FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE COMPUTACIÓN Y SISTEMAS

IMPLEMENTACIÓN DEL SOFTWARE LOG360 PARA EL CUMPLIMIENTO DEL REQUERIMIENTO 10 DEL ESTÁNDAR DE SEGURIDAD DE DATOS PARA LA INDUSTRIA DE TARJETA DE PAGO

PRESENTADA POR

DAVID ARMANDO LAVADO SARMIENTO

ASESORES

LUZ SUSSY BAYONA ORE

LUIS ESTEBAN PALACIOS QUICHIZ

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE COMPUTACIÓN Y SISTEMAS

LIMA – PERÚ

2019

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

IMPLEMENTACIÓN DEL SOFTWARE LOG360 PARA EL CUMPLIMIENTO DEL REQUERIMIENTO 10 DEL ESTÁNDAR DE SEGURIDAD DE DATOS PARA LA INDUSTRIA DE TARJETA DE PAGO

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE COMPUTACIÓN Y SISTEMAS

PRESENTADO POR

LAVADO SARMIENTO, DAVID ARMANDO

LIMA – PERÚ

2019

DEDICATORIA

A mi familia, de manera especial.

A mis padres Francisco Lavado y Teresa Sarmiento quienes han puesto toda su confianza para lograr un objetivo más en mi vida.

AGRADECIMIENTO

A Dios por sus bendiciones y cuidar de mí y a mi familia.

A la Dra. Sussy Bayona O. y el Mg. Luis Palacios Q. Por sus enseñanzas, y paciencia brindada.

Al Dr. Gimmy Asmad Mena y al Mg. Carlos Valencia Morocho, por su amistad y apoyo incondicional.

A la universidad por la formación profesional para desempeñarme en el mundo laboral.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente estudio tiene como propósito implementar un software SIEM (Gestión de información y eventos de seguridad) para cumplir con el requerimiento 10 de la norma PCI DSS, la cual es un estándar de seguridad de datos para la industria de tarjetas de pago. Para el desarrollo del proyecto se utilizó una variación de la metodología PDCA adaptada a las necesidades de la organización y aprobada por la unidad de cumplimiento normativo del banco. Se utilizó un cuestionario planteado por el concilio que desarrolló la normativa en estudio, a fin de identificar la situación actual de la entidad financiera y, con dicha información, se realizó un análisis de brechas, utilizando la metodología GAP de análisis para determinar los puntos a mejorar. Se usó herramientas de gestión de proyectos para la elaboración del plan de trabajo y para el rastreo de la realización de los procesos durante la implementación del control de seguridad. Por último, debido al proceso de mejora continua, se verificó nuevamente el nivel de cumplimiento del objetivo. Como resultado, la entidad financiera automatizó el proceso de auditoría de registros de eventos de los componentes que transmiten, procesan y almacenan data confidencial durante una transacción de pago; además, tiene visibilidad de lo que sucede en la red, por lo que está en la capacidad de detectar amenazas y anomalías en el comportamiento de usuarios utilizando tecnologías emergentes, como la inteligencia artificial. Por lo tanto, se concluye del proyecto que, la entidad financiera cumple eficientemente con el requerimiento 10 de la norma PCI DSS.

***Palabras clave*:** SIEM, PCI DSS, PDCA, auditoría, registros de eventos, data confidencial, amenazas, anomalías, inteligencia artificial.

ABSTRACT

This thesis was developed with the purpose of implementing a SIEM software (Security information and events management) to comply with the requirement 10 of the PCI DSS standard, which is a data security standard for the payment card industry. For the development of the project, a variation of the PDCA methodology adapted to the needs of the organization and approved by the regulatory compliance unit of the bank was used. A questionnaire was used by the council that developed the regulations under study, in order to identify the current situation of the financial institution and, with this information, a gap analysis was carried out, using the GAP analysis methodology, to determine the points to get better. Project management tools were used to prepare the work plan and to monitor the execution of activities during the implementation of the security control. Finally, due to the process of continuous improvement, the level of compliance with the objective was verified again. As a result, the financial institution automated the process of auditing the event records of the components that transmit, process and store confidential data during a payment transaction; In addition, it has visibility into what happens on the network, so it is able to detect threats and anomalies in user behavior using emerging technologies such as artificial intelligence. Therefore, it is concluded from the project that the financial institution complies efficiently with the requirement 10 of the PCI DSS standard.

Keywords: SIEM, PCI DSS, PDCA, audit, event logs, confidential data, threats, anomalies, artificial intelligence.

INTRODUCCIÓN

El sector financiero es uno de los más regulados, ya que las entidades bancarias deben darle prioridad a la ciberseguridad, para garantizar a sus clientes que su información confidencial y su dinero están protegidos. Es por ello, que este tipo de organizaciones deben cumplir normativas como el PCI DSS estándar de seguridad de datos, para la industria de tarjeta de pago, que de no hacerlo, puede traer consecuencias negativas.

La Organización de Estados Americanos (OEA, 2018), en un estudio realizado respecto al estado de la ciberseguridad en el sector bancario en América Latina y el Caribe, señaló que el 88 %, de una muestra de 722 usuarios, utilizan los canales digitales de pago para operaciones bancarias, mientras el 12 % no lo utiliza; de estos últimos, el 59 % indican que una de las razones es la desconfianza.

El recelo, debido a los riesgos de ciberseguridad afecta la decisión de los usuarios para hacer uso de sistemas de pago digitales, como manifiesta la OEA (2018).

Asimismo, los costos de recuperación ante incidentes relacionados a seguridad digital son muy altos: en el 2017 fue alrededor de USD$ 809 millones en América Latina (OEA, 2018).

El presente estudio tuvo como objetivo, la implementación de un control de seguridad, que permita prevenir riesgos y detectar amenazas de forma proactiva por medio de la gestión de eventos e información de seguridad, el cual proporcionará una visibilidad de lo que sucede en la red de la entidad. Lo mencionado, está relacionado al requerimiento 10 del PCI DSS.

Su estructura está comprendida en el capítulo 1, en el cual se plantea el problema y se describe de forma declarativa su formulación y, en base a ello, definir el objetivo de la tesis, el cual se divide en objetivos específicos, a fin de dar dirección al proyecto; además, se elabora la justificación e importancia del tema de interés y la viabilidad del proyecto. El capítulo 2, describe los antecedentes del trabajo de investigación, en el cual se evalúan artículos, tesis, etc. A nivel mundial, relacionados a la normativa PCI DSS. Asimismo, se sustenta la originalidad del tema elegido, y se detalla las bases teóricas que se utilizan como fundamento para el desarrollo de la tesis. Por último, se definen los términos básicos que se mencionaron en el marco teórico. En el capítulo 3, se definen las herramientas necesarias y la metodología a seguir para desarrollar el proyecto, así como las actividades a realizarse a fin de dar solución al problema planteado. El capítulo 4, muestra el detalle de cómo se han realizado las actividades para el cumplimiento de los objetivos específicos, según las fases de la metodología establecida para el desarrollo del proyecto. El capítulo 5, muestra los resultados, describiendo el antes y después de la implementación realizada por cada objetivo específico para el cumplimiento del objetivo general de la tesis. Finalmente, en el capítulo 7, se analizan e interpretan los resultados por cada objetivo específico descritos en el capítulo anterior para su discusión.

CAPÍTULO I. PLANTEAMIENTO DEL PROBLEMA

En este capítulo se plantea el problema y se describe de forma declarativa, la formulación de este, para definir el objetivo de la tesis, el cual se divide en los objetivos específicos a fin de dar dirección al proyecto. Además, se describe la justificación e importancia del tema de interés y la viabilidad del proyecto.

1.1 Situación problemática

Hoy en día las empresas competitivas cuentan con sistemas, recursos y plataformas TIC, con un alto nivel de disponibilidad, lo que demanda una adecuada administración y un proceso de innovación digital. Para Gener (2019), refiere que este proceso trae como consecuencia la posibilidad que se perpetre ataques contra la seguridad de la data. Es por ello que, las entidades deben de procurar mayor atención a protegerse contra eventuales eventos dañinos.

La seguridad se ha convertido en una dificultad para la mayoría de las empresas, la cual es ineludible por la imposición de cumplir obligaciones legales como la Ley de Protección de Datos (Ley N° 29733) u otras normativas dependiendo del rubro de la empresa, como la Ley Sarbanes-Oxley (SOX, 2002) para las entidades que realizan transacciones en la bolsa; el patrón de seguridad de datos para las empresas que prestan servicio con la utilización de tarjeta de pago (PCI DSS, 2018a).

Según estudios de Crowd Research (2018), el 90 % de las empresas consultadas en el último informe, se consideran, vulnerables, y de estas, el 53% de las compañías aseguran haber sufrido ataques internos en los últimos doce meses. Esto se debe a la falta de visibilidad de lo que sucede dentro de la organización y el exceso de usuarios con privilegios, además, de la falta de control, lo que permite un fácil acceso para los cibercriminales a información confidencial. Como menciona Ramakrishnan (2013), los principales protagonistas son los propios empleados, como también hay que tener en cuenta, el papel de los consultores, proveedores y trabajadores temporales; quienes también pueden suponer una amenaza interna.

