los administradores de infraestructura y oficiales de seguridad de las entidades.

Se identifica que por cada 3 entidades encuestadas se considera un nivel de confianza del 80% y el margen de error está en el intervalo de ±37% respecto a

cada dato obtenido en la encuesta, esto conociendo que la población total de entidades financieras en colombia es de 181. A continuación, se relacionan los resultados.

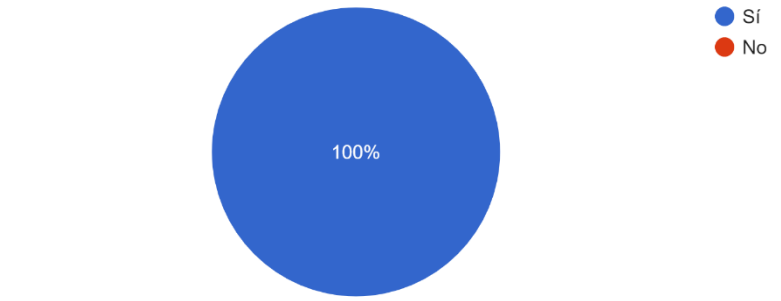






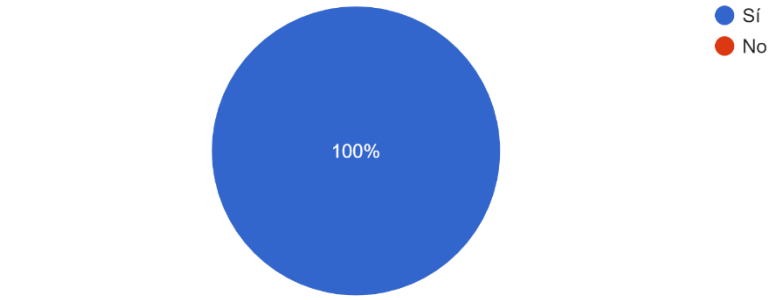
¿Cuentan con un servidor de gestión de accesos (Active Directory)?

3 respuestas



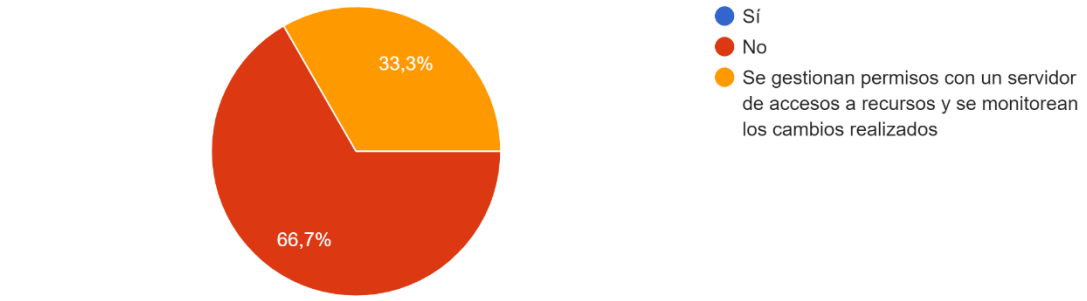
¿Cuentan con servidor de repositorio de archivos (file server)?

3 respuestas



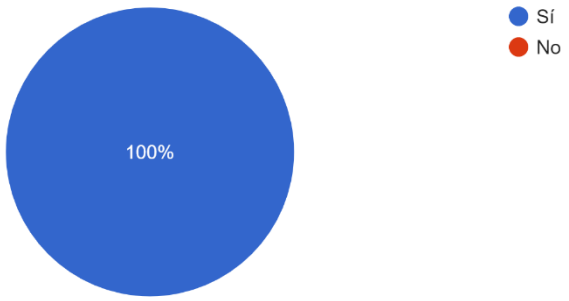
¿Cuentan con una solución DLP (Data Loss Prevention)?

3 respuestas



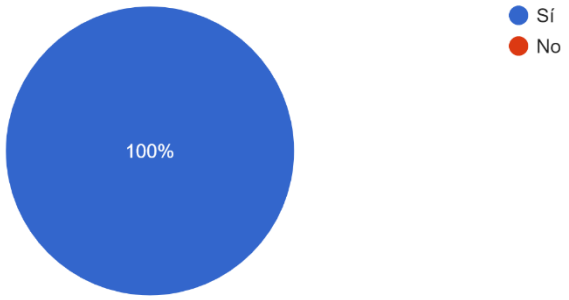
¿Cuentan con servidores de bases de datos?

3 respuestas



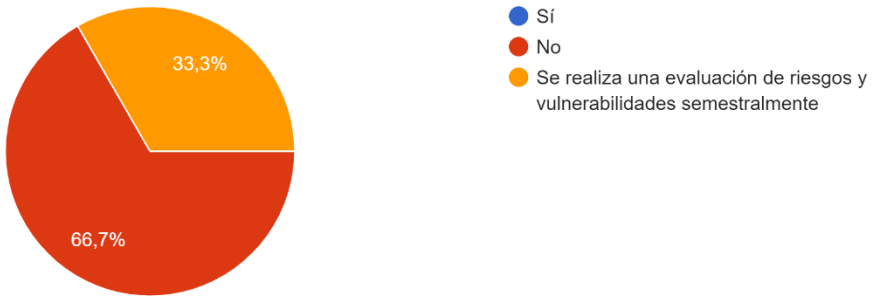
¿Cuentan con un servicio de antivirus o detección de malware ?

3 respuestas



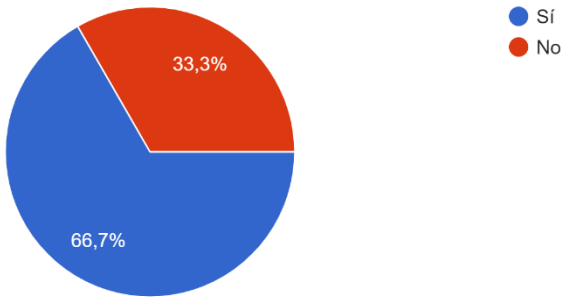
¿Cuentan con un servicio o software de análisis de vulnerabilidades?

3 respuestas



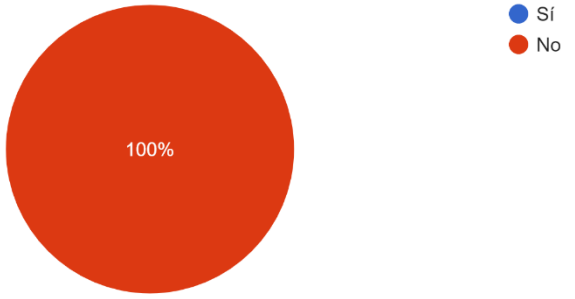
¿Cuentan con SIEM (Gestor de Eventos e Información de Seguridad) ?

3 respuestas



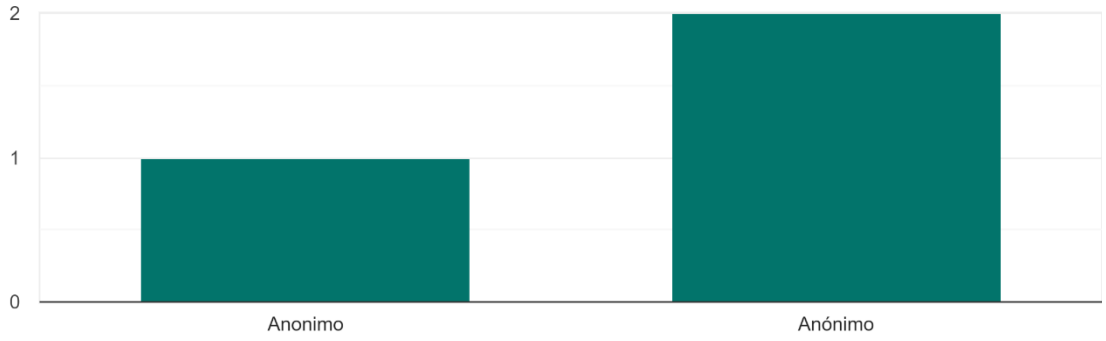
¿Cuentan con servidores de aplicaciones diferentes a los mencionados en las preguntas anteriores?

3 respuestas



Nombre del encuestado

3 respuestas



Con los resultados obtenidos se determinan los sistemas de información que se agregaran al monitoreo del SIEM para las buenas practicas. A continuación se muestra un resumen de los resultados (Gráfico 3).

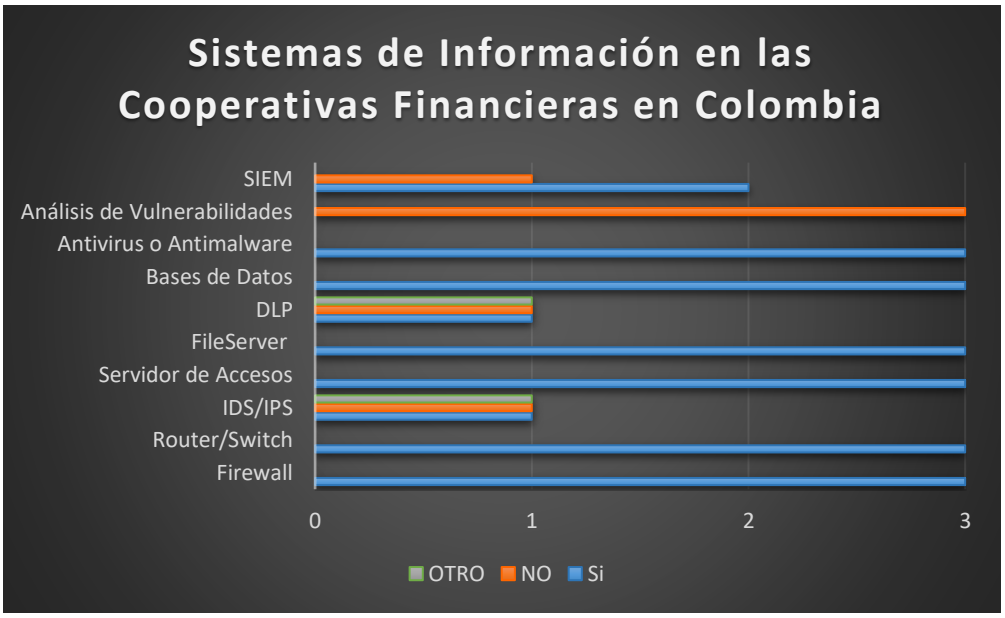


Gráfico 3. Resumen de los resultados obtenidos en la encuesta.

Se identifica de las encuestas realizadas que el 100% de las entidades cuentan con sistemas de firewall, sistemas de red como router o switches, servidores de gestion de accesos, servidores de archivos (file server), sistemas de bases de datos y sosftware de detección de malware. El 66% cuentan con un sistemas SIEM y el 33% cuentan con sistemas de IDP/IPS, DLP (data loss prevention) u otro.

2. ANALISIS DE LOS SISTEMAS RECOMENDADOS POR LA CIRCULAR 042.

Son muchos sistemas generadores o fuentes de logs en una entidad financiera, se debe tener una lista de activos y sistemas a monitorear dependiendo de la criticidad o importancia del activo y su función para la entidad.

Teniendo en cuenta que la circular 007 de 2018 no menciona que activos, dispositivos o software se deben monitorear o integrar al SIEM si no que por el contrario se deja muy a la interpretación de la entidad financiera o del usuario, es necesario basarse en un análisis de las circulares anteriores que las rigen donde mencionen que dispositivos se deben utilizar para no incumplir con la superintendencia financiera. En la circular externa 042 de 2012 de requerimientos mínimos de seguridad y calidad para la realización de operaciones, menciona en sus numerales algunos tipos de tecnologías o en otros no explícitamente

menciona que dispositivo utilizar, pero asemejando los requerimientos y conociendo las funciones que cumplen cada uno de los dispositivos o tecnologías que se listan a continuación se cumplen los lineamientos estipulados en cada numeral.

7.2.1. FIREWALL

Estas soluciones ofrecen servicios tales como bloqueo de paquetes, también se pueden usar para restringir el acceso a nivel de red interna o externa y agregar una capa de protección entre clientes y servidores. Los firewalls permiten o bloquean la actividad según una política; usan métodos sofisticados para examinar el tráfico de red, también pueden rastrear estado del tráfico de red y realizar inspección de contenido. Estos tienden a ser más complejos en cuanto las políticas y a generar registros de actividad más detallados como IP de origen y destino, usuarios, URLs, puertos y protocolos[16].

Podrían considerarse una de las herramientas más importantes en cuanto a envió de información en logs ya que se tiene una visión general del tráfico generado por aplicaciones, servidores, estaciones finales de trabajo. Adicional muchos de estos dispositivos cuentan con servicios de gestión de accesos por VPN, análisis de tráfico en red, inclusive sistemas de detección de intrusos (IDS).

El acceso remoto a menudo se otorga y se asegura a través de redes virtuales privadas (VPN). Los sistemas VPN que admiten control de acceso granular, muchos de estos servicios VPN pueden registrar información detallada sobre el uso de los recursos utilizados por cada usuario.

7.2.2. SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS IDS/IPS (INTRUSION DETECTION SYSTEMS / INTRUSION PREVENTION SYSTEM)

Estos sistemas registran información detallada sobre comportamiento sospechoso y ataques detectados, así como cualquier acción realizada por los sistemas de prevención de intrusos para detener la actividad maliciosa en progreso.
Algunos sistemas se dividen también en dos esquemas que son el HIDS basados en host o el NIDS basados en red. Para los NIDS, una firma puede ser tan simple como un patrón específico que coincida con una porción de un paquete de red. La firma del paquete o el contenido del encabezado pueden indicar acciones no autorizadas, la aparición de una firma no puede significar un intento real no autorizado de acceso, pero es una buena idea configurar alertas[17].

[16] SCARFONE, K.; HOFFMAN, P. 2009. Guidelines on Firewalls and Firewall Policy. p. 2.5.
[17] ZHENGBING, H.; ZHITANG, L.; JUNQI, W. A Novel Network Intrusion Detection System (NIDS)

IDS de red (NIDS): ubicado en puntos estratégicos de una red para monitorear el tráfico entre dispositivos y hosts dentro de la red.
IDS basado en el host (HIDS): se ejecuta en sistemas host individuales y supervisa el tráfico desde y hacia el sistema host, así como las actividades en el sistema mismo.

7.2.3. ROUTER Y SWITCH

Estos dispositivos pueden configurarse para permitir o bloquear ciertos tipos de tráfico de red en función de una política igual que los firewalls. Los Routers generalmente están configurados para registrar los campos más básicos de la actividad bloqueada.

7.2.4. SERVIDORES DE ACCESOS Y GESTIÓN DE PERMISOS

Este servidor contiene las credenciales de todos los usuarios de la entidad, así como las diferentes políticas de acceso de los usuarios. Es el responsable de permitir o denegar mediante una autenticación el acceso al usuario a los dispositivos asignados y los elementos de red que a este se le otorgue acceso[18].

Servidores de autenticación, incluidos servidores de directorio o dominio, estos registran cada intento de autenticación, incluido su origen, nombre de usuario, éxito o fracaso, fecha y hora. Estos eventos pueden mostrar problemas con un usuario o conjunto de usuarios.