Según Smith (2016), "Con un 42 %, Brasil se convierte en el país con más ventas registradas en Latinoamérica, seguido por México con un 12,3 % y Argentina con un 8,9 %". Como menciona Framingham (2018), uno de los factores por el cual esta tendencia sigue creciendo, es el aumento del uso de los dispositivos inteligentes. Por ello, la estrategia de la organización financiera en estudio es impulsar su canal de comercio electrónico, pero garantizando a los usuarios que sus datos sensibles y transacciones están protegidos.

1.2 Definición del problema

Con el avance de la tecnología, las organizaciones financieras deben implementar servicios que den facilidades a sus clientes; servicios como el comercio electrónico que permite comprar desde cualquier lugar y a cualquier hora, con el uso de las tarjetas bancarias.

En el 2018, se mejoró el marco metodológico de seguridad de la información, con la finalidad de incorporar los requerimientos técnicos y operativos, según la normativa PCI DSS para el procesado y acopio de datos de tarjetas. Como resultado de la revisión periódica del cumplimiento y evaluación de la efectivad de los controles de seguridad ya en funcionamiento, se observó el problema de la falta de transparencia de lo que está sucediendo en la red y de la ineficiencia para detectar y obtener información sobre las amenazas potenciales, a fin de realizar las correcciones necesarias antes de que se conviertan en un ataque. Esta brecha de seguridad está relacionada

al requerimiento 10 del estándar de seguridad mencionado, en el cual nos enfocaremos en este trabajo de tesis.

1.3 Formulación del problema

En razón a lo expuesto, el estudio tiene como propósito dar una alternativa de solución al siguiente problema de investigación:

1.3.1 Problema general.

Obsoleto control de seguridad de información para cumplir con el requerimiento 10 de la normativa PCI DSS en una entidad bancaria.

1.3.2 Problemas específicos.

1. Alto porcentaje de brechas por la limitada gestión de eventos e información de seguridad debido al control compensatorio en uso.
2. Ineficiente proceso para cumplir con los requerimientos de auditoría del Área de Seguridad de Información del Banco.
3. Complejo proceso para detectar amenazas internas y comportamientos inusuales de los usuarios internos del banco.

1.4 Objetivos

1.4.1 Objetivo general.

Cumplir con el requerimiento 10 del estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS) en la entidad bancaria.

1.4.2 Objetivos específicos.

1. Disminuir las brechas identificadas por medio de la implementación de un software SIEM, como control de seguridad seleccionado, para el cumplimiento del requerimiento 10 de la norma PCI DSS.
2. Reducir el tiempo de atención de los requerimientos de auditoría a través de la recolección y procesamiento automático de eventos de los servidores auditados.

3. Aumentar la eficiencia del proceso de detección de amenazas internas y comportamientos inusuales de los usuarios internos en la organización.

1.5 Importancia de la investigación

La banca es uno de los sectores financieros con mayor índice de ciberataques, debido a la cantidad de dinero que manejan y el aumento en la tendencia del uso de sistemas de pago digitales. Como consecuencia de la utilización de esta ventaja tecnológica aparecen nuevas vulnerabilidades, las cuales son aprovechadas por los cibercriminales para obtener información confidencial. Por ello, es importante aplicar la normativa que se estudia en este trabajo de tesis, para garantizar la seguridad de las acciones de pago, beneficiando de esta manera, tanto al banco, como a sus clientes.

El cumplimiento del PCI DSS necesita de una inversión en ciberseguridad, la cual es necesaria para proteger los datos privados de autenticación y del titular de la tarjeta. Pues, las consecuencias de no implementar esta normativa, como interrupciones operativas, pérdidas financieras, daño en su reputación y posición competitiva, excede en muchos casos a varios de miles de dólares.

Muchos de los ataques cibernéticos a este tipo de entidades son desde el interior de la organización, por lo tanto, es crucial monitorear las acciones de los trabajadores y de todo aquel que tenga acceso dentro de la red, y no solo dar importancia a la seguridad perimetral. Según estudios de la Ponemon Institute (2018), refiere que los estudios sobre defensa de datos y tecnologías de información emergentes, el 85 % de las organizaciones han sufrido fugas de información por parte de sus empleados, clientes o proveedores en los últimos dos años. Sin embargo, se puede decir que el 100 % de organizaciones han perdido información, pero aún no lo saben.

Para obtener la visibilidad global de lo que sucede dentro de la organización, tal como lo estípula el requerimiento 10 de la norma PCI DSS, la cual nos enfocaremos en este trabajo de tesis, es necesario recolectar de forma centralizada y segura, los registros de actividades para analizarlas. Pero, debido a la diversidad, cantidad de componentes y volumen de data, es un proceso muy difícil de realizar de forma efectiva, si se hace manualmente,

por lo que es importante contar con las herramientas para la automatización de los procesos de auditoría y utilizar tecnologías emergentes, como Inteligencia Artificial o *Machine Learning*, las cuales resultan muy útiles para identificar patrones sospechosos relacionados a fraude y la prevención de ciberataques, entre otros beneficios.

1.6 Viabilidad de la investigación o presupuesto

A continuación, se describen los materiales y los costos para determinar el presupuesto necesario para la ejecución del proyecto.

Requerimientos de Hardware

Servidor de aplicación

Hardware	Costo ($)
x3250 M6, Xeon 4C E3-1240v5 80W 3.5GHz/2133MHz	951.575
900GB 10K 12Gbps SAS 2.5in G3HS HDD	315.64
9.5mm Ultra-Slim SATA Multi-Burner	44.33
x3250 Optical Disc Drive Cable Kit	8.45
460W Redundant Power Supply	137.91
Total	1 457.90

Requerimientos de Software

Software	Costo ($)
MicroSoft Server 2012 R2	65.00
MicroSoft SQL Standard 2012	- - - -
Software de auditoría	7 455.00
Total	7 520.00

Personal

Rol	Costo ($)
Jefe de proyecto	2 200.00
Implementador	1 500.00
Auditor	- - - -
Jefe de TI	- - - -
Administrador de servidores	- - - -
Jefe de seguridad de información	- - - -
Total	3 700.00

TOTAL GENERAL	**12 677.9**

CAPÍTULO II. MARCO TEÓRICO

El capítulo dos, describe los antecedentes del trabajo de investigación, en el cual se evalúan artículos, tesis, etc. A nivel mundial, relacionadas a la normativa PCI DSS, como también, se sustenta la originalidad del tema elegido. Asimismo, se detalla las bases teóricas que se utilizan como fundamento para el desarrollo de la tesis y, por último, se definen los términos básicos que se mencionaron en este capítulo.

2.1 Antecedentes

En esta sección se evalúa trabajos de investigación de universidades locales o internacionales, relacionados al tema de interés elegido. Por lo que se utilizaron artículos y tesis respecto a la norma PCI DSS y al requerimiento 10 de este estándar de seguridad.

Bernabé (2014) propone una guía para la implementación del estándar de seguridad PCI DSS, para mejorar o garantizar la seguridad en los canales de pago. En este trabajo se realizó encuestas relacionadas a la importancia de los 12 requerimientos de la norma y así medir el conocimiento que tienen las empresas que participaron. Sin embargo, no hay aplicación práctica, en ninguno de los requerimientos, de la metodología que propone, por lo que los resultados son un conjunto de recomendaciones.

Calle y Mejía (2015) realizó un análisis de la implementación del estándar PCI DSS en la seguridad de la información dentro de una institución financiera, con la finalidad de concientizar la importancia del cumplimiento de

la normativa y los beneficios de su implementación. De igual manera que el trabajo anterior, por medio de encuestas, se evalúa el grado de conocimiento y porcentaje de aceptación de las instituciones consultadas.

Benenaula y Ortega (2016) investigaron en relación a la auditoría de sistemas al cumplimiento de los requerimientos 7, 8, 9 de la norma PCI DSS, evaluando el nivel de cumplimiento de los requisitos específicos por medio del cuestionario de autoevaluación que propone el concilio, y realizaron una auditoría de la situación actual, en la cual se identificaron diferentes brechas, por lo que el informe final, describe una serie de recomendaciones para que de esta manera se cumplan los objetivos.

En conclusión, los trabajos de investigación consultados proponen metodologías o planes de implementación, como también, análisis del cumplimiento del estándar de seguridad PCI DSS, pero de manera general, a excepción del trabajo de Benenaula y Ortega, que se enfoca en requerimientos específicos de la norma. La principal diferencia entre estos trabajos y el desarrollado en esta investigación, es que no hay una implementación o caso práctico de los controles de seguridad o medidas necesarias para cumplir con los requerimientos de la norma. Por último, este trabajo hace uso de tecnologías emergentes como la inteligencia artificial, la cual está siendo cada vez más adoptada por los diferentes tipos de entidades, incluyendo la banca.

2.2 Bases teóricas

2.2.1 Estándar de seguridad de datos para la industria de tarjeta de pago (PCI DSS)

Es desarrollado por un concilio formado por las principales compañías de tarjetas de pago, que consiste en un conjunto de requisitos técnicos y operativos que debe seguir toda empresa que transmita, almacene o procese información confidencial del titular de la tarjeta y de autenticación, con el objetivo de aumentar la seguridad de dichos datos (PCI Security Standards Council [PCI SSC], 2018c).

A continuación, en la Tabla 1, se muestra una descripción general de los requisitos mencionados.