7.2.5. SOFTWARE ANTIMALWARE

La forma más común de software antimalware es el antivirus, que normalmente registra todas las clases de malware detectado, intentos de desinfección de archivos y sistemas. También cuenta con características de rastreo o detección de ejecución de nuevos procesos o servicios en segundo plano que por lo general instala el malware, así como el monitoreo del estado de la actualización constante de sus bases de firmas[16].

Based on Signatures Search of Data Mining. First International Workshop on Knowledge Discovery and Data Mining. 2008. p. 10

[18] PEÑA Ninco, J. W. 2015. Instructivo para la implementación efectiva de sistema de información de seguridad y administración de eventos SIEM para la agencia nacional de la superación de la pobreza extrema ANSPE. Universidad Piloto de Colombia. Pag. 28.

7.2.6. SOFTWARE DE ANÁLISIS Y GESTIÓN DE VULNERABILIDADES

Estos sistemas cuentan con software de gestión de parches y software de evaluación de vulnerabilidades, registran el historial de instalación de parches y estado de vulnerabilidad de cada host, que incluye vulnerabilidades conocidas y si faltan actualizaciones de software. Este software de gestión de vulnerabilidades también puede registrar datos adicionales información sobre las configuraciones de los hosts[16].

7.2.7. SISTEMAS OPERATIVOS

Los diferentes sistemas operativos (SO) instalados en servidores o estaciones de trabajo se puede recopilar una gran variedad de información relacionada con eventos o logs de sistema, seguridad o aplicaciones que tengan la capacidad generar logs de auditoria.

- **Eventos de Sistema:** Los eventos del sistema son acciones operativas realizadas por el mismo sistema operativo, como apagar el sistema o iniciar un servicio. Típicamente, eventos fallidos y los más significativos eventos exitosos, pero muchos sistemas operativos permiten a los administradores especificar qué tipos de eventos se registrarán.

- **Registros de auditoría o seguridad:** Los registros de auditoría contienen información de eventos de seguridad, como exitosa e intentos fallidos de autenticación, acceso a archivos, cambios en la política de seguridad, cambios en las cuentas (por ejemplo, cuenta creación y eliminación, asignación de privilegios de cuenta) y uso de privilegios.

7.2.8. SERVIDORES DE APLICACIONES

Existen un sin número de proveedores de aplicaciones como servidores de correo electrónico, servidores web, servidores de archivos (file servers) y clientes de intercambio de archivos (FTP) y servidores de bases de datos: estas aplicaciones generan sus propios registros de logs mientras que otros escriben sobre los registros de del sistema[16].

- **Solicitudes del cliente y respuestas del servidor:** Estos eventos útiles para reconstruir secuencias de eventos y determinar su resultado. Si la aplicación registra autenticaciones de usuarios, generalmente es posible determinar qué usuario realizó cada solicitud. Algunas de las aplicaciones pueden realizar registros altamente detallados. Esta información puede

usarse para identificar o investigar incidentes y monitorear el uso de la aplicación para fines de cumplimiento y auditoría.

7.2.9. BASES DE DATOS

En la actualidad la mayoría de nuestra información ya se encuentra alojada en bases de datos por lo que es necesario darle un aseguramiento y garantizar la confidencialidad, integridad y disponibilidad, estas son un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso[19].

7.2.10. FILESERVER - REPOSITORIO DE ARCHIVOS

Este tipo de servidor que almacena y distribuye diferentes tipos de archivos informáticos entre los clientes de una red de computadoras[20].

Específicamente cumplen con este servicio de almacenamiento que es gestionado principalmente en conjunto con un servidor de accesos mediante las políticas y gestión de accesos garantizando que los usuarios que acceden a estos recursos de red sean los indicados según sus roles o funciones en la entidad (Peña Ninco, 2015).

3. PRINCIPALES APTS Y TECNICAS DE CIBERATAQUES AL SECTOR FINANCIERO

Se realizó una búsqueda de las técnicas más utilizadas por varios grupos de cibercriminales que atacan al sector financiero a nivel mundial según Mitre Att&ck, también se realizó un análisis del esquema de las principales APTs que son un tipo de malware creado específicamente para atacar a una empresa o gobierno concretos con el objetivo principal de robar su información y mantenerse oculto a la vista del mismo el mayor tiempo posible. Cuanto más tiempo permanezca oculto, más información será capaz de extraer[21].

[19] GUERRERO LÓPEZ, F. A.; RODRÍGUEZ PINILLA, J. E. 2013. diseño y desarrollo de una guía para la implementación de un ambiente big data en la universidad católica de colombia. Universidad Católica de Colombia. p. 46.
[20] LEGUIZAMÓN, D. A.; VENGOECHEA A. A. 2017. Solución instalaciones automatizadas sobre sistemas operativos windows. Universidad Católica de Colombia. p. 93.
[21] CARBONÓ, D. 2013. Amenazas persistentes avanzadas. Especialización Seguridad Informática Universidad Piloto de Colombia. ATPs

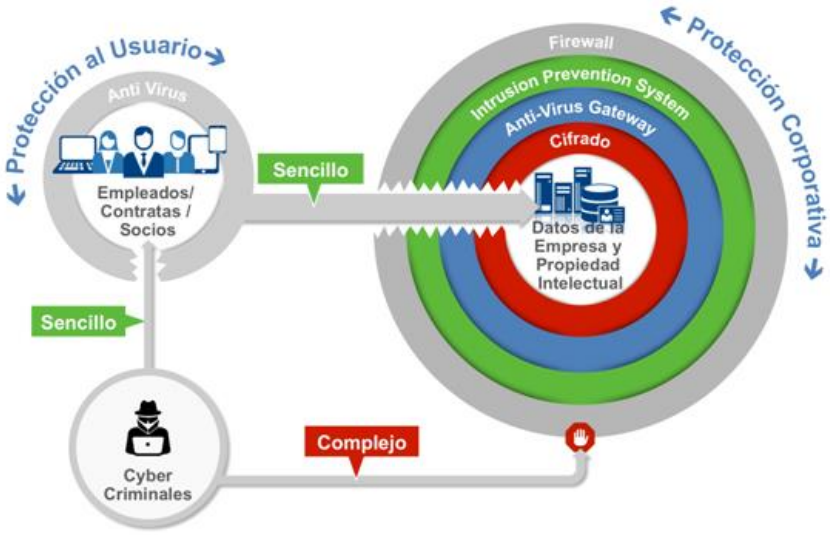


Figura 9. Forma sencilla de afectar la seguridad corporativa. Tomada dehttps://www.ibm.com/blogs/think/es-es/2015/02/24/cuidado-con-las-apts/:

LISTA DE TECNICAS MÁS UTILIZADAS POR CIBERDELINCUENTES SEGÚN MITRE PARA EL SECTOR BANCARIO

Grupo	Código	Tipo de Técnica	S.O.	Fuente de Datos	Componente	Control
APT38	T1059	Command-Line Interface	Linux, macOS, Windows	Agentes SIEM	Monitoreo del proceso, parámetros de la línea de comandos del proceso, registro de Windows.	Audite y / o bloquee intérpretes de línea de comandos innecesarios mediante el uso de herramientas de la lista blanca de aplicaciones, como Control de aplicaciones de Windows Defender, AppLocker o Políticas de restricción de software, según corresponda.
	T1056	Input Capture	Linux, macOS, Windows	Agentes SIEM, registro de eventos	Registro de Windows, controladores de kernel, monitoreo de procesos, monitoreo de API, registro de Windows.	Detección de Keylogers evidenciando cuando se abren ejecutables .exe
	T1057	Process Discovery	Linux, macOS, Windows	Agentes SIEM, registro de eventos, antivirus	monitoreo del proceso, parámetros de la línea de comandos del proceso, registro de Windows.	Audite y / o bloque el descubrimiento o visualización de procesos mediante el establecimiento de privilegios a los usuarios.
	T1049	System Network	Firewall	Firewall - Syslogs	Configuración de políticas de alertamiento	Mediante el control de monitoreo de scaneo de

		Connections Discovery			al detectar eventos de escaneo de puertos.	puertos en los firewalls.
	T1105	Remote File Copy	Linux, macOS, Windows	Agentes SIEM, registro de eventos, DLP, auditoria de archivos.	Monitoreo de archivos, captura de paquetes, uso de procesos de red, flujo de red Netflow, análisis de protocolo de red, monitoreo de procesos, registro de Windows.	Audite los servidores de archivos, los sistemas de detección y prevención de intrusiones en la red identifican la transferencia de datos inusual sobre herramientas y protocolos conocidos como FTP se pueden usar para mitigar la actividad a nivel de red.
	T1494	Runtime Data Manipulation	Linux, macOS, Windows	Agentes SIEM, registro de eventos, antivirus.	Monitoreo de archivos, monitoreo de procesos.	Restringir permisos de archivos y directorios.
	T1089	Disabling Security Tools	Linux, macOS, Windows	Agentes SIEM, registro de eventos, antivirus.	Monitoreo de API, monitoreo de archivos, servicios, registro de Windows, parámetros de la línea de comandos del proceso, antivirus.	Gestión de cuentas con privilegios altos, restringir permisos de archivos y directorios.
Carbanak						
	T1036	Masquerading	Linux, macOS, Windows	Agentes SIEM, registro de eventos, antivirus	Monitoreo de archivos, monitoreo de procesos, metadatos de archivos binarios.	Prevención de ejecución, Restringir permisos de archivos y directorios.

Cobalt	T1050	New Service	Linux, macOS, Windows	Agentes SIEM, registro de eventos, antivirus.	Registro de Windows, supervisión de procesos, parámetros de la línea de comandos del proceso, registros de eventos de Windows.	Limite los privilegios de las cuentas de usuario y remedie los vectores de escalada de privilegios para que solo los administradores autorizados puedan crear nuevos servicios.
	T1085	Rundll32	Windows	Agentes SIEM, registro de eventos, antivirus	Monitoreo de archivos, monitoreo de procesos, parámetros de la línea de comandos del proceso, metadatos de archivos binarios.	Monitorear rundll32.exe ya que puede generar la llamada de ejecución de diferentes ejecutables, protección contra exploits.
	T1068	Exploitation for Privilege Escalation	Linux, macOS, Windows	Agentes SIEM, registro de eventos	Informe de errores de Windows, monitoreo de procesos, registros de aplicaciones.	Audite los cambios realizados en sus servidores de gestión de accesos y en todos los servidores.
	T1107	File Deletion	Linux, macOS, Windows	Agentes SIEM, registro de eventos, antivirus, auditoria de archivos.	Monitoreo de archivos, parámetros de la línea de comandos del proceso, metadatos de archivos binarios.	Alertas de DLP, auditoria de archivos y recopilar argumentos de línea de comandos.
	T1037	Logon Scripts	Linux, macOS, Windows	Agentes SIEM, registro de eventos.	Registros de eventos.	Restrinja el acceso de escritura a los scripts de inicio de sesión a administradores específicos, controle la ejecución de scripts.

	T1046	Network Service Scanning	Firewalls	Firewalls	Análisis de protocolo de red, captura de paquetes, parámetros de línea de comandos de proceso, uso de proceso de red.	Detección / Prevención de intrusiones en la red, Segmentación de red.
GCMAN	T1021	Remote Services	Linux, macOS, Windows	Agentes SIEM, registro de eventos.	Registros de eventos.	Limite las cuentas que pueden usar servicios remotos. Limite los permisos para las cuentas con mayor riesgo de compromiso; limite a los usuarios para que solo puedan ejecutar programas específicos.
Silence	T1053	Scheduled Task	Windows	Agentes SIEM, registro de eventos	Registro de eventos.	Limite los privilegios de las cuentas de usuario y remedie los vectores de escalada de privilegios para que solo los administradores autorizados puedan crear tareas programadas en sistemas remotos.
	T1064	Scripting	Linux, macOS, Windows	Agentes SIEM, registro de eventos	Monitoreo de procesos, monitoreo de archivos, parámetros de la línea de comandos del proceso.	bloquear la ejecución de macros, scripts a través de la Política de grupo.
	T1204	User Execution	Linux, Windows,	Agentes SIEM, registro	Antivirus, parámetros de la línea de comandos	Prevención de ejecución, Prevención detección de

			macOS	de eventos, antivirus	del proceso, monitoreo del proceso.	intrusiones en la red.

Tabla 1. Lista de técnicas más utilizadas por ciberdelincuentes según Mitre Att&ck para sector bancario. Modificado de: https://attack.mitre.org/groups/

4. ANALISIS CIRCULAR 007 DE LA SUPERFINANCIERA

Se realizó un análisis completo de la circular 007 - requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad para identificar a cuáles de sus lineamientos estipulados se pueden apoyar teniendo en cuenta las funciones y características de los SIEM, adicional conociendo los activos o sistemas de información que tienen las cooperativas financieras basándose en una encuesta realizada y en un análisis a la circular 042 de 2012 donde menciona los dispositivos o servicios con los que se debe contar para cumplimiento de la norma.

3. OBLIGACIONES GENERALES EN MATERIA DE CIBERSEGURIDAD

3.2.3. Debe reportar a la junta directiva y a la alta dirección, los resultados de su gestión, especialmente en la evaluación que haga de la confidencialidad, integridad y disponibilidad de la información, identificación de ciberamenazas, resultados de la evaluación de efectividad de los programas de ciberseguridad, propuestas de mejora en materia de ciberseguridad y resumen de los incidentes de ciberseguridad que afectaron la entidad. La periodicidad de los reportes debe ser, al menos, semestralmente.

- Con la función de configuración de reportes apoyará las áreas encargadas de la presentación de los resultados a la junta directiva de cada uno de los programas implementados para garantizar la ciberseguridad como firewall, antivirus y análisis de vulnerabilidades.

3.2.6. Ser la principal responsable en el monitoreo y verificación del cumplimiento de las políticas y procedimientos que se establezcan en materia de ciberseguridad, sin perjuicio a aquellas tareas que realiza la auditoría interna.

- Monitoreo y medición de la efectividad con indicadores de los controles aplicados para las políticas establecidas en los sistemas de seguridad, como ejemplo los bloqueos de navegación, bloqueos de conexiones por protocolos.

3.2.7. Asesorar a la alta gerencia y la junta directiva en temas que considere necesarios sobre seguridad de la información y ciberseguridad para que estas últimas puedan hacer seguimiento y tomar las decisiones adecuadas en esta materia.

- Mediante la configuración de reportes generados por la herramienta SIEM se apoyará a la alta gerencia a la toma de decisiones de si los controles aplicados por las áreas son efectivos

3.4. Implementar controles para mitigar los riesgos que pudieran afectar la seguridad de información confidencial, en reposo o en tránsito.

- Recopilando información de logs de los sistemas de información de red donde se muestre las conexiones establecidas o la información en tránsito de los servidores de archivos, bases de datos teniendo en cuenta la información en reposo, con software de DLP o FIM que ya vienen integradas en los agentes del SIEM, con esta información correlacionar eventos y configurar reglas para evitar que se materialicen los riegos.

3.5. Emplear mecanismos para la adecuada autenticación y segregar las funciones y responsabilidades de los usuarios con privilegios de administrador o que brindan soporte remoto, para mitigar los riesgos de seguridad de la información.

- Monitoreo constante de los mecanismos implementados o adoptados por las cooperativas como servidores de directorio activo donde se evidenciarán las respectivas autentificaciones de los usuarios, las acciones y modificaciones realizadas por los usuarios con roles de administradores o soporte evidenciando que estas modificaciones sean aprobadas por las áreas correspondientes y pasen por su respectivo control de cambios.

3.7.1. Información que reportará a la SFC, sobre incidentes de ciberseguridad que afecten de manera significativa la confidencialidad, integridad o disponibilidad de la información de la entidad, haciendo una breve descripción del incidente, su impacto y las medidas adoptadas para gestionarlo.

- Configurando la adecuada correlación con el fin de detectar las principales técnicas utilizadas por los ciberdelincuentes se logrará la detección de incidentes y se facilita el análisis forense sobre los eventos generados por las diferentes fuentes de logs.

3.11. Contar con indicadores para medir la eficacia y eficiencia de la gestión de la seguridad de la información y la ciberseguridad.

- Los indicadores y monitoreo se realizarán sobre los controles aplicados en los sistemas de información o software de seguridad que a su vez serán fuentes generadoras de logs evidenciando la eficiencia de los controles, se pueden programar en reportes o en dashboards.

4. ETAPAS

Para la gestión de la seguridad de la información y la ciberseguridad las entidades deberán considerar, como mínimo, las siguientes etapas:

4.1. Prevención

4.1.1. Establecer, mantener y documentar los controles de acceso (lógicos, físicos y procedimentales) y gestión de identidades bajo la premisa que las personas solo pueden disponer de los recursos que demande su trabajo, durante el tiempo que ello sea necesario.

- Integrando al monitoreo los servidores de acceso, sistemas operativos, aplicaciones como bases de datos, servidores de archivos los cuales generaran logs de autenticaciones generadas, sesiones establecidas por usuarios y de esta manera registrar los accesos lógicos o físicos.

4.1.2. Adoptar políticas, procedimientos y mecanismos para evitar la fuga de datos e información.

- Mediante la identificación de los usuarios que deben tener acceso a los recursos, servicios o repositorios de información dispuestos por la entidad y configurando grupos que funcionen como listas blancas o negras en el SIEM para garantizar el adecuado acceso y evitando la fuga de datos.

4.1.9. De acuerdo con la estructura, canales de atención, volumen transaccional y número de clientes, monitorear diferentes fuentes de información tales como sitios web, blogs y redes sociales, con el propósito de identificar posibles ataques cibernéticos contra la entidad.

- Con la integración de los diferentes sistemas o fuentes de información al SIEM donde se configurarán reglas de correlación y se identificarán las técnicas más utilizadas por los ciberdelincuentes al sector financiero.

4.2. Protección y detección

Las entidades deben desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad. La función de protección y detección permite el descubrimiento oportuno de eventos e incidentes de ciberseguridad y cómo protegerse ante los mismos. Las entidades deben:

4.2.1. Adoptar procedimientos y mecanismos para identificar y analizar los incidentes de ciberseguridad que se presenten

- Se podrá realizar un estudio forense de los incidentes presentados haciendo un análisis de los sistemas involucrados y así detectar la mejor forma de implementar los respectivos controles y evitar que se repitan.

4.2.3. Realizar un monitoreo continuo a su plataforma tecnológica con el propósito de identificar comportamientos inusuales que puedan evidenciar ciberataques contra la entidad.

- Con la configuración de dashboards donde el personal a cargo del SOC o del SIEM pueda estar en el constante monitoreo de los comportamientos anómalos que se puedan presentar e identificar si pueden ser incidentes de seguridad.

4.3. Respuesta y comunicación

Aún con las medidas de seguridad adoptadas, las entidades deben desarrollar e implementar actividades para mitigar los incidentes relacionados con ciberseguridad. Para hacerle frente a esta situación las entidades deben:

4.3.1. Establecer procedimientos de respuesta a incidentes cibernéticos tales como: desconexión automática de equipos, cambios de contraseñas, actualizar la base de firmas del antivirus, bloqueo de direcciones IP o cualquier otro que determine la entidad.

- Dentro de las funciones que tienen algunos SIEM cuentan con la capacidad de responder automáticamente a los comportamientos inusuales y que se puedan categorizar como incidentes de seguridad y generar respuestas activas como la desconexión de tarjetas de red, apagado o desconexión de los equipos, bloqueo de direcciones IP, reinicio de servicios, desconexión de usuarios.

4.3.5. En la medida de lo posible, preservar las evidencias digitales para que las áreas de seguridad o las autoridades puedan realizar las investigaciones correspondientes.

- Los SIEM funciona como un servidor Syslog en donde puede consultar las evidencias a través del tiempo como históricos y si bien no cuenta con esta opción se configuran reportes automáticos en donde se pueda tener las evidencias para las investigaciones o auditorias pertinentes.

5. EVENTOS POR MONITOREAR COMO BUENAS PRÁCTICAS.

Teniendo en cuenta los dispositivos mencionados anteriormente, el análisis realizado a la circular 007 de la SFC y las técnicas o APTs (Amenaza persistentes avanzadas) más utilizadas por los ciberdelincuentes según Mitre Att&ck, se definieron una serie de eventos de cada uno de los dispositivos a monitorear

7.5.1. EVENTOS A MONITOREAR DE UN FIREWALL.

Monitoreo de accesos o cambios de los usuarios fuera de los horarios laborales que estipule la entidad financiera. Es claro que las entidades financieras podrían contar con personal que cumple con horarios de disponibilidad y 24/7 como lo podría ser el área de tecnología, por lo que hay que definir grupos que tengan permitido este acceso en estos horarios, pero aun así continuar con el monitoreo constante de ellos. En el caso del personal que no deba conectarse en horarios diferentes a los permitidos por la entidad establecer una serie de alarmas que estén informando al personal encargado del monitoreo cuando pasen estos eventos e identificar si se puede tratar de un incidente de seguridad.

- Numerales a los que aplica según circular 007 3.2.3 - 3.2.6 - 3.4 - 3.7.1 - 4.1.1 - 4.1.2 - 4.2.3

Creación o cambios de las políticas configuradas (reglas de acceso). Tener un registro de todos los cambios a nivel de reglas de acceso aprobados por los oficiales de seguridad o del área encargada donde se debe tener un seguimiento y evidencia de las actividades realizadas durante los cambios.

- Numerales a los que aplica según circular 007 3.2.6 - 3.4 - 3.11 - 4.1.1 - 4.1.2 - 4.3.5

Cambios en el estado de servicios (apagado, reinicio de procesos o sistema) Monitorear el performance del dispositivo garantizando la disponibilidad de los servicios, establecer listas de procesos a monitorear; como una lista blanca de procesos aprobados para el funcionamiento en los servidores o en los hosts finales de los usuarios, así mismo como una lista de negra de procesos de que no deberían ejecutarse por que puedan afectar la seguridad de la información en la entidad y catalogarse como un posible incidente.

- Numerales a los que aplica según circular 007 3.2.6 - 3.4 - 3.11- 4.1.9 - 4.2.3

Detención de actividad sospechosa (URLs con amenazas, escaneo de redes y puertos) Tomando los datos de navegación como las URLs y comparándola con los sitios conocidos con amenazas determinar si se llega a establecer una conexión con estos sitios, evidenciar los escaneos de la red y de puertos buscando una correlación para determinar si ocurre un incidente.

- Numerales a los que aplica según circular 007 3.2.6 - 3.4 - 3.7.1 - 3.11 - 4.1.9 - 4.2.1 - 4.2.3

Registrar intentos fallidos y exitosos de inicio de sesión por VPN. Hay que realizar una segregación de usuarios buscando evidenciar a que sitios o recursos de red tienen permitido ingresar teniendo en cuenta sus roles y funciones por tal motivo es necesario registrar todas autenticaciones por VPN evidenciando a que recursos de red están ingresando. Así como las autenticaciones fallidas de usuarios que no pertenezcan a la entidad y si son muy concurrentes establecer bloqueos de IPs evitando posibles incidentes.

- Numerales a los que aplica según circular 007 3.5 - 4.1.1 - 4.1.2

Puertos utilizados para conexiones de aplicaciones o servicios. Cada aplicación o servicio utilizan puertos específicos para sus conexiones de red, estas conexiones deben estar permitidas desde ciertos segmentos de red o desde determinados host, por tal motivo es necesario evidenciar cuando se presentan eventos de descubrimiento de puertos abiertos a los servidores o servicios y así lograr detectar posibles conexiones fallidas o exitosas a estos puertos. Como ejemplo podemos tomar unos des estos puertos que son unos de los más utilizados. (Tabla 2)

- Numerales a los que aplica según circular 007 3.2.6 - 3.4 - 4.1.1 - 4.1.2 – 4.1.9

Puerto	Nombre	Descripción
20/tcp	ftp-data	FTP - File Transfer Protocol (Protocolo de Transferencia de Ficheros) - Datos
21/tcp	ftp-control	FTP File Transfer Protocol (Protocolo de Transferencia de Ficheros) - Control
22/tcp	ssh	SSH, scp, SFTP
23/tcp	telnet	Telnet manejo remoto de equipo, inseguro

25/tcp	smtp	SMTP Simple Mail Transfer Protocol (Protocolo Simple de Transferencia de Correo)
80/tcp	http	HTTP HyperText Transfer Protocol (Protocolo de Transferencia de HiperTexto) (WWW)
107/tcp	rtelnet	Telnet remoto
109/tcp	pop2	POP2 Post Office Protocol (E-mail)
110/tcp	pop3	POP3 Post Office Protocol (E-mail)
115/tcp	sftp	SFTP Protocolo de transferencia de archivos seguros
443/tcp	https	HTTPS/SSL usado para la transferencia segura de páginas web
3389/tcp	rdp	RDP (Remote Desktop Protocol) Terminal Server

Tabla 2. Principales puertos de red información tomada de https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt

7.5.2. EVENTOS A MONITOREAR DE UN IDS / IPS

Numero de autenticaciones exitosas y fallidas en los hosts. Basados en un esquema de HIDS detectar las autenticaciones en los servidores o host finales, en tal caso de que se utilicen servicios de escritorio remoto segregar los usuarios que deberían contar con los permisos a estos.

- Numerales a los que aplica según circular 007: 3.4 - 3.5 - 3.7.1. - 4.1.1 - 4.1.2 - 4.2.1 - 4.2.3 - 4.3.1 - 4.3.5

Numero de alertamientos. Enviar las alertas configuradas cuando se presenten, un ejemplo es si el usuario no puede iniciar sesión en el sistema por tres veces, entonces el HIDS detectará este comportamiento por el patrón de "tres inicios de sesión fallidos" teniendo en cuenta que este podría ser un intento de autenticación de fuerza bruta y se podría materializar y convertirse en un incidente.

- Numerales a los que aplica según circular 007: 3.2.3. - 3.2.6. - 3.2.7 - 3.4 - 3.5 - 3.11 - 4.1.1 - 4.1.2 - 4.2.1 - 4.2.3 - 4.3.1 - 4.3.5

Acciones realizadas por el IPS. Como ejemplo podemos tomar cuando se presentan autenticaciones exitosas de cuentas las cuales no deberían contar con permisos se deben configurar acciones proactivas de cierre de sesión de la cuenta.

- Numerales a los que aplica según circular 007: 3.2.3 - 3.2.6. - 3.2.7 - 3.4 - 3.5 - 4.1.1 - 4.1.2 - 4.2.1 - 4.2.3 - 4.3.5

7.5.3. EVENTOS A MONITOREAR DE DISPOSITIVOS DE RED (ROUTER/SWITCH)

Autenticaciones exitosas o fallidas a estos dispositivos. Registrar todo tipo de autenticaciones y protocolos empleados, así como los orígenes desde donde se presentan estas identificando que sean de la red corporativa o de un origen confiable y no llegase a ser intentos de autenticaciones externas.

- Numerales a los que aplica según circular 007: 3.5. - 4.1.1 - 4.3.5

Cambios en la configuración o políticas. Registros de los cambios realizados en las políticas que se tengan configuradas y que estas hallan pasado por aprobaciones previas de las áreas encargadas.

- Numerales a los que aplica según circular 007: 3.4. - 3.5 - 4.1.2 - 4.2.3. - 4.3.5

Cambios en los estados de los puertos. Evidenciar cuando hay cambios físicos o errores lógicos en los dispositivos como los estados Up o Down garantizando la disponibilidad de acceso a la información.

- Numerales a los que aplica según circular 007: 3.7.1. - 3.11. - 4.3.5.

7.5.4. EVENTOS A MONITOREAR DE UN SERVIDOR DE ACCESOS.

Con la adecuada configuración de auditoria en estos servidores se pueden registrar los eventos necesarios para detectar cambios en el sistema, en las políticas, en las cuentas, y autenticaciones realizadas.

Múltiples autenticaciones fallidas a cuentas existentes y no existentes. Recolectar los eventos de autenticaciones fallidas reportadas en el dominio e identificar el origen de donde se generan ya que al ser cuentas no existentes

podría tratarse de un ataque de fuerza bruta.

- Numerales a los que aplica según circular 007: 3.2.3. - 3.2.6. - 3.4. - 3.5 - 3.7.1. - 3.11. - 4.1.1. - 4.2.3. - 4.3.1. - 4.3.5.

Escalamiento de privilegios (grupos administradores). Realizando la segregación de cuentas e identificando cuales son las que hacen parte de los grupos con altos privilegios, grupos VIP o grupos de soporte e identificar que los cambios realizados por el personal autorizado, así mismo identificar los grupos con alta criticidad que cuentan con más privilegios.

- Numerales a los que aplica según circular 007: 3.2.3. - 3.2.6. - 3.4. - 3.5 - 3.11. - 4.1.1. - 4.2.3. - 4.3.1. - 4.3.5.

Autenticaciones a cuentas genéricas o por default. Conociendo que se deben eliminar por completo las cuentas genéricas como por ejemplo las cuentas administrador, admin, soporte, root, etc, así mismo sería bueno monitorearlas identificando si los hay alguien que esté intentando contar con acceso desde esas cuentas.

- Numerales a los que aplica según circular 007: 3.2.3. - 3.2.6. - 3.4. - 3.5 - 3.7.1. - 3.11. - 4.1.1. - 4.2.3. - 4.3.1. - 4.3.5.

Creación, borrado, inhabilitación o cambios en las cuentas. Realizar el monitoreo constante de la creación, borrado, inhabilitación o cambios en las cuentas dominio y locales, enviar alertas informando quien, que y cuando realizo estas acciones y llevando un control de esos eventos.

- Numerales a los que aplica según circular 007: 3.2.3. - 3.2.6. - 3.4. - 3.5 -- 3.11. - 4.1.1. - 4.2.3. - 4.3.1. - 4.3.5.

7.5.5. EVENTOS A MONITOREAR DE UN ANTIVIRUS O SOFTWARE ANTIMALWARE

Acciones tomadas frente a la detección de software malintencionado. Enviar todo tipo de alertamiento generado por la consola de antivirus, así como las acciones realizadas cuando detecta un virus o malware (puesto en cuarentena, eliminados, no se pudo realizar ninguna acción)

- Numerales a los que aplica según circular 007: 3.2.3. - 3.2.6 - 3.2.7. - 3.7.1 -

3.11. - 4.2.3. - 4.3.1. - 4.3.5.