Tabla 1

Los 12 requisitos de la norma PCI DSS versión 3.2.1

Desarrolle y mantenga redes y sistemas seguros.	1.	Instale y mantenga una configuración de *firewall* para proteger los datos del titular de la tarjeta.
	2.	No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
Proteger los datos del titular de la tarjeta	3.	Proteja los datos del titular de la tarjeta que fueron almacenados
	4.	Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
Mantener un programa de administración de vulnerabilidad	5.	Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente.
	6.	Desarrollar y mantener sistemas y aplicaciones seguros
Implementar medidas sólidas de control de acceso	7.	Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.
	8.	Identificar y autenticar el acceso a los componentes del sistema.
	9.	Restringir el acceso físico a los datos del titular de la tarjeta.
Supervisar y evaluar las redes con regularidad	10.	Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta
	11.	Probar periódicamente los sistemas y procesos de seguridad.
Mantener una política de seguridad de información	12.	Mantener una política que aborde la seguridad de la información para todo el personal

Nota: Tomado de PCI Security Standards Council (2018b)

El cumplimiento de esta normativa ofrece los siguientes beneficios:

1. Aumenta la confianza de los clientes, mejorando la reputación e imagen de la empresa.
2. Ayuda a prevenir fraudes, riesgos y detectar violaciones en la seguridad, los cuales pueden traer como consecuencia pérdidas económicas, multas por incumplimientos, demandas legales y el impacto negativo de la imagen de la entidad.
3. Facilita el cumplimiento de otros estándares de seguridad, ya que muchos requisitos coinciden con otras normativas, por lo que contribuye en el cumplimiento de estos, para complementar la seguridad en la entidad.

2.2.2 Alcance de PCI DSS.

El primer paso para la evaluación e implementación del PCI DSS, es determinar cuál es el alcance; para lo cual se debe identificar los componentes en los cuales se tiene que aplicar esta normativa. Los componentes de una entidad se pueden clasificar en tres tipos:

Componentes del CDE.

Componentes conectados o que impactan en el CDE.

Componentes fuera del CDE.

Para identificar el tipo de componente, como primera actividad, se debe identificar cómo y dónde la organización recibe el CHD, desde el punto en que se recibe, hasta el punto de destrucción, disposición o traslado. Una vez identificado todos los canales de pago y métodos para aceptar CHD, es necesario documentar y determinar los componentes que son parte del flujo de ese tipo de datos, es decir, cualquier persona, procesos, tecnologías, etc. que transmite, almacena y procesa información confidencial de las tarjetas de pago. El conjunto de todos los componentes de este tipo se le conoce como CDE y se les debe aplicar todos los requerimientos que estipula el estándar PCI DSS (PCI Security Standards Council [PCI SSC], 2018a).

La siguiente actividad consiste en identificar los otros componentes que deben validarse con cada requerimiento del PCI DSS, los cuales son los conectados o que dan acceso al CDE y que impactan en su configuración o seguridad (PCI SSC, 2018a).

Con respecto a los componentes fuera del CDE, son aquellos que no cumplen con lo mencionado anteriormente, por lo que en ellos, no aplica la normativa PCI DSS, pero es importante que se implemente controles de seguridad en base a buenas prácticas para que este grupo de componentes no sea un riesgo para el CDE (PCI SSC, 2018b).

Una vez identificado los componentes de cada tipo se deben separar entre ellos, por medio de la segmentación lógica o física de la red, lo que permite limitar el alcance donde se debe aplicar el PCI DSS, como también, reducir costos, riesgos y complejidad en la implementación y monitoreo de los diferentes controles de seguridad para cumplir con la normativa PCI DSS. En la Figura 1 se muestra un ejemplo para determinar si un componente debe incluirse en el alcance del estándar de seguridad en estudio (PCI SSC, 2018b).

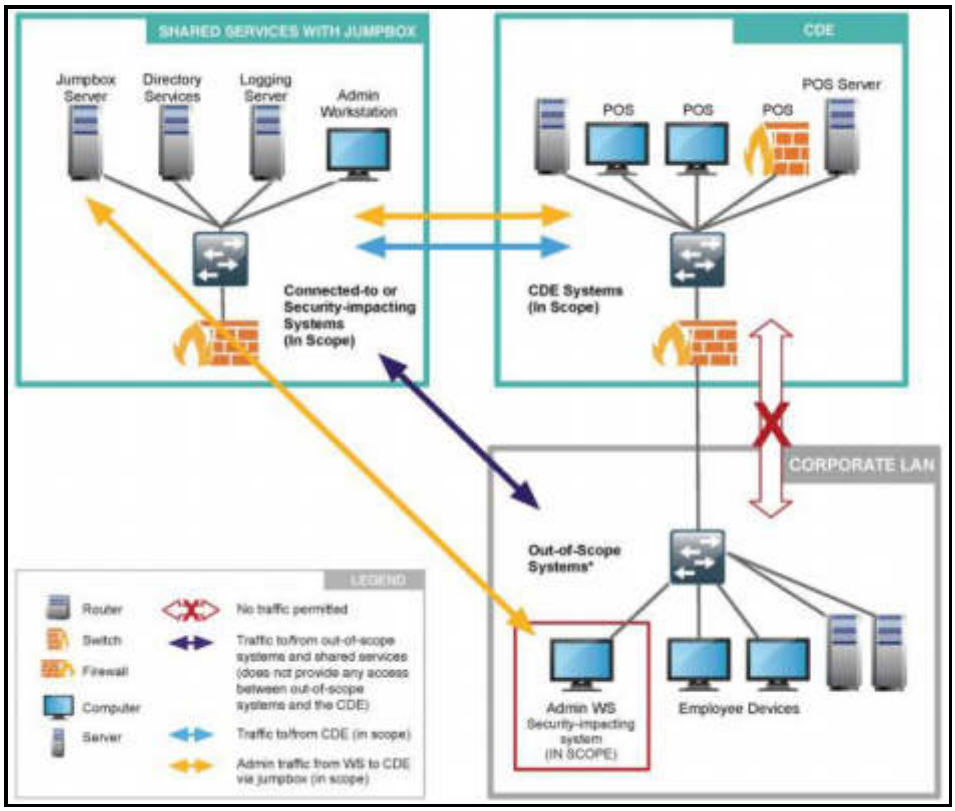


Figura 1. Segmentación de redes

Nota: Tomado de PCI Security Standards Councilt (2018b)

En este escenario, un administrador debe tener acceso a ciertos componentes del CDE, desde su estación de trabajo en la red corporativa, como se puede ver en la Figura 1, no hay una conexión directa entre el CDE y la red corporativa; para ello, se debe usar como intermediario un componente en el segmento de red de servicios compartidos llamado JUMP Server, el cual es un control que nos va a permitir acceso al CDE. En este caso, la estación de trabajo se debe considerar en el alcance del PCI DSS, ya que es un componente que puede impactar en la CHD.

2.2.3 Proceso de sistema de pago.

A fin de proteger la información confidencial del titular de la tarjeta, se debe comprender el proceso de cómo se registra un pago y tomar en cuenta que mientras más complejo sea el sistema de pago, más difícil será protegerlo, ya que estas funcionalidades adicionales pueden tener vulnerabilidades que sean aprovechadas por los ciberdelincuentes (PCI SSC, 2016).

A continuación, la figura 2 muestra un ejemplo del sistema de pago:

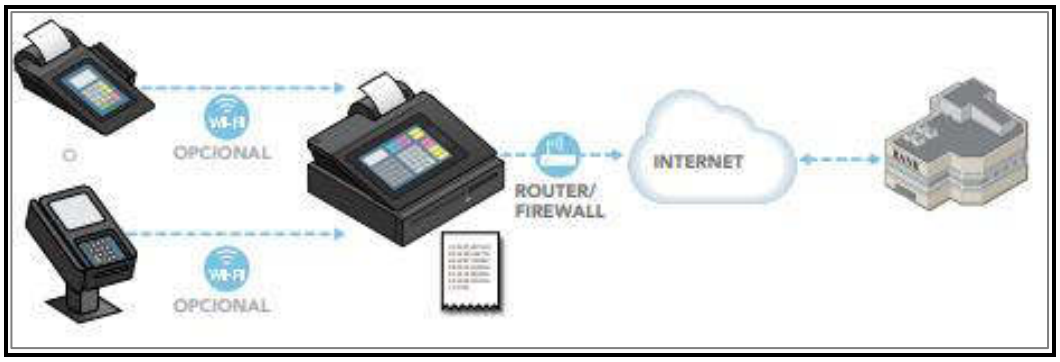


Figura 2. Sistema de pago digital

Nota: Tomado de PCI Security Standards Councilt (2018b)

Un sistema de pago está conformado por diferentes dispositivos que reciben información confidencial de la tarjeta del titular. A continuación, se describen los más comunes:

Terminal de pago: También conocido como POS. Existen los que escanean la banda magnética, o leen el chip de la tarjeta. Estos dispostivos almacenan temporalmente en su memoria, información de la tarjeta.

Terminal de pago integrado: Tiene la función de registradora, la cual calcula la transacción y la de terminal de pago.

Banco comercial. Es la institución financiera, el cual recibe la información para procesar el pago.

2.2.4 Información confidencial en transacciones bancarias.

El propósito de la norma PCI DSS es proteger los datos de los titulares de las tarjetas, a fin de evitar fraudes. La Tabla 2 muestra la data sensible que se debe resguardar.