Estado de los agentes. Validar los estados de conexión o de desconexión con la consola de administración del antivirus con el fin de validar si los procesos que se corren en segundo plano están ejecutándose y si tienen la protección activa.

- Numerales a los que aplica según circular 007: 3.2.3. - 3.7.1 - 3.11. - 4.2.3. - 4.3.1. - 4.3.5.

Estado de su base de firmas (actualizaciones al día). Conociendo que los antivirus trabajan con un esquema de firmas las cuales se van actualizando a medida que aparecen nuevos virus y los proveedores las registran como en sus bases de datos es necesario mantener los agentes actualizados al día, en tal caso que no se tenga actualizado en un activo y se presente actividad inusual hay que realizar el análisis correspondiente para descartar que pueda ser un incidente de seguridad.

- Numerales a los que aplica según circular 007: 3.2.3. - 3.2.6 - 3.7.1 - 3.11. - 4.2.3. -4.3.1. - 4.3.5.

7.5.6. EVENTOS A MONITOREAR DE UN SOFTWARE DE ANÁLISIS DE VULNERABILIDADES

Monitoreo constante de activos con vulnerabilidades. Este software genera reportes de los activos donde encuentra vulnerabilidades los cuales hay que tener en constante monitoreo como prioridad por lo menos hasta que sea subsanada esa vulnerabilidad.

- Numerales a los que aplica según circular 007: 3.2.3. - 3.2.6 - 3.2.7. - 4.3.5.

7.5.7. EVENTOS A MONITOREAR DE SISTEMAS OPERATIVOS

Estado de las actualizaciones pendientes. Al igual que se mencionó el parcheo de vulnerabilidades se debe tener actualizados los sistemas operativos y evidenciar en cuales no se les han aplicado las actualizaciones o en cuales se han presentado errores.

- Numerales a los que aplica según circular 007: 3.2.3. - 3.2.6 - 3.2.7. - 3.11. - 4.1.1. - 4.1.2. - 4.2.3. - 4.3.1. - 4.3.5.

Instalación y upgrade de programas. Se debe contar con un listado de programas aprobados por la entidad e incluirlos en una lista blanca y monitorear todos los demás programas que se instalen y validar su procedencia al igual que contar con información de que usuario realizo estas acciones.

- Numerales a los que aplica según circular 007: 3.2.3. - 3.2.6 - 3.2.7. - 3.11. - 4.1.1. - 4.1.2. - 4.2.3. - 4.3.1. - 4.3.5.

Ejecución de programas y cambios de estado de los servicios. Monitorear tanto la ejecución de programas como los servicios que se tengan asociados, en este caso elaborar listas blancas de los procesos aprobados y si estos procesos deben estar siempre en ejecución configurar reglas que realicen estas tareas de manera automática.

- Numerales a los que aplica según circular 007: 3.2.3. - 3.2.6 - 3.2.7. - 3.11. - 4.1.1. - 4.1.2. - 4.2.3. - 4.3.1. - 4.3.5.

7.5.8. EVENTOS A MONITOREAR EN SERVIDORES DE APLICACIONES

Eventos de autenticación exitosos e intentos fallidos. Registrar logs de las autenticaciones exitosas y fallidas a las aplicaciones que se tengan para uso interno y externo garantizando que las personas que se están autenticando cuenten con los privilegios según sus roles.

- Numerales a los que aplica según circular 007: 3.2.3. - 3.2.6 - 3.2.7 - 3.4. - 3.5 - 4.1.1. - 4.3.1. - 4.3.5.

Creación, eliminación y cambios en las cuentas. Evidenciar todos los cambios realizados en cuanto a permisos de accesos a las aplicaciones como por ejemplo creación, eliminación y cambios en las cuentas identificando los responsables de esos cambios que sea el personal autorizado y ese aprobado por el comité de control de cambios.

- Numerales a los que aplica según circular 007: 3.2.3. - 3.2.6 - 3.2.7 - 3.4. - 3.5 - 4.1.1. - 4.3.1. - 4.3.5.

Inicio y cierre de aplicaciones y servicios. Garantizando la disponibilidad de servicios y continuidad de la operación es necesario monitorear las aplicaciones que hacen parte del core de negocio y configurar acciones automáticas que

reestablezcan el servicio.

- Numerales a los que aplica según circular 007: 3.2.3. - 3.2.6 - 3.2.7 - 4.1.9. - 4.2.3. - 4.3.1. - 4.3.5.

Fallas de aplicaciones y operacionales. La gran mayoría de aplicaciones cuentan con generación de códigos de errores en logs estos pueden ser utilizados para evidenciar en tiempo real los eventos de warning (aviso) antes de que llegue a producirse una afectación de servicios y causar indisponibilidad o incidente de seguridad.

- Numerales a los que aplica según circular 007: 3.2.3. - 3.2.6 - 3.2.7 - 4.1.9. - 4.2.3. - 4.3.1. - 4.3.5.

7.5.9. EVENTOS A MONITOREAR DE BASES DE DATOS

Monitoreo de los usuarios que ejecuten comandos o cambios en la base de datos. Se debe habilitar la auditoria en la base de dato para registrar la ejecución de estos eventos ya sean por parte de aplicaciones externas o por conexión directa desde algún motor de bases de datos evidenciando según sea la necesidad ejecuciones de insert, delete, update, create, grant, update.

- Numerales a los que aplica según circular 007: 3.2.3. - 3.2.6 - 3.2.7 - 4.3.5.

Captura de sentencias que han sido ejecutadas por los usuarios. Así como se monitorean acciones básicas como las mencionadas anteriormente, también es necesario una auditoria más profunda donde se vea toda la sentencia ejecutada, el origen, destino y demás de información relevante que registre el log.

- Numerales a los que aplica según circular 007: 3.2.3. - 3.2.6 - 3.2.7 - 4.3.5.

7.5.10. EVENTOS A MONITOREAR DE UN FILESERVER - REPOSITORIO DE ARCHIVOS

Autenticaciones al servidor y acceso a los recursos compartidos. Evidenciar las cuentas que están accediendo a los recursos compartidos en la red y de las cuentas que registran acceso fallido haciendo énfasis en estas descartando que sean intentos de acceso forzado.

- Numerales a los que aplica según circular 007: 3.2.3. - 3.2.6 - 3.2.7 - 3.4. - 3.5 - 3.7.1. - 4.1.1.- 4.1.2. - 4.3.1. - 4.3.5.

Creación, modificación y eliminación de archivos. Mantener el registro de los cambios o acciones que tienen sobre los recursos compartidos, principalmente en las rutas críticas de almacenamiento de información en el file server.

- Numerales a los que aplica según circular 007: 3.2.3. - 3.2.6 - 3.2.7 - 3.7.1. - 4.1.1. - 4.1.2. - 4.2.1. - 4.3.1. - 4.3.5.

6. PRUEBA DE CONCEPTO

El mercado ofrece varias soluciones SIEM, unas Open Source y la gran mayoría de pago las cuales se destacan por sus fabricantes, estas tienen en común las características y funciones explicadas anteriormente por lo que para la prueba de concepto se realiza con un SIEM de Solarwinds con el cual se busca demostrar el apoyo que este software brinda a la circular 007 a los requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad teniendo en cuenta el análisis que se realizó de los numerales y los dispositivos con los que deben contar las cooperativas financieras según la circular 042.

Se cuenta con un ambiente donde se tienen monitoreados unos servidores de aplicaciones como bases de datos, antivirus y un servidor de archivos, en estos se tiene instalado un agente del SIEM el cual se encarga de recopilar eventos y de generar varias acciones sobre los servidores.

7.6.1. MONITOREO DE HORARIOS LABORALES

Para esta prueba se tuvieron como foco en los numerales de la circular 3.4. Implementar controles para mitigar los riesgos que pudieran afectar la seguridad de información confidencial, en reposo o en tránsito, 4.1.1. Establecer, mantener y documentar los controles de acceso (lógicos, físicos y procedimentales) y gestión de identidades bajo la premisa que las personas solo pueden disponer de los recursos que demande su trabajo, durante el tiempo que ello sea necesario. 4.1.2 Adoptar políticas, procedimientos y mecanismos para evitar la fuga de datos e información. 4.3.1 Establecer procedimientos de respuesta a incidentes cibernéticos tales como: desconexión automática de equipos, cambios de contraseñas, actualizar la base de firmas del antivirus, bloqueo de direcciones IP o cualquier otro que determine la entidad.

Se define el horario aprovado para laborar (Figura 10)en la entidad de 7:00am a 6:00pm de lunes a viernes, hay que tener claro que se pueden realizar ventanas de mantenimiento programadas o posiblemente se manejen turnos 7x24 por lo que seria necesario establecer una lista con los usuarios para excluirlos de los alertamientos.

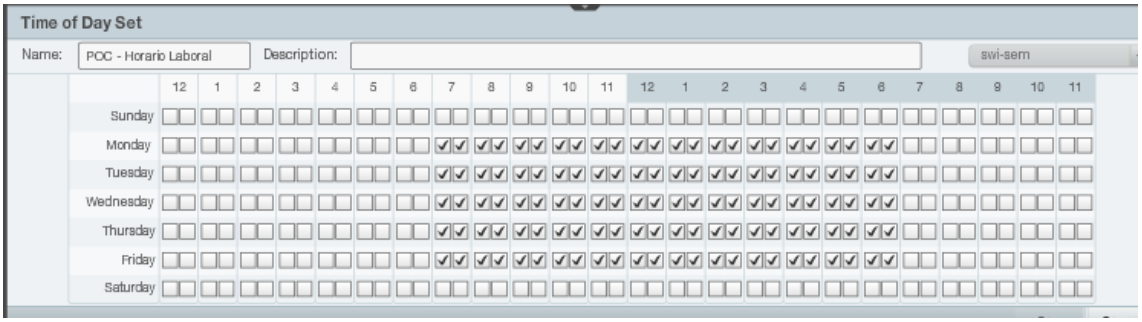


Figura 10. Horario Laboral

- Regla configurada

Se establen las condiciones que debe cumplir para activar la regla (Figura 11), como se ve en la primera condición se aclara que se haber un evento de UserLogon es decir una autenticación de satisfactoria desde cualquier fuente de información, en la segunda que el evento no debe ser detectado dentro de POC – Horario Laboral, para las últimas tres condiciones se establece que solo se debe cumplir una de ellas: que sea una autenticación de tipo Windows: Remote Desktop, Windows: interactive y Windows Interactive Logon, cada una de estas es decir que el usuario tenga interacción con una maquina ya que si no lo aclaramos podemos activar la regla con una autenticación de tipo Network y esta es muy comun que registre actividad cuando no se apaga un equipo y esta ejecuntando procesos en segundo plano.

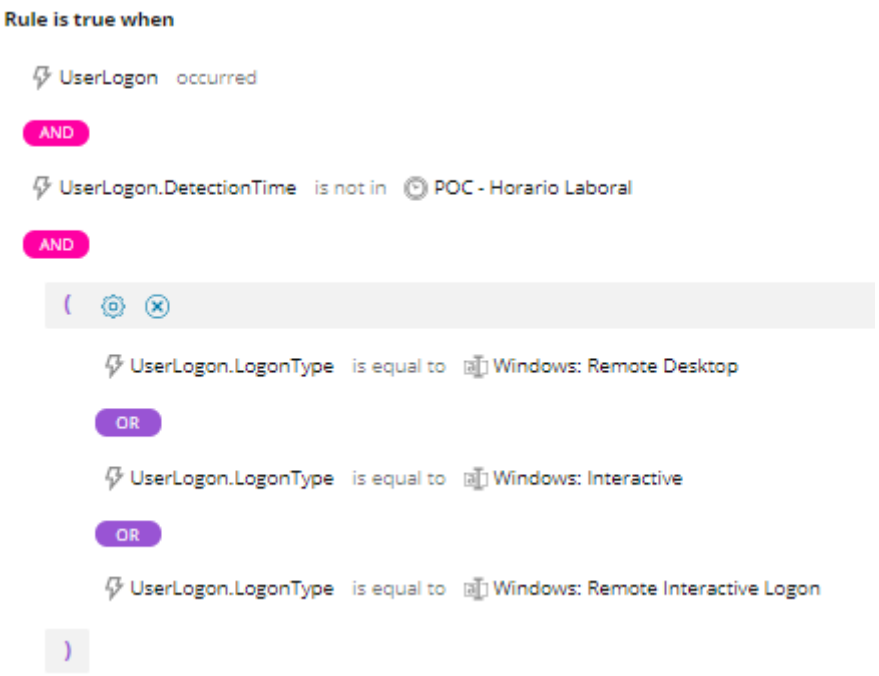


Figura 11. Regla configurada

- Acciones a ejecutar ante el evento o posible incidente.

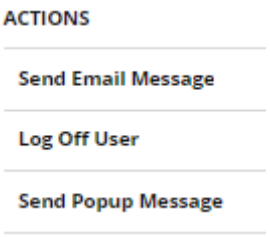


Figura 12. Acciones configuradas

Send Email Message: Enviará un correo electrónico mostrando información del evento.
Log Off User: Cierra la sesión abierta
Send Popup Message: Mostrará un mensaje en pantalla.
Dashboard: Se configurá para que se vean los eventos del ultimo día.

- Pruebas

Se conecta desde un equipo a un servidor al que se tenian permisos de acceso y este sistema genera el siguiente evento (Figura 13) con el que cumple las condiciones de la regla para activarse según cada uno de sus campos (Figura 14).