Tabla 2

Información confidencial que se necesita proteger

Datos de cuentas	
Los datos de titulares de tarjetas incluyen	Los datos confidenciales de autenticación incluyen
Número de cuenta principal	Contenido completo de la pista (datos de la banda magnética)
Nombre del titular de la tarjeta	
Fecha de vencimiento	CAV2/CVC2/CVV2/CID
Código de servicio	PIN/Bloqueos de PIN

Nota: Tomado de PCI Security Standards Council (2018b)

En la figura 3 se muestra la ubicación de estos datos en la tarjeta:

Figura 3. Tipos de datos en una tarjeta de pago

Nota: Tomado de PCI Security Standards Council (2018b)

Número de cuenta principal (PAN). Es el número de tarjeta. La longitud de los números depende de la marca, pero generalmente son 16 dígitos, los cuales tienen un significado (Acosta, 2018a). En la Figura 4 se muestra como está distribuido los dígitos y lo que representan.

Figura 4. Distribución de dígitos PAN

Nota: Tomado de Acosta (2018a)

MII: El primer dígito representa el tipo de sistema. Estos pueden ser banca y finanzas (VISA, Mastercard), viajes (American Express, Diners Club, etc.).

IIN/BN: Está conformado por los seis primeros dígitos que permiten identificar el banco emisor de la tarjeta.

IAI: Está conformado desde el séptimo, hasta el penúltimo dígito, y representa el número de cuenta.

Check Digit: Es el dígito final el cual es calculado utilizando el algoritmo de Luhn (Acosta, 2018a).

Nombre del titular de la tarjeta. Es el nombre de la persona, dueño de la cuenta o tarjeta.

Fecha de vencimiento. Es la fecha en la cual caduca la tarjeta, después de la fecha, está inoperativa y no puede extenderse la fecha de vencimiento.

Con respecto a los datos de autenticación, estos incluyen:

Contenido completo de la pista: La información se almacena en bandas magnéticas o chips, la cual contiene datos de la tarjeta y el propietario (Acosta, 2018d).

CAV2/CVC2/CVV2/CID: Es un código de verificación generado junto con el PAN que permite validar la integridad de la tarjeta. Las iniciales varían según la marca que emite la tarjeta (Acosta, 2018b).

PIN/Bloqueos de PIN: Es el código personal del titular para comprobar su identidad. Está relacionado con el contenido completo de la pista como control de seguridad, pues al validar el PIN se tiene acceso a la información almacenada en la banda magnética o chip (Acosta, 2018c).

Durante el proceso de pago, una vez autorizado, determinados datos de la tarjeta no deben almacenarse. A continuación, la Tabla 3 muestra por tipo de información confidencial, cuáles pueden almacenarse y cuáles deben transmitirse de forma encriptada.

Tabla 3

Datos confidenciales de cuentas

		Elemento de datos	Almacenamiento permitido	Datos almacenados ilegibles según el Requisito 3.4
Datos de cuentas	Datos del titular de la tarjeta	Número de cuenta principal (PAN)	Sí	Sí
		Nombre del titular de la tarjeta	Sí	No
		Código de servicio	Sí	No
		Fecha de vencimiento	Sí	No
	Datos confidenciales de autenticación[2]	Contenido completo de la pista[3]	No	No se pueden almacenar según el Requisito 3.2
		CAV2/CVC2/CVV2/CID[4]	No	No se pueden almacenar según el Requisito 3.2
		PIN/Bloqueo de PIN[5]	No	No se pueden almacenar según el Requisito 3.2

Nota: Tomado de PCI Security Standards Council (2018a)

2.2.5 Requerimiento 10 de PCI Security Standards Council.

Este requerimiento establece que se “rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta” (PCI SSC, 2018b). Todo sistema, aplicación, servicio, etc. genera los registros de los accesos y actividades que suceden en estos, por lo que es responsabilidad hacer un seguimiento de esos eventos, para saber qué está sucediendo y cómo se están usando. El requerimiento 10 de la norma PCI DSS tiene como objetivo monitorear y hacer seguimiento de los registros a fin de tener una visibilidad de lo que sucede dentro del CDE, para la detección y prevención de una amenaza y así minimizar el impacto en los datos confidenciales (Manage Engine, 2018a).

Este requerimiento se divide en 9 puntos que se describen a continuación:
1. Aumentar las pistas de auditoría con el fin de enlazar el acceso a los elementos del sistema con clientes particulares.

Se debe asegurar que todo componente que conforme el CDE debe generar eventos de sus accesos y estos registros deben estar asociados a usuarios específicos, esto último para identificar responsables.

2. Accionar las pistas de auditoría en todos los elementos del sistema.

Validar que se están registrando los accesos y acciones de los usuarios de todos los componentes que conforma el CDE, a fin de identificar y rastrear, por medio de un historial, actividades malintencionadas.

3. Anote los ingresos a las pistas de los elementos.

A lo menos, se deben tener registrados los datos importantes de la operación y que responde a cinco preguntas básicas de control:

Identificación de clientes. Es quien realizó la operación: ¿Quién lo hizo?

Evento. Es el proceso que se realiza de parte del cliente que accedió, puede hacer cambios, eliminar, crear objetos: ¿Qué hizo?

Fecha y hora. Nos indica cuándo se realizó el evento: ¿Cuándo lo hizo?

Indicación de éxito o error. Indica el proceso correcto o errado, ejecutado por el cliente; además, las veces fallidas permite conocer las intenciones del cliente.

Origen del evento.

Identidad de los datos, elementos del sistema: Indica el dispositivo en dónde se realizó la operación (CDE): ¿Dónde lo hizo?

4. Asegúrese que los tempos y relojes estén sincronizados para adquirir, distribuir y almacenar tiempos**.**

El propósito es uniformar todos los tiempos exactos, lo cual indica cuándo se realizó un evento, y la correlación de eventos entre los componentes.

5. Resguarde las pistas de control para que no se puedan alterar.

Ya que, las pistas de auditoría son la fuente de los registros de las acciones que se realizaron en los componentes del sistema, es importante proteger su integridad para que no sean eliminadas o alteradas. Este requerimiento da recomendaciones de cómo proteger las pistas de auditoría por medio de copias de seguridad, control de accesos, segregación de redes, monitoreo de integridad de archivos y carpetas, entre otros.

6. Inspeccione los datos y eventos de seguridad en todos los componentes para observar las singularidades o acciones dudosas.

Este requisito consiste en la revisión diaria de las pistas de seguridad de los componentes críticos del sistema, para detectar proactivamente amenazas, actividades no autorizadas o mal intencionadas. El intervalo de las revisiones periódicas de los otros componentes se realiza según la evaluación anual de riesgos definida por la organización.

7. Almacene todos los registros de los eventos y controles al menos, un año, con un mínimo de vigencia para observación tres meses.

Se deben almacenar las pistas de auditoría en un repositorio seguro y centralizado, para tener un historial de mínimo un año, lo cual permite realizar un análisis forense. También, se debe tener a disposición inmediata al menos tres meses de los registros para detectar y minimizar rápidamente el impacto de violaciones de seguridad.

8. Exigencias para algunos proveedores de servicios: Agenciar un protocolo de localización e informe de fallas del sistema de seguridad crítica.
9. Cerciórese que las políticas de seguridad y protocolos para supervisar los accesos a los recursos de la red y datos del titular de la tarjeta, se encuentren registrados físicamente, efectuados y que ambas partes tengan conocimiento.

Por medio de entrevistas se verifica que el personal conoce y respeta las normas de seguridad de la organización.

2.2.6 Metodología PDCA.

También conocido como Ciclo de Deming, es una metodología de mejora continua para mantener y mejorar el desempeño de un proceso. Puede ser utilizado en diferentes entornos como la seguridad de la información (ESAN, 2016). Se divide en las siguientes etapas:

Planificación (plan): Durante esta fase se elabora una estrategia de acuerdo con los objetivos y el alcance del proyecto.

Hacer (do): Consiste en implementar el plan elaborado.

Verificar (check): En esta fase se evalúa los resultados para comprobar el cumplimiento de los objetivos.

Actuar (act): Consiste en corregir las brechas o puntos a mejorar.

2.2.7 Metodología GAP análisis.

Es una metodología que se utiliza para determinar el nivel de cumplimiento de una norma o estándar. Consiste en la comparación de la situación actual con la expectativa, o situación deseada, para identificar las brechas o puntos a mejorar y, en base a ellas, desarrollar un plan de acción para cubrir las deficiencias encontradas. En la Figura 5 se muestra las fases del GAP Análisis (Addagada, 2012).

Figura 5. GAP análisis

Identificar el estado actual: ¿Dónde estamos? Reconocer la situación actual de lo que deseamos mejorar. En base a los resultados del cuestionario.

Definir Expectativa: ¿A dónde deberíamos llegar? En base al estándar en estudio.

Identificar brecha: ¿Qué hace falta? Determinar las medidas necesarias para cumplir las expectativas.

El GAP análisis se utiliza en mejora continua para analizar los resultados, una vez ejecutado o implementado el plan de acción, asegurando que se haya cumplido los objetivos y mantener la eficiencia.

2.2.8 Gestión de eventos e información de seguridad (SIEM).

Es una tecnología que nace de la combinación de un SEM (Gestión de eventos de seguridad), que consiste en la recopilación y análisis en tiempo real de lo que ocurre en la red, y SIM (Gestión de información de seguridad), que permite guardar a largo plazo datos para analizarlos posteriormente. (Manage Engine, 2018b).

A continuación, en la figura 6 se muestra los componentes del software.

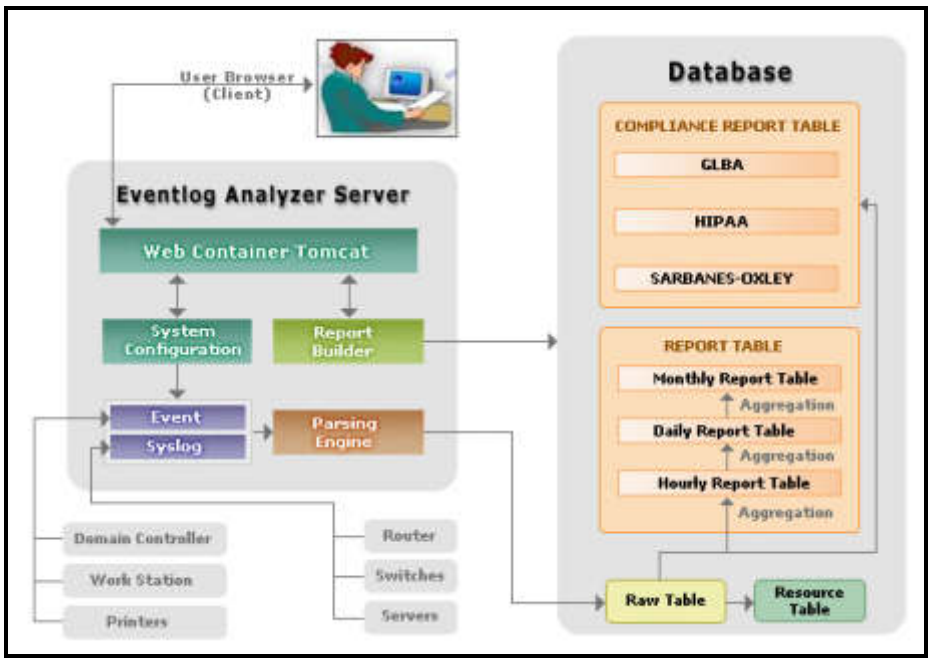


Figura 6. Componentes de Log360

Nota: Tomado de Manage Engine (2018b)

Un SIEM recopila en tiempo real los registros de eventos de diferentes recursos como aplicaciones, servicios, dispositivos de red, servidores, etc. por medio de protocolos como WMI, en el caso de Windows, o Syslog, para almacenarlos de forma centralizada a fin de procesar esa información y generar reportes que nos proporciona visibilidad global de lo que sucede en la red de la organización con la finalidad de prevenir amenazas (Manage Engine, 2018b).

El componente *Parsing Engine* automatiza el proceso de *Log Parser*, consiste en capturar información importante de la data en bruto, que proporciona los registros de eventos, por medio de consultas, *querys* o comandos, para mostrarlos de forma ordenada a fin de facilitar su análisis (Microsoft, 2005).

La figura 7, muestra un ejemplo del formato de un registro de evento de un controlador de Dominio, respecto a la autenticación de un usuario a una estación de trabajo.

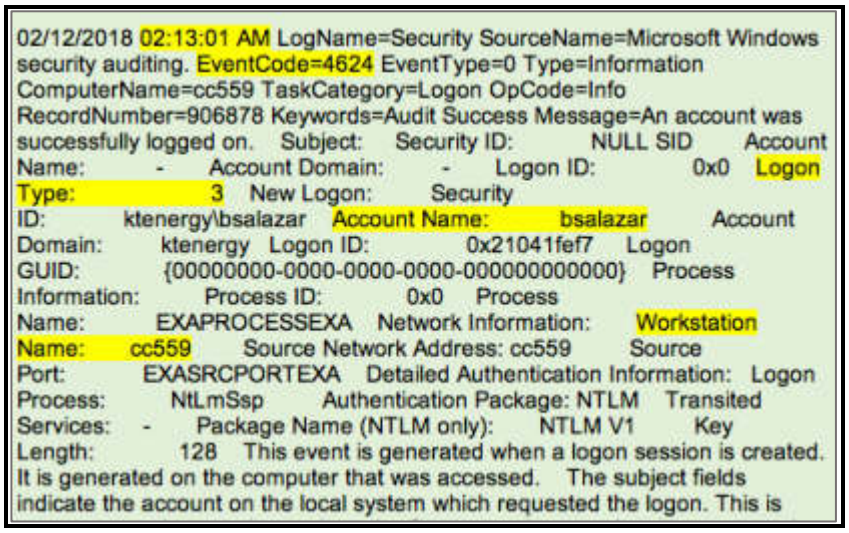

02/12/2018 02:13:01 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4624 EventType=0 Type=Information ComputerName=cc559 TaskCategory=Logon OpCode=Info RecordNumber=906878 Keywords=Audit Success Message=An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 New Logon: Security ID: ktenergy\bsalazar Account Name: bsalazar Account Domain: ktenergy Logon ID: 0x21041fef7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: EXAPROCESSEXA Network Information: Workstation Name: cc559 Source Network Address: cc559 Source Port: EXASRCPORTEXA Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 128 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is

Figura 7. Detalles de un registro de evento

Nota: Tomado de Microsoft (2005)

Debido a que los identificadores de los eventos y el formato varían según la versión o tipo de recurso, el componente “Parsing Engine” debe interpretar la información que proporciona diferentes modelos de registros (Manage Engine, 2018b).

La tabla 4, se muestra la variación en los identificadores de los registros de eventos de un mismo sistema operativo, pero de diferente versión.

Tabla 4

ID de eventos por versión de OS

Event Description	Win XP Event ID	Win 7/8 Event ID	Log type
Special Privileges assigned to new logon	576	4672	Security log
User Right was assigned	608	4704	Security log
User Right was removed	609	4705	Security log
System Security Access was granted to an account	621	4717	Security log
System Security Access was removed from an account	622	4718	Security log
User Account was created	624	4720	Security log
User Account was enabled	626	4722	Security log
User Account was disabled	629	4725	Security log
User Account was deleted	630	4726	Security log
User Account was changed	642	4738	Security log
User Account was locked out	644	4740	Security log
Computer Account was created	645	4741	Security log
Computer Account was changed	646	4742	Security log
Computer Account was deleted	647	4743	Security log
User Account was unlocked	671	4767	Security log
Domain Controller attempted to validate the credentials for an account		4776	Security log
Domain Controller failed to validate the credentials for an account	675	4777	Security log
Name of an Account was changed	685	4781	Security log

Nota: Tomado de Microsoft, 2010

Las principales funcionalidades de un SIEM son las siguientes:

Recopilar registros de eventos: Compendiar de forma segura los eventos de diferentes recursos antes que se pierdan o se sobrescriban (Manage Engine, 2018b).

Almacenar registros de eventos como data histórica: Debe almacenar de forma centralizada y segura los registros de eventos para mantenerlos como históricos y poder consultarlos cuando sea necesario. Algunos estándares de seguridad requieren, para su cumplimiento, mantener los registros de eventos de varios años (Manage Engine, 2018b).

Generar reportes: Debe procesar rápidamente grandes volúmenes de registros de diferentes recursos para generar reportes intuitivos (Manage Engine, 2018b).

Generar ROC (Report Of Compliance) de normativas: Los últimos softwares de este tipo están alineados a diferentes estándares de seguridad como ISO 27001, GDPR, SOX, PCI DSS, etc., para generar reportes automáticos de cumplimiento de estas normativas (Manage Engine, 2017).

Detectar amenazas externas e internas: En base a criterios, se pueden crear reglas que permitan detectar amenazas, tanto externas como internas, y reducir falsos positivos. Al detectar una amenaza debe generar una alerta y notificar al responsable del recurso que lo originó (Manage Engine, 2019).

Ejecutar acciones: Debe permitir utilizar las alertas como disparador para ejecutar determinadas acciones a fin de corregir, bloquear o mitigar el impacto de la amenaza (Manage Engine, 2018b).

Correlación de eventos: Son reglas que permiten relacionar eventos de diferentes recursos para determinar la causa raíz de un problema (Manage Engine, 2018b).

2.2.9 User Behavior Analytics (UBA).

Es una tecnología reciente, que utiliza Machine Learning, un área de la inteligencia artificial, que por medio de algoritmos y análisis avanzado de estadísticas, identifica patrones del comportamiento de los usuarios en base a un gran volumen de data de los registros de sus actividades (Manage Engine, 2018b).

El UBA establece una línea base dinámica, ya que aprende constantemente de las acciones del usuario, y lo usa de referencia para identificar anomalías en su comportamiento, por lo que a más data, más confiable serán sus tendencias o predicciones, lo cual se traduce en mayor precisión en la detección de anomalías (Manage Engine, 2018b).

En la figura 8, se muestra cómo se detecta una anomalía cuando se compara con una línea base establecida.

Figura 8. Detección de una anomalía

Nota: Tomado de Varonis (2018)

Esta tecnología se está incluyendo en software de seguridad tipo SIEM, lo cual permite lo siguiente:

Detectar fraudes

Prevenir amenazas

Reducir falsos positivos

2.3 Definición de términos básicos

Seguidamente, se anotan términos o acrónimos que se mencionaron en las bases teóricas (PCI SSC, 2016; (Manage Engine, 2017ª; (Manage Engine, 2018b).