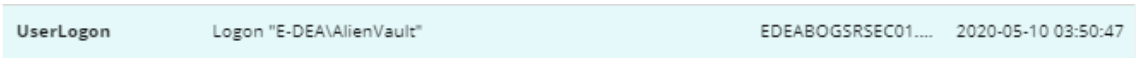


Figura 13 Evento generado

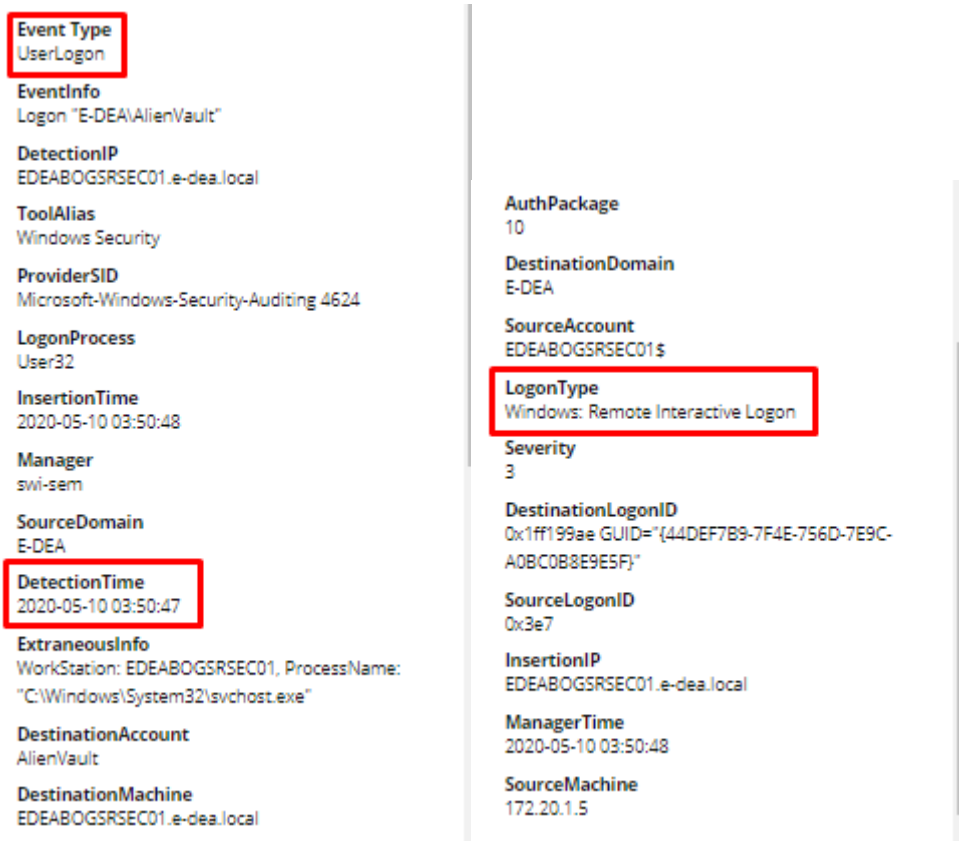


Figura 14 Campos en el evento generado de UserLogon

- Resultado

Se disparan las acciones configuradas: mensaje Pop Pup (Figura 15), Log Off User (Figura 16), Send Mail Message (Figura 17) y activación de Dashboard (Figura 18).

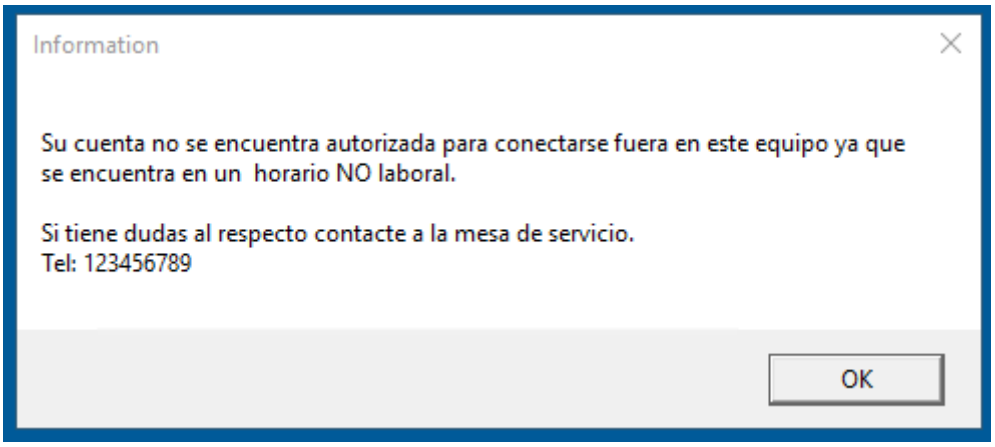


Figura 15. Popup en pantalla de carácter informativo

Se registra el evento de cerrado de sesión en el servidor.

Figura 16.Evento generado al dispararse la acción de Log Off User

Se recibe el correo electrónico con información de un evento para realizar.

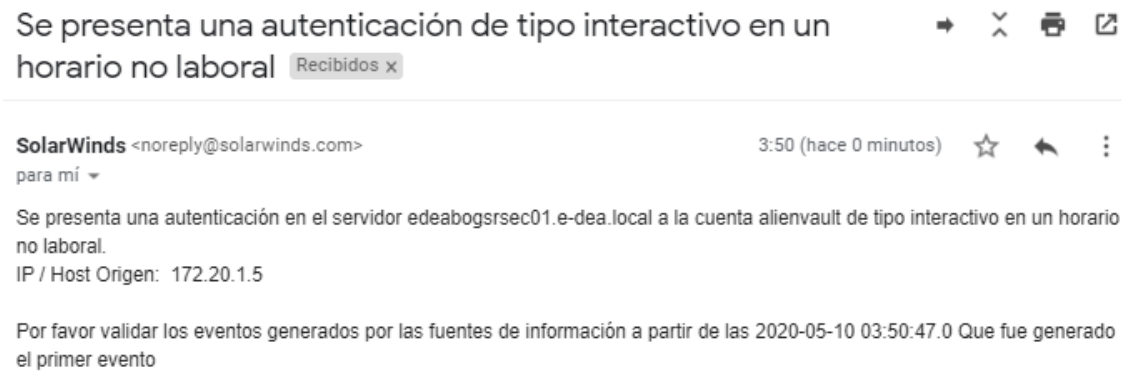


Figura 17. Activación del envió de correo

Figura 18. Dashboard con usuarios conectados fuera del horario laboral

7.6.2. SEGREGACIÓN DE USUARIOS Y RESPUESTA AUTOMÁTICA.

Para esta prueba se enfocó en los numerales de la circular 3.5 donde indica que se deben segregar las funciones y responsabilidades de los usuarios con privilegios y el numeral 4.3.1 que indica que se deben establecer respuestas ante los incidentes.

Se ha definido una lista de usuarios (Figura 19) los cuales tienen permitido autenticarse en unos servidores de virtualización de la entidad (Figura 20), si llega a presentarse una autenticación a estos servidores desde cuentas que no están autorizadas dentro de ese listado se generará una respuesta automática mostrando un mensaje de alerta y posteriormente se cerrará la sesión.

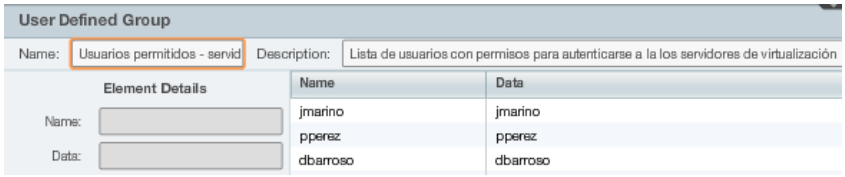


Figura 19. Lista de usuarios permitidos para conectarse

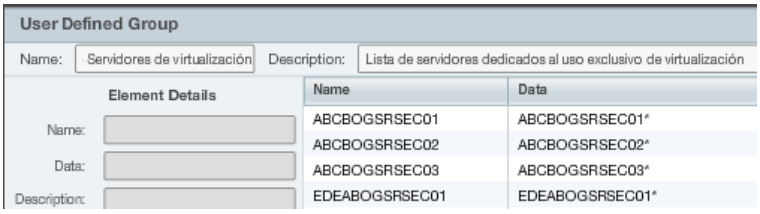


Figura 20. Lista de servidores.

- Regla configurada

  Se especifican los campos o condiciones con los que debe cumplir para ejecutar las acciones.
  Para la primera condición debe coincidir con una autenticación en el servidor, la segunda condición es que el evento sea de tipo “interactive” este tipo de evento se genera cuando se desbloquea la sesión de un computador y se tiene control interactivo, para la tercera condición que la IP de detención es decir la fuente que genera el evento debe pertenecer al “POC – Servidores de virtualización” (Figura 20) y como cuarta condición que sea un usuario que no esté contenido dentro del grupo “POC – Usuarios permitidos – servidores de virtualización” (Figura 19)

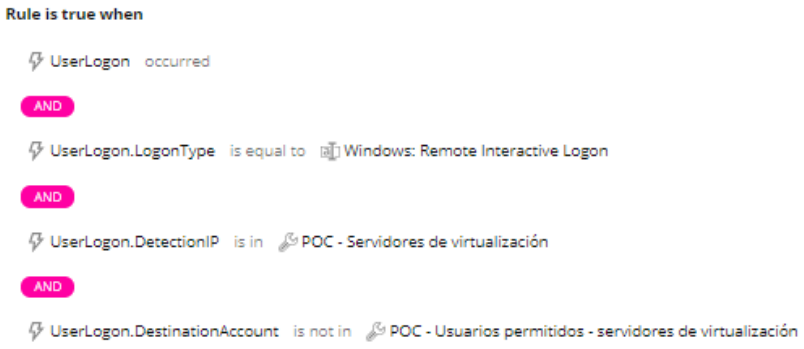


Figura 21. Regla de correlación configurada.

- Acciones a ejecutar ante el evento o posible incidente

  Se configuran las siguientes acciones de respuesta automática.

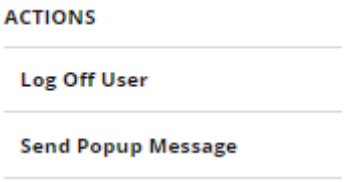


Figura 22. Acciones a ejecutar.

Log Off User: Cerrará la sesión abierta por el usuario.
Send Popup Message: Mostrará un mensaje en pantalla.

- Pruebas

  Se realiza desde un equipo de escritorio una conexión a uno de los servidores de la lista (Figura 19) y se evidencia el evento generado (Figura 23) y a partir de este se dispara la regla configurada cumpliendo con los parámetros de correlación los cuales se resaltan en la imagen.

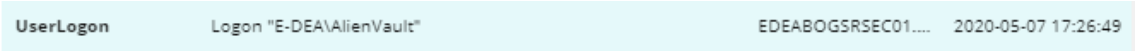


Figura 23. Evento generado desde un servidor de la lista

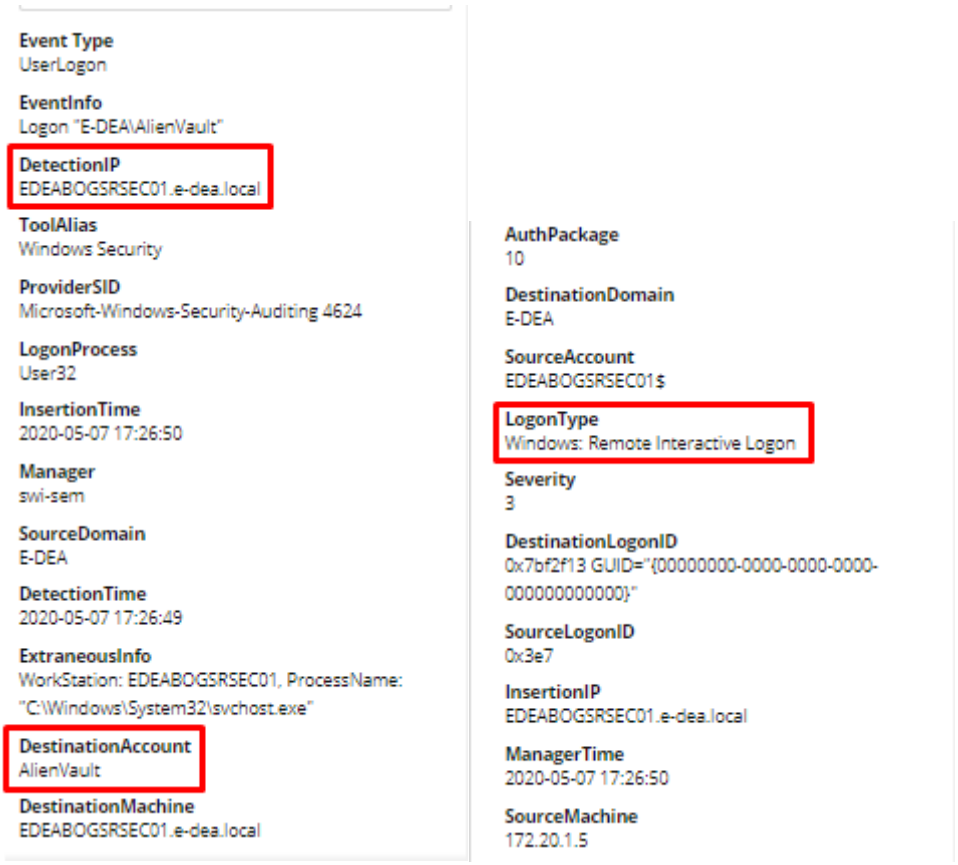


Figura 24. Campos del evento de conexión por escritorio remoto

- Resultado

  Se evidencia en la sesión de escritorio remoto que aparece el mensaje que se configuró en la regla como primera acción y posterior se dispara la segunda acción la cual cerrará la sesión automáticamente.

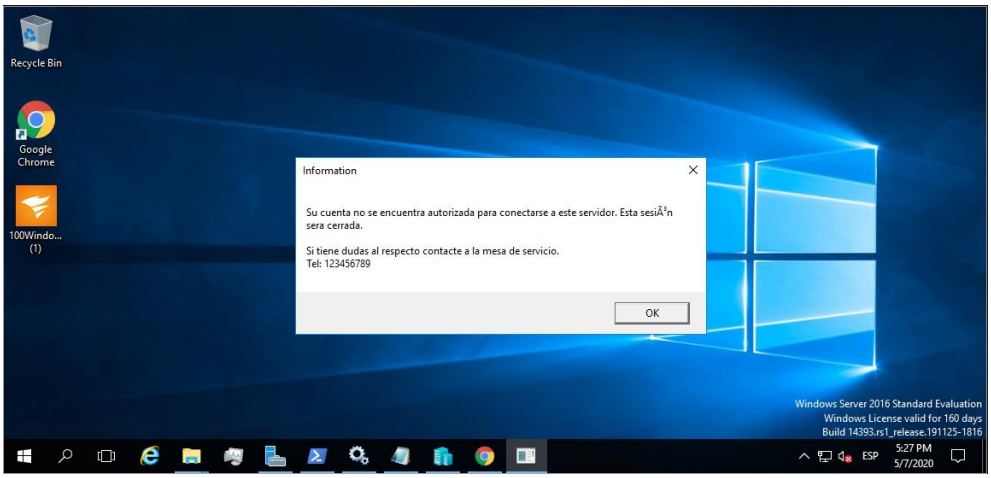


Figura 25. Acciones ejecutadas automáticamente por la regla de correlación.

7.6.3. DESCUBRIMIENTO DE SOFTWARE DE SEGURIDAD Y REINICIO DE SERVICIOS

Para esta prueba se enfocó en dos técnicas utilizadas por ciberdelincuentes cuando ya logran tener control de algunos equipos o servidores y pueden ejecutar varias acciones como la técnica T1063 - Security Software Discovery (Mitre ATT&CK), tiene que ver cuando los adversarios obtienen una lista de software de seguridad, configuraciones, herramientas defensivas y sensores instalados en el sistema y la técnica T1489 - Service Stop (Mitre ATT&CK) donde los adversarios pueden detener o deshabilitar los servicios en un sistema para que esos servicios no estén disponibles para usuarios legítimos. La interrupción de los servicios críticos puede inhibir o detener la respuesta a un incidente o ayudar a los objetivos generales del adversario a causar daños al medio ambiente.

Se realiza un listado de procesos más comunes que se ejecutan en los servidores Windows dentro los cuales se encuentran agentes de antivirus, de monitoreo, de firewall, anti-spyware y se aplica la técnica T1063 - Security Software Discovery de Atomic Red Team que es un grupo enfocados a realizar pruebas individuales (atómicas) de MITRE ATT&CK Framework[22].

Nombre	Procesos
Anti-Trojan	*\ANTI-TROJAN*
Avast	*\AVASTSVC *
AVG Business Security	*\AVGSVC *
Bitdefender	*\VSSERV *
Eset nod32	*\EKRN *
F-Prot	*\FPROT *
F-Prot 2	*\F-PROT *
F-Prot 3	*\F-PROT95 *
F-secure antivirus	*\FSHOSTER32 *
IBM	*\IBMASN *
IBM 2	*\IBMAVSP*
Kapersky	*\AVP.EXE*
McAfee	*\VSHWIN32*
McAfee 2	*\MFEMMS*
Norton AV	*\NAVNT*
Norton AV 2	*\NAVW32*
Norton AV 3	*\NAVWNT*
PC-Cillin	*\PCCWIN98*

[22] Descubrimiento de software de seguridad. Mitre ATT&CK. [On-line]

Sophos	*\SAVSERVICE*
Trend Micro Antivirus	*\CORESERVICESHELL*
USB Defender	*USB-Defender*
Webroot	*\WRSA*
Windows Defender	*\MSMPENG*
ZoneAlarm	*\ZONEALARM*

Tabla 3. Listado de procesos seguros de agentes de antivirus

- Regla configurada

  La regla se activará al reconocer que ha recibido un evento de ServiceStop (servicio detenido) del grupo POC – Procesos seguros.

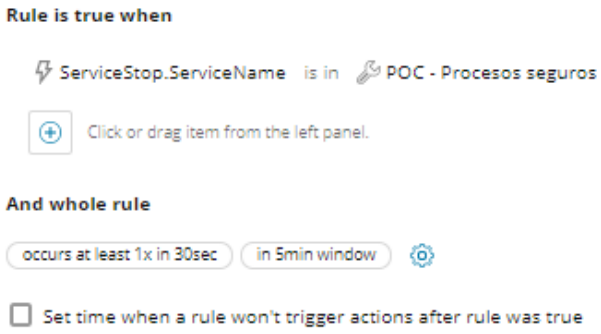


Figura 26. Regla de correlación configurada.

- Acciones a ejecutar ante el evento o posible incidente

  Se configuran las siguientes acciones de respuesta automática

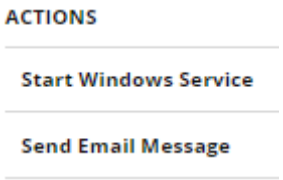


Figura 27.Acciones de respuesta configuradas.

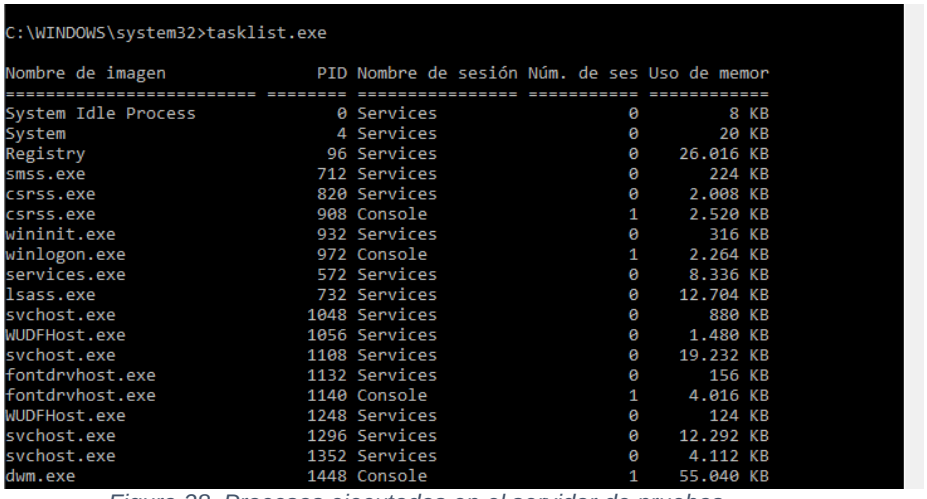
  Start Windows Service: Inicia automáticamente el servicio que se registró como detenido y se encuentre dentro del listado de procesos seguros.
  Send Email Message: Enviará un correo electrónico mostrando información del evento.

- Pruebas

Dentro de uno de los servidores ejecutamos las siguientes líneas de código con el que los adversarios pueden intentar obtener una lista de software de seguridad, configuraciones, herramientas defensivas y sensores instalados en el sistema. Este incluye las reglas de firewall local, antivirus y agentes.

```
tasklist.exe
tasklist.exe | findstr /i virus
tasklist.exe | findstr /i Protection
tasklist.exe | findstr /i defender
tasklist.exe | findstr /i AV
tasklist.exe | findstr /i anti
tasklist.exe | findstr /i agent
```

La primera línea muestra las tareas que están corriendo en el servidor.



```
C:\WINDOWS\system32>tasklist.exe

Nombre de imagen              PID Nombre de sesión Núm. de ses Uso de memor
========================= ======== ================ =========== ============
System Idle Process             0 Services                   0         8 KB
System                          4 Services                   0        20 KB
Registry                       96 Services                   0    26.016 KB
smss.exe                      712 Services                   0       224 KB
csrss.exe                     820 Services                   0     2.008 KB
csrss.exe                     908 Console                    1     2.520 KB
wininit.exe                   932 Services                   0       316 KB
winlogon.exe                  972 Console                    1     2.264 KB
services.exe                  572 Services                   0     8.336 KB
lsass.exe                     732 Services                   0    12.704 KB
svchost.exe                  1048 Services                   0       880 KB
WUDFHost.exe                 1056 Services                   0     1.480 KB
svchost.exe                  1108 Services                   0    19.232 KB
fontdrvhost.exe              1132 Services                   0       156 KB
fontdrvhost.exe              1140 Console                    1     4.016 KB
WUDFHost.exe                 1248 Services                   0       124 KB
svchost.exe                  1296 Services                   0    12.292 KB
svchost.exe                  1352 Services                   0     4.112 KB
dwm.exe                      1448 Console                    1    55.040 KB
```

Figura 28. Procesos ejecutados en el servidor de pruebas

Con las siguientes líneas de código mostrará específicamente de ese listado los procesos que tengan nombres relacionados con “virus, protection, defender, AV, anti y agent”

Figura 29. Búsqueda de servicios con nombres relacionados a "virus, protection, defender, AV, anti y agent"

Con esta información los atacantes ya pueden detener los servicios con lo cual se afecta la gestión o monitoreo de nuestros servidores, se aplicará la técnica T1489 - Service Stop.

Para continuar con este ejemplo se detendrá el servicio de USBDefender.exe el cual se encuentra en el listado de procesos seguros (Tabla 3) del SIEM con la siguiente línea ejecutas en PowerShell.

```
Stop-Service -Name USB-Defender
```

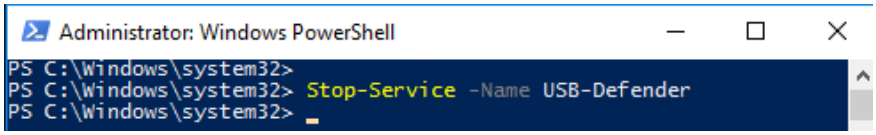


Figura 30. Ejecución de comando en powershell

Se generará el siguiente evento en el SIEM

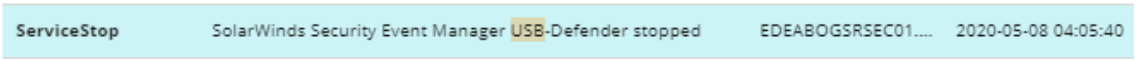


Figura 31. Se recibe el evento de servicios detenidos en el servidor

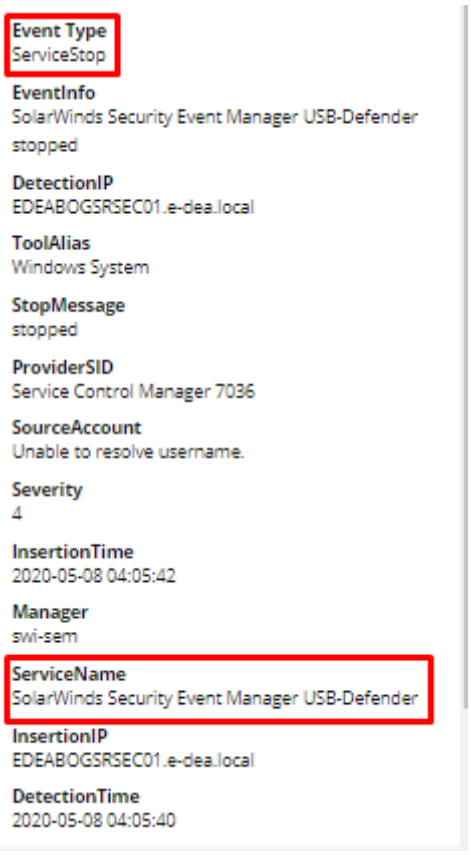


Figura 32. Campos del evento de ServiceStop

- Resultado

  Se envió el correo electrónico según una platilla configurada donde se muestran las variables como el servicio, el servidor que fue fuente del evento y un análisis y el ID según Mitre Att&ck.

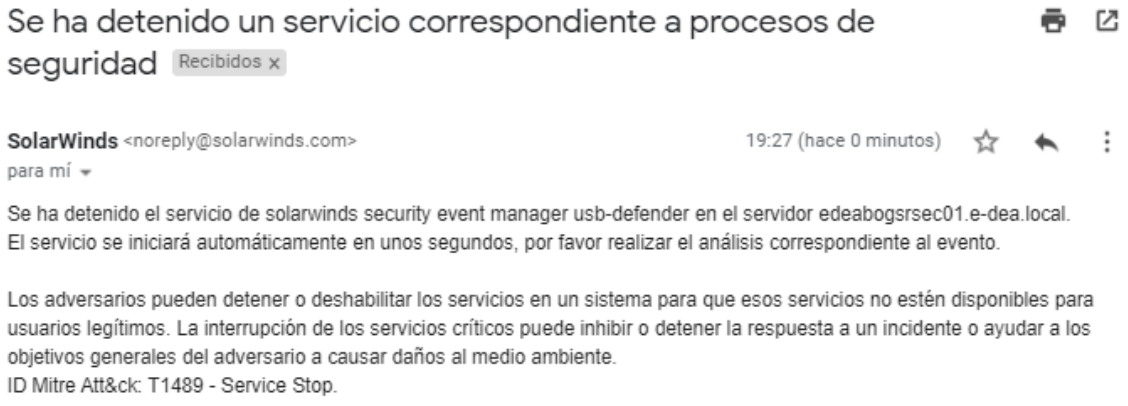


Figura 33. Correo enviado al activarse la regla de correlación.

Posteriormente muestra que el servicio ha sido iniciado de manera automática (Figura 34) con menos de 1 segundo de indisponibilidad, lo que es favorable ya que la interrupción de los servicios críticos puede inhibir o detener la respuesta a un incidente o ayudar a los objetivos del adversario a causar daños ya que los atacantes no podrán realizar cambios que tengan dependencia del servicio.

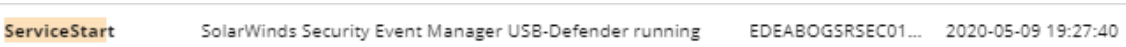


Figura 34.Reinicio de servicio. Acción automática realizada al activarse la regla.

7.6.4. EJECUCIÓN DE SOFTWARE NO PERMITIDO

Para esta prueba se enfocó en los numerales de la circular 3.4 donde indica que se deben implementar controles para mitigar los riesgos que pudieran afectar la seguridad de información confidencial, en reposo o en tránsito, 3.5 donde indica que se deben segregar las funciones y responsabilidades de los usuarios con privilegios de administrador o que brindan soporte remoto, para mitigar los riesgos de seguridad de la información, 4.1.2. Adoptar procedimientos y mecanismos para evitar la fuga de datos e información, el numeral 4.3.1 que indica que se deben establecer respuestas ante los incidentes y la técnica T1021 de servicios remotos la cual el adversario puede utilizar para aceptar conexiones remotas, como software de terceros y realizar acciones como usuario conectado.

Se define un listado de ejecutables utilizados para conexiones remotas (Tabla 4) y un grupo de usuarios que cuentan con altos privilegios, para este caso en específico pueden realizar la ejecución de software y utilizarlo.

Nombre del Software	Ejecutable
Anydesk	*\AnyDesk.exe
Generic VNC	*\vnc*
GoToMeeting	*\g2mcomm.exe*
GoToMeeting 10	*\g2mview.exe*
GoToMeeting 2	*\g2mchat.exe*
GoToMeeting 3	*\g2mhost.exe*
GoToMeeting 4	*\g2mInstaller.exe*
GoToMeeting 5	*\g2mlauncher.exe*
GoToMeeting 6	*\g2mmatchmaking.exe*
GoToMeeting 7	*\g2msessioncontrol.exe*
GoToMeeting 8	*\g2mstart.exe*
GoToMeeting 9	*\g2mui.exe*
GoToMyPC	*\gotomypc.exe*

MS Remote Desktop	*\mstsc.exe*
MS Telnet Server	*\tlntsvr.exe*
MyWebExPC	*\atagtctl.exe*
MyWebExPC 2	*\raagtx.exe*
MyWebExPC 3	*\raagtapp.exe*
MyWebExPC 4	*\atnthost.exe*
PC Anywhere	*\awhost32.exe*
PC Anywhere 2	*\ph32svc.exe*
WebEx	*\atcliun.exe*
WebEx 2	*\atmgr.exe*
WebEx 3	*\atshell.exe*

Tabla 4. Listado de software para conexiones remotas. POC – Software de escritorio remoto

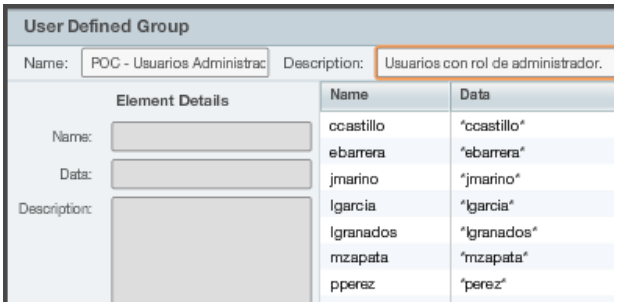


Figura 35. Listado de usuarios con rol de administrador. POC – Usuarios Administradores

- Regla configurada

  La regla se activará el detectar que un proceso ha sido iniciado y que pertenezca a uno de los procesos que están incluidos en la lista POC – Software de escritorio remoto (Figura 34) y que la cuenta de origen sea diferente a las cuentas de la lista POC – Usuarios Administradores (Figura 35).

Figura 36. Configuración de regla de correlación.

- Acciones a ejecutar ante el evento o posible incidente.

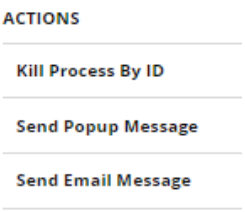


Figura 37. Acciones configuradas de respuesta automática.

Kill Process By ID: Cerrará el ID proceso desencadenado por la ejecución del software.
Send Popup Message: Mostrará un mensaje en pantalla.
Send Email Message: Enviará un correo electrónico mostrando información del evento.