PCI: *Payment Card Industry* (en español es Industria de Tarjeta de Pago)

PCI SSC: *PCI Security Standard Council*. Es el cónclave de las principales industrias de pago, que desarrolla y actualiza la normativa PCI DSS.

PCI DSS: *PCI Data Security Standard*. Es el estándar de seguridad para el resguardo de data confidencial del titular.

PA DSS: *Payment Application Data*. Es un estándar de seguridad para las aplicaciones que procesan pagos.

CDE: *Cardholder Data Enviroment*, es un conjunto de componentes en una red segmentada que transmiten, procesan y almacenan data durante una transacción de pago.

CHD: *Card Holder Data*. Son los datos confidenciales del titular de la tarjeta.

SAD: *Sensitive Authentication Data*, es la data confidencial de autenticación que se utiliza en una transacción de pago.

QSA: *Qualified Security Assessor*, auditor certificado por el PCI SSC, para la validación del cumplimiento de las exigencias de la norma PCI DSS.

SAQ: *Self-Assessment Questionnaire*. Es un cuestionario propuesto por PCI SSC para la autoevaluación del cumplimiento de la norma PCI DSS.

Fraude Financiero: acción ilegal de una persona que daña la economía de otra por beneficio propio.

POS: *Point Of Sale*, es una terminal utilizada en el sistema de pago para la recepción de tarjetas.

DMZ: *Demilitarized Zone*, tecnología que permite ensanchar la red privada y su acceso por medio de la Internet.

VPN: *Virtual Private Network*, tecnología que permite ampliar la red privada a través de una red de internet.

JumpBox Server: servidor intermediario para gestionar el acceso a redes privadas.

SIEM: *Security Information and Event Management*. Tipo de software para la administración centralizada de registros de eventos.

Logs: registros de las actividades en un sistema operativo, aplicación, servicio o dispositivos que deben generarse automáticamente.

Pista de auditoría: Bitácora de las actividades de un componente o sistema, el cual nos da el detalle de lo que sucede desde el comienzo hasta el final de un procesamiento o transacción.

Log Parser: Proceso que consiste en obtener datos a partir de un formato o patrón de información.

Syslog: Protocolo para el envío de registros o información de un evento determinado, los cuales se almacenan en un SIEM.

ROC: *Report Of Compliance*, es un informe, respecto al cumplimiento de standard o buenas prácticas.

UBA: *User Behavior Analytics*, es una tecnología de inteligencia artificial para la identificación de patrones de comportamiento de usuarios (Manage Engine, 2018b).

UEBA: *User and Entity Behavior Analytics*, tecnología de inteligencia artificial para la identificación de patrones de comportamiento de usuarios y dispositivos.

Machine Learning: rama de la inteligencia artificial que por medio de algoritmos y análisis estadísticos puede detectar, prevenir y predecir algún evento.

CAPÍTULO III. METODOLOGÍA

En este acápite se mencionan los procedimientos necesarios a seguir para desarrollar el estudio. También, las actividades a realizarse a fin de dar solución al problema planteado.

3.1 Método

La metodología utilizada para alcanzar el objetivo de cumplir con el requerimiento 10 de la norma PCI DSS, es la propuesta por el auditor externo y aprobado por la unidad de cumplimiento normativo del banco, la cual es una variación de la metodología PDCA, adaptada a las necesidades particulares de la organización. Consiste en las siguientes fases:

1. Acopio de la información
2. Diagnóstico
3. Planeamiento
4. Implementación
5. Verificación

Fase 1: Levantamiento de Información.

El propósito de esta fase en recolectar información de la situación actual, respecto al cumplimiento del requerimiento 10 de la norma PCI DSS en el banco. Para ello, se está utilizando la herramienta de cuestionario. En el desarrollo de esta etapa se realizaron las siguientes actividades:

Definir objetivo.

En este primer paso se define el objetivo de la encuesta para darle una orientación a las preguntas que se van a formular, a fin de obtener la información que necesitamos.

Identificar a quien va dirigido: En esta actividad se determina la persona que cuenta con la información que necesitamos.

Diseño del cuestionario: En base al objetivo del cuestionario, se enuncia las preguntas adecuadas para obtener la información que necesitamos.

Ejecución del cuestionario: En este paso, la persona a quien va dirigido el cuestionario, desarrolla cada pregunta formulada.

Analizar los resultados: La información obtenida del cuestionario es procesada para analizar los resultados.

Fase 2: Diagnóstico.

El objetivo de esta fase es identificar las brechas para cumplir con el requerimiento 10 de la norma PCI DSS. Para ello, se realizó una comparativa de la información recopilada en la fase 1, la situación actual, con lo estipulado en la norma en estudio: la situación deseada. Para el desarrollo de esta fase se utilizó la metodología de diagnóstico y análisis de brechas: el GAP análisis.

Fase 3: Planeamiento.

El propósito de esta fase es establecer un plan de trabajo que sirva como guía durante la implementación y para su correcto control y seguimiento. En base a los resultados obtenidos en la fase 2, se va a determinar el plan de acción o las actividades necesarias para cubrir las brechas encontradas. A continuación, se indican las actividades realizadas:

Kick Off. Es la reunión inicial del proyecto en la cual se trata principalmente los siguientes puntos:

Definir objetivos.

Establecer los objetivos de la implementación.

Definir alcance**:** Delimitar el alcance de la implementación asegurando que se cumplan los objetivos definidos.

*Identificar Stakeholders***:** Determinar los interesados y participantes en el proyecto y sus roles.

*Definir canales de comunicación***:** En esta actividad se define los miembros del proyecto que van a interactuar, para limitar los canales de comunicación a fin de hacer la comunicación efectiva durante el desarrollo del proyecto.

Establecer el plazo y fechas críticas: Se estima el tiempo que tomará realizar la implementación y se identifica los hitos.

Elaborar acta de reunión: Se emite un acta, en el cual se registra los temas tratados, los acuerdos y compromisos de los miembros del proyecto.

Elaborar diagrama de Gantt.

Es una herramienta para proyectar y programar tareas de un ciclo explícito, permite hacer rastreo del avance de las actividades a realizar por medio de la representación gráfica de estas en forma de barras que indica su duración. Para elaborar el diagrama de Gantt se realizó los siguientes pasos:

Definir lista de actividades, según el alcance definido.
Determinar tiempo estimado, según el alcance definido.
Establecer línea base.

Elaborar matriz RACI: RACI es una herramienta que se usa para asignar responsabilidades a todas las partes involucradas, a fin de ofrecer claridad y entendimiento de los diferentes roles en el proyecto. Para elaborar la matriz RACI se realizó los siguientes pasos:
Establecer actividades.
Identificar Stakeholders y roles.

Elaborar diagrama de arquitectura de Software: Se realiza un diagrama de los componentes y su relación entre ellos, para comprender el funcionamiento del software a implementar**.**

Definir casos de usos para pruebas: Se elabora un plan de pruebas para asegurarnos que el software está funcionando correctamente.

Fase 4: Implementación.

Para la implementación del plan de trabajo elaborado en la fase 3, a fin de cubrir cada brecha identificada, se realizaron las siguientes actividades:

Instalación del Software

Hardening del Software

Las siguientes actividades se realizarán por módulo:

Configuración del control de seguridad

Pruebas Post-Configuración

Liberar Módulo

Fase 5: Verificación.

El propósito de esta fase es validar las mejoras, después de la implementación de las medidas necesarias para el cumplimiento del requerimiento 10 de la norma PCI DSS. Esta etapa es importante para los procesos de mejora continua del banco, los cuales están documentados y activos para monitorear y optimizar sus controles de seguridad forma periódica.

Validar cumplimiento de metas: Para la verificación se desarrolló nuevamente el cuestionario.

CAPÍTULO IV. DESARROLLO DEL PROYECTO

En el presente capítulo se describe el detalle de lo realizado para lograr cada objetivo específico, lo cual se traduce en conseguir el objetivo general: cumplir con el requerimiento 10 del estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS) en la Entidad Bancaria.

4.1 Fase 1: Levantamiento de información

Para conocer el estado actual del cumplimiento de la normativa en estudio, se utilizó un cuestionario a fin de recolectar información necesaria. Se realizó los siguientes pasos:

Definir objetivo: El objetivo del cuestionario está alineado al primer objetivo específico: Evaluar el nivel de cumplimiento del requerimiento 10 de la norma PCI DSS.

Identificar a quien va dirigido: Se determinó que la persona más idónea para resolver el cuestionario es el responsable del Área de Seguridad de Información del banco.

Diseño del cuestionario: Las preguntas que conforma el cuestionario están basadas en lo propuesto por el consulado del estándar de seguridad PCI DSS, enfocado al requerimiento 10.

Ejecución del cuestionario: El cuestionario se ejecutó durante una reunión entre el auditor y el Jefe de Seguridad de Información del banco, en la cual se presentó las evidencias para sustentar el cumplimiento de cada punto del cuestionario (Los resultados se muestran en el anexo 1).

Analizar los resultados: Del cuestionario realizado, se muestran los resultados en la figura 9.