- Pruebas

Se realiza la prueba con la aplicación de AnyDesk la cual se ejecuta en el computador.

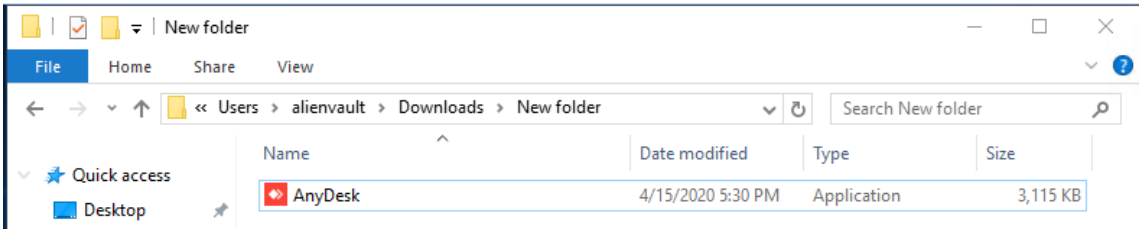


Figura 38. Software a utilizar para la prueba

Se genera el evento desde nuestra fuente de información en este caso el sistema operativo del computador y muestra los siguientes campos que corresponden a las condiciones configuradas en la regla.

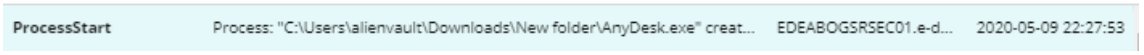


Figura 39. Evento generado al abrir la aplicación de AnyDesk.

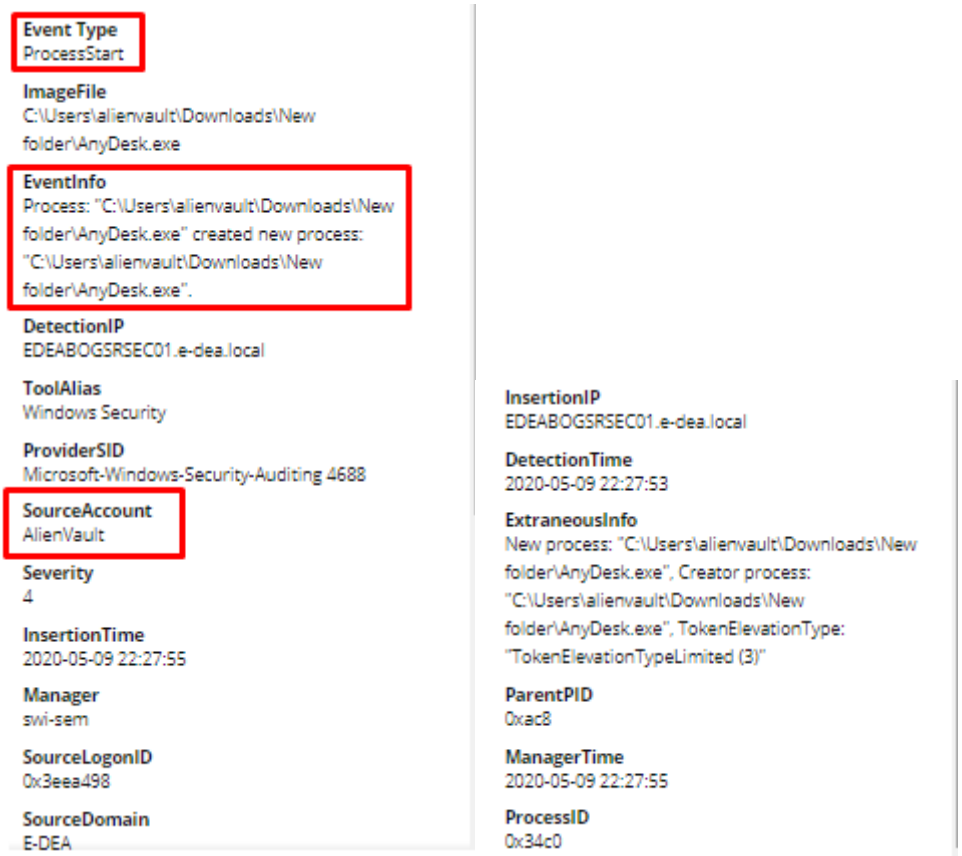


Figura 40. Campos del evento generado por abrir la aplicación de AnyDesk desde nuestra fuente de información.

- Resultado

  Se evidencia que dos segundos después de detectar el evento genera un nuevo evento informando que ya se ha cerrado el proceso generado por el software (Figura 42)

Figura 41. Evento de finalización del proceso de AnyDesk.

Posteriormente mostrará un mensaje en la pantalla del usuario dándole información acerca de lo que ha pasado (Figura 42.)

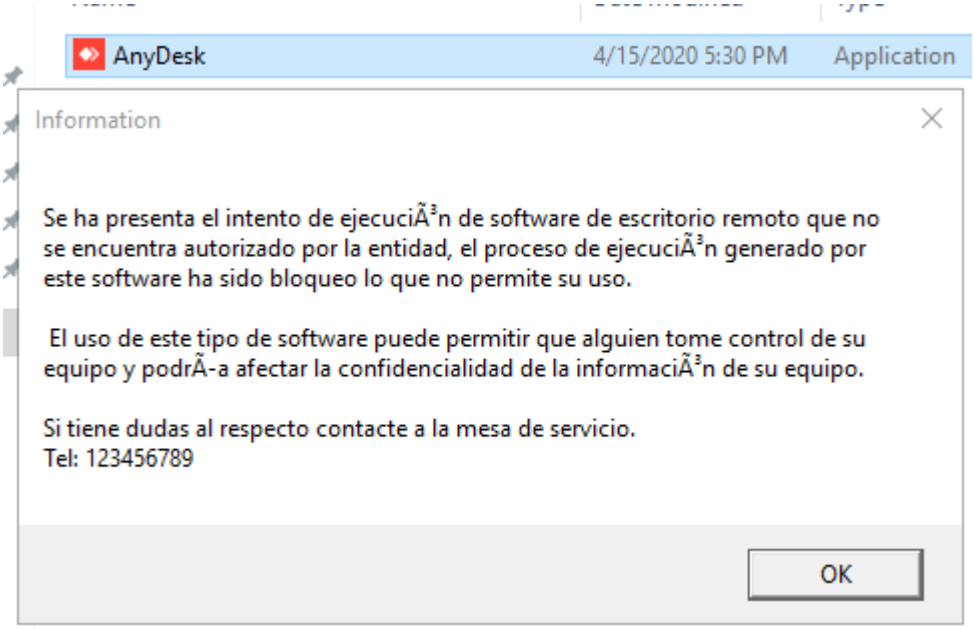


Figura 42. Mensaje Popup disparado por la regla como acción automática.

Por último, se evidencia él envió de correo electrónico con información acerca del evento.

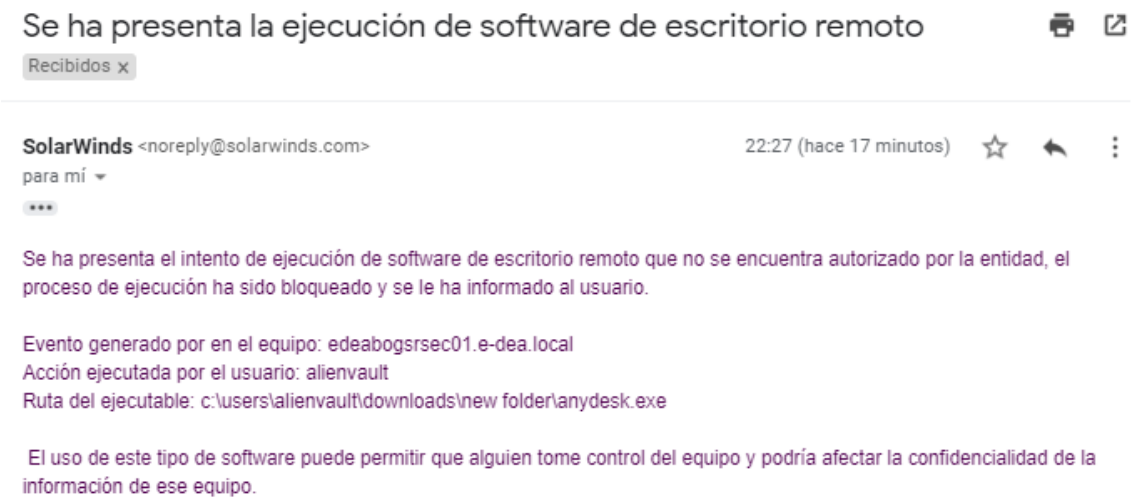


Figura 43. Correo recibido como respuesta automática al activarse la regla de correlación.

7.6.5. GENERACIÓN DE REPORTES

Los SIEM cuentan con la función de generar reportes para diferentes enfoques ya

sea realizar un análisis de datos, tener evidencia probatoria, un análisis de un incidente o para cumplir con procesos establecidos por las entidades regulatorias. En este caso se utilizó una aplicación de reportes del fabricante Solarwinds donde ya cuenta con reportes preestablecidos para el cumplimiento de diferentes normativas como lo es PCI que es una de las conocidas del sector bancario (Figura 44).

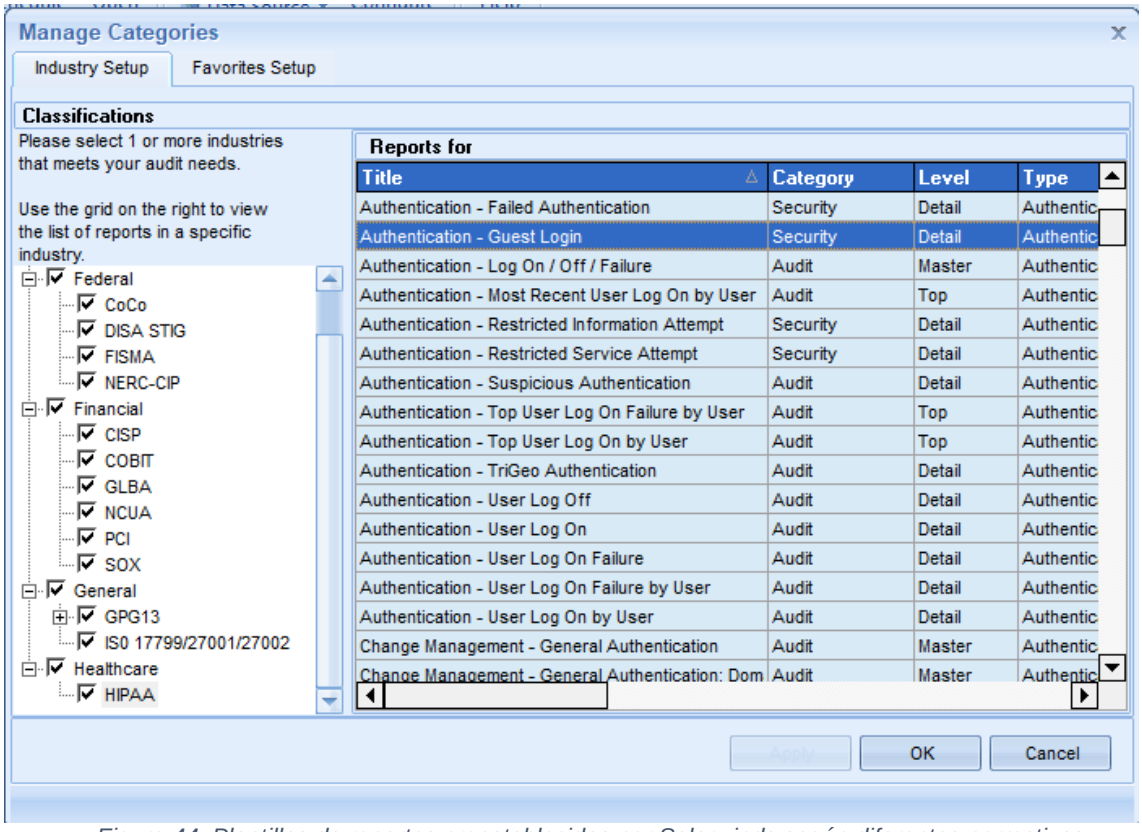


Figura 44. Plantillas de reportes preestablecidos por Solarwinds según diferentes normativas.

Para esta prueba se enfocó en los numerales 3.2.3 debe reportar a la junta directiva y a la alta dirección, los resultados de su gestión, 3.2.7 asesorar a la alta gerencia y la junta directiva en temas que considere necesarios sobre seguridad de la información y ciberseguridad para que estas últimas puedan hacer seguimiento y tomar las decisiones adecuadas en esta materia, 3.5. emplear mecanismos para la adecuada autenticación y segregar las funciones y responsabilidades de los usuarios con privilegios de administrador o que brindan soporte remoto, para mitigar los riesgos de seguridad de la información, 3.11. Contar con indicadores para medir la eficacia y eficiencia de la gestión de la seguridad de la información y la ciberseguridad, 4.1.1. Establecer, mantener y documentar los controles de acceso (lógicos, físicos y procedimentales) y gestión de identidades bajo la premisa que las personas solo pueden disponer de los recursos que demande su trabajo, durante el tiempo que ello sea necesario, 4.2.3.

Realizar un monitoreo continuo a su plataforma tecnológica con el propósito de identificar comportamientos inusuales que puedan evidenciar ciberataques contra la entidad, 4.3.5 En la medida de lo posible, preservar las evidencias digitales para que las áreas de seguridad o las autoridades puedan realizar las investigaciones correspondientes.

Se aplicó la generación de un reporte de autenticaciones satisfactorias, cierre de sesión y fallos de autenticación (Figura 45) en un periodo de tiempo de una semana para la muestra.

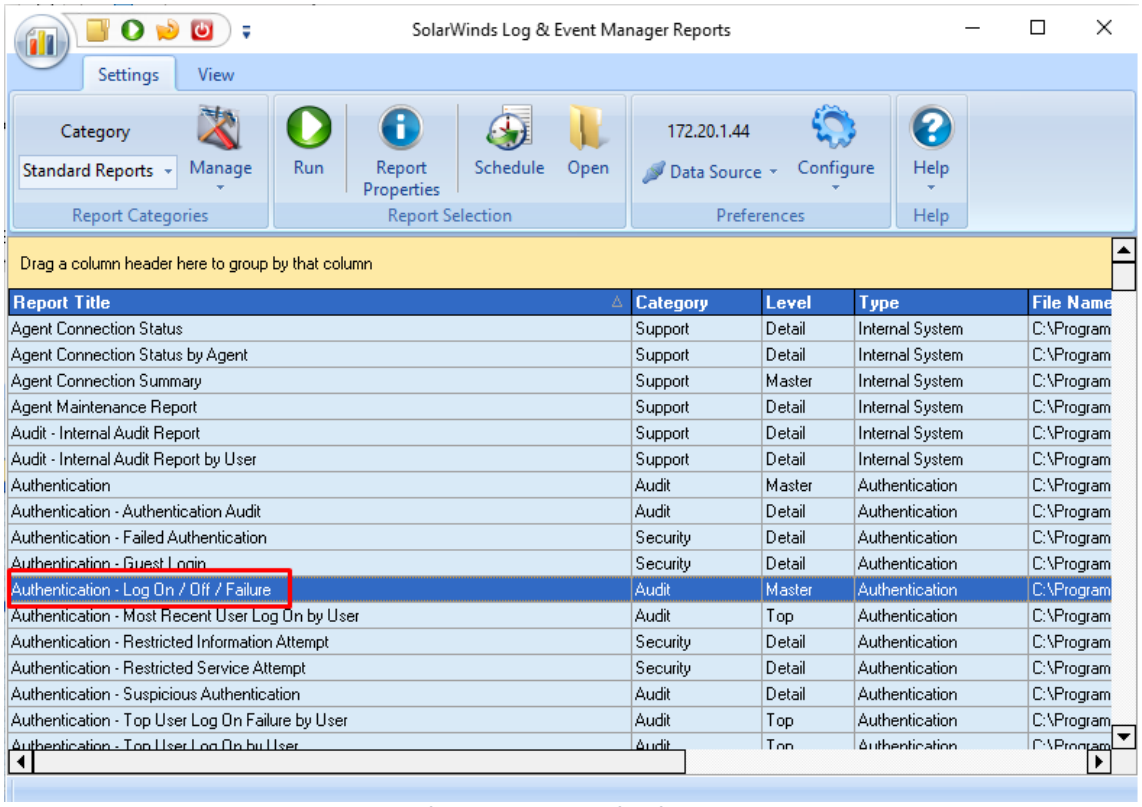


Figura 45. Generador de reportes.

Se obtiene los siguientes resultados como reporte donde muestra los resultados en una gráfica (Figura 46) y una tabla con el detalle de los resultados (Figura 47), la cual se puede exportar en diferentes formatos dependiendo del uso que se le quiera dar.

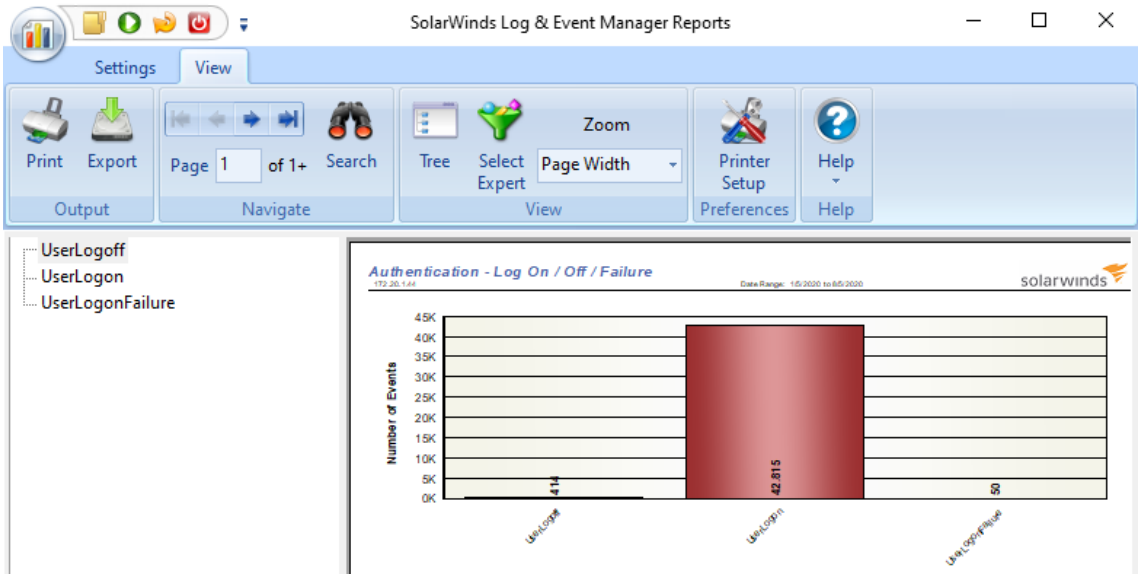


Figura 46. Reporte generado de autenticaciones satisfactorias, cierre de sesión y fallos de autenticación

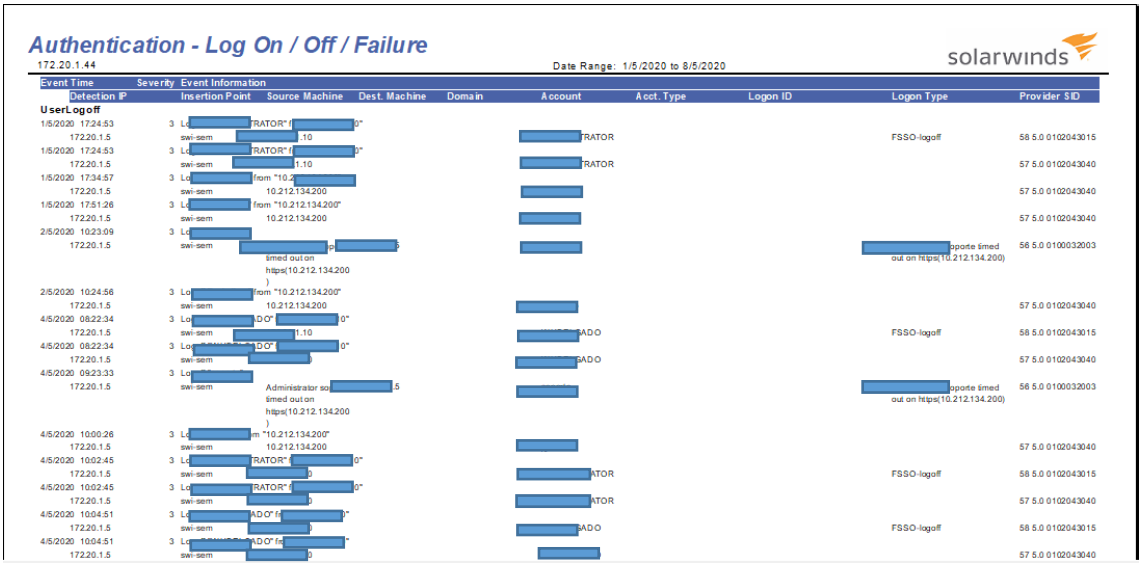


Figura 47. Reporte de autenticaciones satisfactorias, cierre de sesión y fallos de autenticación

8. CONCLUSIONES

Se evidenció que la superintendencia en la circular 007 no especifica en sus lineamientos que sistemas de información se deben monitorear por lo que se debe realizar un análisis basado en otras normas o circulares que apliquen al sector financiero para integrarlos al SIEM.

Se identifica que toda entidad financiera debería tener un ambiente de pruebas en donde puedan generar ataques simulados y bajo control, identificando mediante sus diferentes herramientas de seguridad y apoyándose en el SIEM para detectarlos a tiempo y no cuando se hubiesen materializado y generado incidentes dentro de la entidad.

Con el monitoreo adecuado de los eventos presentados en este trabajo de buenas prácticas no solo se lograrán identificar los eventos para evidencias o reportes, sino que también se agilizan los procesos o acciones ante posibles incidentes de seguridad con las respuestas activas que tienen los SIEM no obstante como la tecnología va avanzando los cibercriminales también irán cambiando sus técnicas de ataques por lo que siempre hay que estar actualizado ante nuevas amenazas.

Mientras se realizaba la prueba de concepto de las buenas prácticas a monitorear se identifica que en cada una de las fuentes de información hay que definir y configurar la adecuada auditoria con el fin de generar los logs o eventos específicos con el que se quiere alimentar al SIEM ya que se puede generar logs innecesarios que pueden sobrecargar el rendimiento tanto de la fuente de información como del SIEM.

Cuando se planifico el desarrollo de este trabajo las expectativas en cuanto los resultados en la prueba de concepto eran más amplios, pero generar un tipo de alertamiento para cada evento resultaba muy extenso, pero con las reglas configuradas se cubre una gran parte de los eventos que se querían monitorear de los sistemas de información además de cubrir con varias técnicas utilizadas por los cibercriminales según Mitre Att&ck al sector bancario.

9. BIBLIOGRAFÍA

ARACIL ORDUÑA, E. 2019. Desarrollo y Despliegue de Servicios Web integrados mediante un Servidor de Autenticación único basado en Roles. Universidad Autónoma De Madrid. Escuela Politécnica Superior. Pag. 8. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/688990/aracil_ordu%c3%b1a_enrique_tfg.pdf?sequence=1&isAllowed=y

Asobancaria. Informe Internacional de Regulación- edición N° 31. Developer Increnta. COMUNICADO DE PRENSA 13 / 10 de mayo de 2019. Disponible en: https://www.asobancaria.com/informe-mensual/

AVELLA CORONADO, J. D.; CALDERON BARRIOS, L. F.; MATEUS DÍAS, C. A. 2015. Guía Metodológica para la gestión centralizada de registros de seguridad a través de un siem [on-line]. Tesis- Especialista en Seguridad en Redes Pag. 17. Universidad Católica de Colombia. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/2847/1/GU%C3%8DA%20METODOL%C3%93GICA%20PARA%20LA%20GESTI%C3%93N%20CENTRALIZADA%20DE%20REGISTROS%20DE%20SEGURIDAD%20A%20TRAV%C3%89S%20DE%20UN%20SIEM.pdf

CARBONÓ CARBONÓ, D. 2013. Amenazas persistentes avanzadas. Especialización Seguridad Informática Universidad Piloto de Colombia. ATPs. Disponible en: http://polux.unipiloto.edu.co:8080/00002479.pdf
Descubrimiento de software de seguridad. Mitre ATT&CK. [On-line] Disponible en: https://attack.mitre.org/techniques/T1063/

CHINE LÓPEZ, J. 2014. Tipos de herramientas básicas para garantizar la ciberseguridad en la empresa [on-line]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/herramientas-basicas-ciberseguridad-empresa

FERNÁNDEZ GRANADOS, J. E.; HERRERA Kairuz, J. H.; GARCÍA, J. C. Implementación de un security information and event management –siem– en el comando de la armada nacional [on-line]. Dirección de tecnologías de la información y las comunicaciones. Tesis - Especialización en Seguridad Informática – Pag.18. Universidad Piloto de Colombia. Disponible en: http://polux.unipiloto.edu.co:8080/00003801.pdf

Financial Services Attack Economy. Akamai Intelligent Security Starts at the Edge. Vol 5, Issue 4. On-line: https://www.akamai.com/es/es/multimedia/documents/state-of-the-internet/soti-security-financial-services-attack-economy-report-2019.pdf

Gestión de Riesgo. Circular externa 007 [on-linne]. 2018. Disponible en:

https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/10097769/f/0/c/00

GUERRERO LÓPEZ, F. A.; RODRÍGUEZ PINILLA, J. E. 2013. diseño y desarrollo de una guía para la implementación de un ambiente big data en la universidad católica de colombia. Universidad Católica de Colombia. Trabajo de Grado para optar al título de Ingeniero de Sistemas. Pag. 46. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/1320/1/DISE%c3%91O%20Y%20DESARROLLO%20DE%20UNA%20GU%c3%8dA%20PARA%20LA%20IMPLEMENTACI%c3%93N%20DE%20UN%20AMBIENTE%20BIG%20DATA%20EN%20LA%20UNIVERSIDAD%20CAT%c3%93LICA%20DE%20COLOMBIA.pdf

Grupo Smartekh. ¿Qué es Hardening? [on-line]. 2012. Disponible en: https://blog.smartekh.com/que-es-hardening

HEINERT VILLACIS, L. A. Implementación De Una Solución Data Loss Prevention (Dlp) En Una Empresa Con Actividades De Servicios Alimenticios [on-line]. Tesis- Magister en seguridad informática aplicada Pag.3. 2016. Escuela Superior politécnica del litoral. Facultad de Ingeniería en Electricidad y Computación. Disponible en: http://www.dspace.espol.edu.ec/xmlui/bitstream/handle/123456789/43610/D-106368.pdf?sequence=-1&isAllowed=y

JASO MARQUINA, L. M. & LOZANO MERINO, M. A. 2018. Ventajas e implementación de un sistema SIEM [on-line]. Tesis- Máster en Seguridad de las tecnologías de la información y de las telecomunicaciones. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81267/6/ljasomarTFM0618memoria.pdf

KAVANAGH, K.; BUSSA, T.; SADOWSKI, G. 2020. Magic Quadrant for Security Information and Event Management. Gartner. Disponible en: https://www.gartner.com/en/documents/3981040

LEGUIZAMÓN, D. A.; VENGOECHEA A. A. 2017. Solución instalaciones automatizadas sobre sistemas operativos windows. Universidad Católica de Colombia. Trabajo de Grado para optar al título de Ingeniero de Sistemas. Pag. 93. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/15596/1/Documento%20Final.pdf

MUÑOZ, Victor Manuel. Foro de Ciberseguridad y encuentro de equipos de respuesta a incidentes cibernéticos (CSIRTs). 2018. (Consultado: https://www.dataifx.com/noticias/sector-financiero-y-de-telecomunicaciones-los-que-m%C3%A1s-ataques-cibern%C3%A9ticos-reciben-en)

PEÑA Ninco, J. W. 2015. Instructivo para la implementación efectiva de sistema de información de seguridad y administración de eventos SIEM para la agencia nacional de la superación de la pobreza extrema ANSPE. Universidad Piloto de Colombia. Trabajo de grado para optar al título de Especialista en Seguridad Informática. Pag. 28. Disponible en: http://polux.unipiloto.edu.co:8080/00002356.pdf

RAMÍREZ Luna, H. E.; MEJIA Miranda, J. 2015. Propuesta de infraestructura técnica de seguridad para un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT) [on-line]. ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica. Vol. 4 N°1, Pag. 9. Disponible en: https://www.redalyc.org/busquedaArticuloFiltros.oa?q=Propuesta%20de%20infraestructura%20t%C3%A9cnica%20de%20seguridad%20para%20un%20Equipo%20de%20Respuesta%20ante%20Incidentes%20de%20Seguridad%20(CSIRT)

SÁNCHEZ SOLÁ, A. P. 2013. Diseño de un sistema de gestión de la seguridad de la información para un comercio electrónico basado en la ISO 27001 para pequeñas y medianas empresas en la ciudad de Quito [on-line]. Tesis-Carrera de ingeniería de sistemas y computación, Pag 15. Pontificia Universidad Católica del Ecuador. Facultad de Ingeniería. Disponible en: http://repositorio.puce.edu.ec/handle/22000/6293

SCARFONE, K.; HOFFMAN, P. 2009. Guidelines on Firewalls and Firewall Policy. Pag 2.5-4.4. Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

YAGUAL DEL VALLE, C.; CHILÁN RODRÍGUEZ, L. 2014. Análisis para la integración de un Sistema de Gestión de Seguridad de Información (SGSI) ISO-27001 Utilizando OSSIM para empresa Industrial [on-line]. Tesis- Ingeniería de sistemas con mención de Telemática – Pag. 7. Universidad politécnica salesiana sede Guayaquil. Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/7401/1/UPS-GT000773.pdf

ZHENGBING, H.; ZHITANG, L.; JUNQI, W. 2008. A Novel Network Intrusion Detection System (NIDS) Based on Signatures Search of Data Mining. First International Workshop on Knowledge Discovery and Data Mining (WKDD 2008), Adelaide, SA, pp. 10-16, doi: 10.1109/WKDD.48.