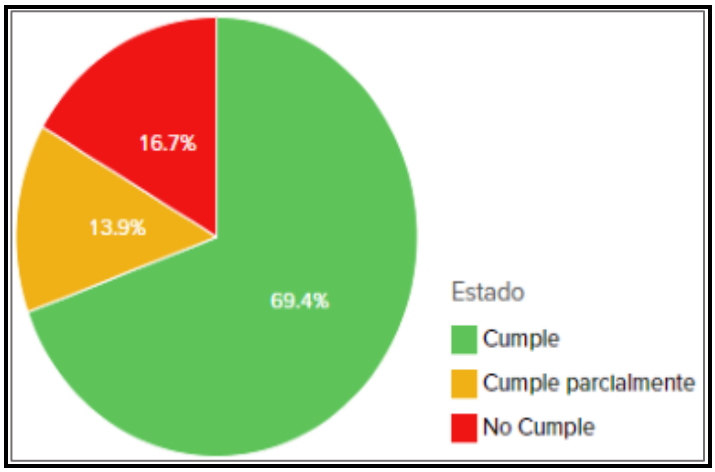


Figura 9. Cumplimiento del requerimiento 10 en el banco

Del análisis de resultados se concluye que el porcentaje de cumplimiento del requerimiento 10 de la norma PCI DSS era de 69.4 %. La diferencia de porcentaje está conformada por requerimientos que se cumplen parcialmente con un porcentaje de 13.9 % y los que no se cumplen con 16.7 %.

4.2 Fase 2: Diagnóstico.

Por medio de la información recolectada en el cuestionario realizado en la fase 1, se conoce la situación actual del banco con respecto al nivel de cumplimiento del requerimiento 10 de la norma PCI DSS. Esta información es utilizada para el análisis de brechas por medio de la metodología GAP Análisis. Los resultados del GAP Análisis se muestran en el anexo 2.

Como conclusión del análisis de brechas, se determinó que el control de seguridad que cubre las deficiencias encontradas es un software de Gestión Centralizada de Eventos (SIEM).

4.3 Fase 3: Planeamiento

En esta fase se realiza el plan de implementación del control de seguridad elegido para cubrir con las brechas encontradas en la fase 2. Para ello se realizó las siguientes actividades:

Kick Off

Es la reunión inicial del proyecto en la cual se trata principalmente los siguientes puntos:

Definir objetivos. El objetivo establecido es el siguiente: Implementar el software Log360 para el cumplimiento del requerimiento 10 de la norma PCI DSS.

Definir alcance. El control de seguridad es un SIEM, por lo que soporta la recolección de varios recursos o componentes como aplicaciones, dispositivos de red, servidores, etc. Sin embargo, por el presupuesto y prioridades, se determinó que el alcance de la implementación es auditar los tipos de servidores que se muestran en la tabla 5.

Tabla 5

Número de servidores para auditar

	Servidores para auditar	**Total de servidores**
Controladores de dominio	9	9
File Servers	4	4
Member Servers	50	457

Identificar Stakeholders: Los stakeholders identificados son los siguientes:

Personal del banco
Jefe de seguridad de información
Gestor de proyecto
Jefe de TI
Administrador de servidores
Proveedores
Auditor externo
Gestor de proyecto
Implementador

Definir canales de comunicación: En este paso se define quién se comunica con quién para que la comunicación sea efectiva durante la

implementación del control de seguridad. Se definió como único punto de contacto, los gestores del proyecto por parte del banco y el proveedor. A continuación, la Figura 10, representa el canal de comunicación definido:

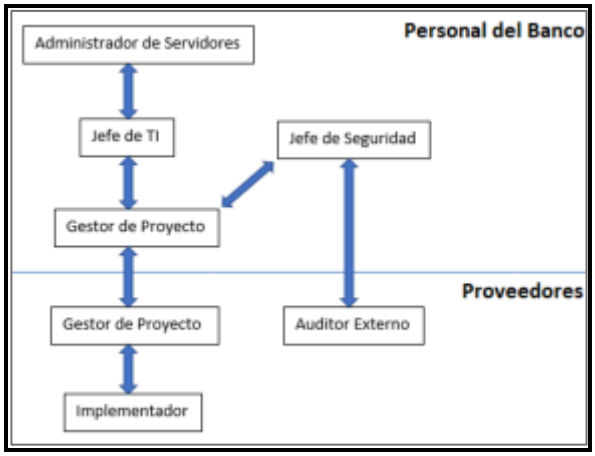


Figura 10. Canal de comunicaciones definido

Establecer el plazo y fechas críticas: Se estima que la duración del proyecto es de 39 días. Se muestra los detalles e hitos en la tabla 6.

Tabla 6 *Plazos de implementación e hitos*

Nombre de tarea	Duración	Comienzo	Fin
Fase 4: Implementación	**39 días**	**lun 4/03/19**	**lun 29/04/19**
Instalación	**1 día**	**lun 4/03/19**	**lun 4/03/19**
Módulo de Auditoría de Controladores de Dominio	**9 días**	**mar 5/03/19**	**vie 15/03/19**
Hito: Módulo de Auditoría de DCs acabado	0 días	vie 15/03/19	vie 15/03/19
Módulo de Auditoría de File Servers	**10 días**	**lun 18/03/19**	**vie 29/03/19**
Hito: Módulo de Auditoría de File Servers acabado	0 días	vie 29/03/19	vie 29/03/19
Módulo de Auditoría de Member Servers	**13 días**	**lun 1/04/19**	**mié 17/04/19**
Hito: Módulo de Auditoría de Member Servers acabado	0 días	mié 17/04/19	mié 17/04/19
Configuraciones Generales	**5 días**	**lun 22/04/19**	**vie 26/04/19**
Capacitación	1 día	lun 29/04/19	lun 29/04/19
Hito: Implementación terminada	0 días	lun 29/04/19	lun 29/04/19

Elaborar acta de reunión: Se emite un acta en la cual se registra lo mencionado en los puntos anteriores. Por motivos de confidencialidad no se puede anexar el acta por contener datos sensibles.

Elaborar diagrama de Gantt: Para elaborar el diagrama de Gantt se desarrollaron los siguientes pasos:

Definir lista de actividades.

Determinar tiempo estimado.

Tabla 7

Lista de actividades y duración

Nombre de tarea	Duración
Proyecto: Implementación Log360	**39 días**
Hito: Levantamiento de Información completado	0 días
Hito: Diagnóstico completado	0 días
Hito: Planeamiento completado	0 días
Fase 4: Implementación	**39 días**
Instalación	**1 día**
Instalar Software	1 día
Configurar Base de Datos	1 día
Hardening de Log360	1 día
Módulo de Auditoría de Controladores de Dominio	**9 días**
Agregar Dominio	1 día
Descubrir Controladores de Dominio	1 día
Habilitar Auditoría	3 días
Configurar Recolección de Eventos	2 días
Configurar Perfiles de Alertas	2 días
Pruebas Post-Configuración	2 días
Ajustes Finales	1 día
Hito: Módulo de Auditoría de DCs acabado	0 días
Módulo de Auditoría de File Servers	**10 días**
Descubrir File Servers	1 día
Descubrir recursos compartidos	1 día
Habilitar SACL	4 días
Configurar Recolección de Eventos	1 día
Configurar Perfiles de Alertas	2 días
Pruebas Post-Configuración	2 días
Ajustes Finales	1 día
Hito: Módulo de Auditoría de File Servers acabado	0 días
Módulo de Auditoría de Member Servers	**13 días**
Descubrir Member Servers	1 día
Habilitar Auditoría	3 días
Configurar Recolección de Eventos	1 día
Configurar File Integrity	2 días
Configurar Perfiles de Alertas	2 días
Pruebas Post-Configuración	3 días
Ajustes Finales	3 días
Hito: Módulo de Auditoría de Member Servers acabado	0 días
Configuraciones generales	**5 días**
Configurar archivado de Eventos	1 día
Configurar repositorio centralizado	1 día
Nombre de tarea	
Configurar horario de trabajo	1 día
Habilitar UBA	1 día
Programar Reportes	1 día
Administración de Técnicos	1 día
Habilitar Automonitoreo	1 día
Ajustes finales	2 días
Capacitación	1 día
Hito: Implementación completada	0 días
Fase 5: Verificación	0 días

En la tabla 7, se muestra la duración de cada actividad a realizar en la fase de implementación para cubrir las brechas identificadas. Los hitos que nos dan visibilidad del avance del desarrollo del proyecto, se representan con duración cero.

Establecer línea base: Una vez aprobado el diagrama de Gantt, se establece como línea base para determinar fácilmente si hay retrasos o adelantos en la implementación del control de seguridad (Anexo 3).

Elaborar matriz RACI.

Para la elaboración de la matriz RACI se realizó los siguientes pasos:

Establecer actividades: Lo que se muestra en la tabla 7.

Identificar Stakeholders y roles: Lo que se identificó en la actividad referente a stakeholders en el Kick Off. Como resultado se obtiene la matriz RACI (Anexo 4).

Elaborar diagrama de arquitectura de software: Se identificó los componentes necesarios los cuales se comunicarán entre ellos para llevar a cabo el proceso de auditoría de servidores:

Servidor de aplicación: Servidor donde se encuentra instalado el software.

Servidor de base de datos: Servidor donde se almacena de forma centralizada los registros de los servidores que se están auditando.

Servidores por auditar: Como se describió en el alcance, el control de seguridad va a auditar los siguientes tipos de servidores:

Servidor controlador de dominio
Servidor file servers
Servidores miembros

Servidor de almacenamiento: Servidor donde se almacenan los eventos archivados de todos los servidores que se están auditando.

Estación de trabajo: Terminal que, por medio del browser, se accede a la consola de la aplicación web. La figura 11, representa la arquitectura del software:

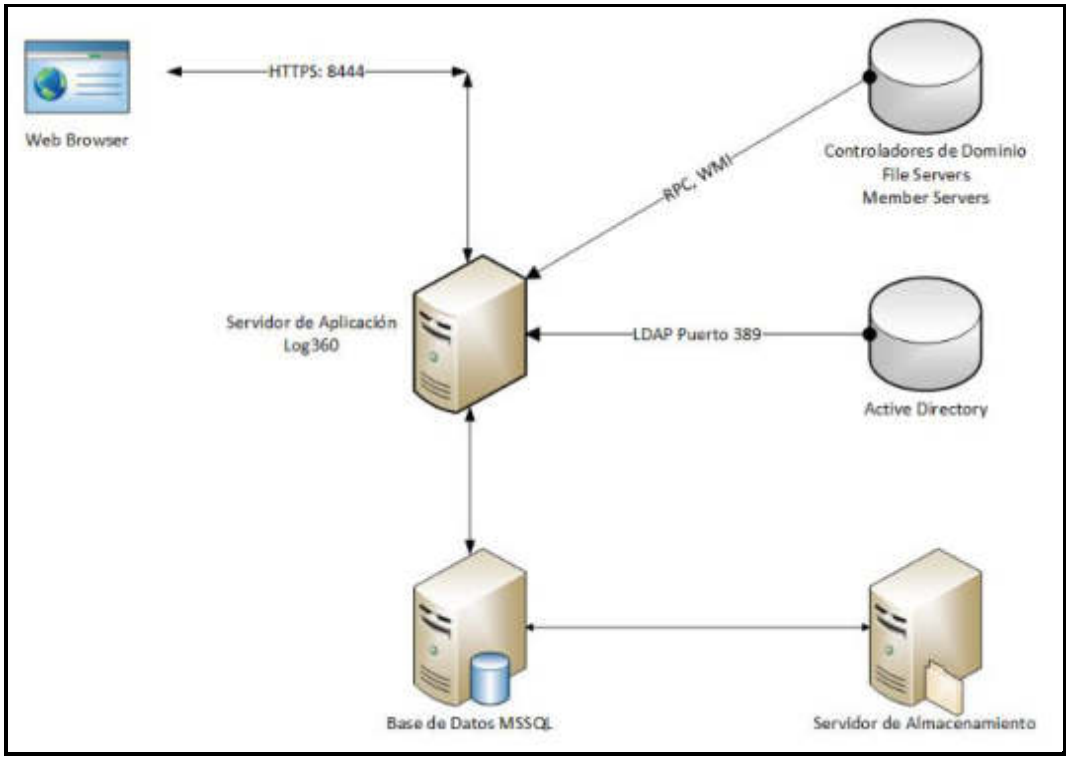


Figura 11. Arquitectura Software Log360

Definir casos de usos para pruebas: Las pruebas consisten en la simulación de eventos y validar que las actividades realizadas en los servidores auditados, estén registradas en el control de seguridad implementado. Se valida en los registros, los atributos mínimos que menciona el requerimiento 10.3.

4.4 Fase 4: Implementación

Instalación del Software: Se instalaron los componentes de la aplicación web, lo cuales son:

Tomcat 7.0.26
Java JRE 1.7.0_55
MSSQL 2016 Standard

Se crearon excepciones en el firewall para los puertos requeridos:
Puerto “389” para la comunicación con el protocolo LDAP.
Puerto “135” para la comunicación con RPC.
Puerto “445” para la comunicación con NetBios Session Service.

Hardening del Software: Como política del banco, todo software dentro de la organización debe pasar por un proceso de *Hardening* para asegurar la data que transfiere y procesa. Para esta actividad se siguió el manual propuesto por el fabricante. (Anexo 5).

Configuración del control de seguridad: En esta sección nos enfocaremos en los requerimientos no cubiertos, según el análisis de brechas, y las medidas realizadas durante la implementación para cumplir con lo que estipula el estándar de seguridad.

A continuación, se describe las actividades realizadas por cada brecha identificada:

Requerimiento 10.2.2. Son procesos realizados por personas que cuentan con autorización (PCI SSC, 2018).

Actividades realizadas.

Módulo de auditoría de controladores de dominio: habilitar auditoría.
Módulo de auditoría de File Servers: habilitar auditoría.
Módulo de auditoría de Member Servers: habilitar auditoría.

Se realizaron las configuraciones descritas en el anexo 6.

Requerimiento 10.2.5. Uso y cambios de los mecanismos de identificación y autenticación, incluidos, entre otros, la creación de nuevas cuentas y el aumento de privilegios, y de todos los cambios, incorporaciones y eliminaciones de las cuentas con privilegios administrativos o de raíz.

Actividades realizadas.

Módulo de auditoría de controladores de dominio: Habilitar auditoría.
Módulo de auditoría de File Servers: Habilitar auditoría.
Módulo de auditoría de Member Servers: Habilitar auditoría.

Se realizaron las configuraciones (descritas en el anexo 7).

Requerimiento 10.5.1. Control limitado de visualización de las pistas solo lo necesiten por motivos laborales.

Actividades realizadas.

Configuraciones generales - Administración de técnicos.

El control de seguridad permite la creación de roles para definir los permisos y privilegios de visualización a determinadas funcionalidades o reportes de pistas de auditoría. Cada usuario que requiera acceso se le creó una cuenta y rol asociado para auditar sus acciones en el software.

Se crearon los siguientes roles:

Administrador: este rol está asociado a un único usuario para evitar el riesgo de cambios no autorizados en el software.

Auditor: este rol tiene privilegios de solo lectura para consultar determinados reportes y evitar que realice cambios en la configuración del software. Se crearon tres cuentas asociados a este rol.

Requerimiento 10.5.2. Protege la data de vías de auditoría contra alteraciones no permitidas.

Actividades realizadas:

Módulo de auditoría de controladores de dominio: Configurar recolección de eventos.

Módulo de auditoría de File Servers: Configurar recolección de eventos.

Módulo de auditoría de Member Servers: Configurar recolección de eventos.

Con la recolección de eventos, configurada la lectura de registros y su procesamiento es interno, por lo que no está expuesta para evitar el riesgo de alteración o eliminación de pistas de auditoría. Se muestra la figura 12, como evidencia de la configuración de la recolección de eventos en tiempo real de los nueve controladores de dominio.

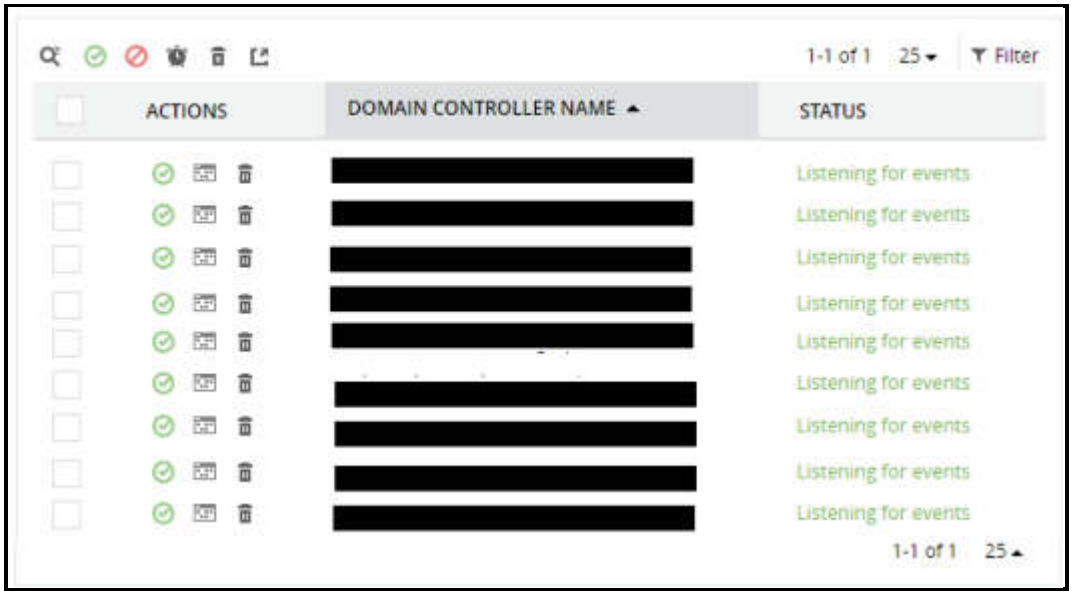


Figura 12. Recolección de eventos de los Domain Controllers auditados

Nota: Tomado de ManageEngine (2017a)

Requerimiento 10.5.3. Realice copias de seguridad de los archivos de las pistas de auditoría de manera oportuna en medios o servidores de registros centralizados que sean difíciles de modificar.

Actividad realizada.

Configuraciones generales: archivado de eventos.

La funcionalidad de archivados eventos permite hacer una copia de seguridad de las pistas de auditoría de diferentes categorías para que estas puedan ser consultadas, siempre que se necesite, restaurándolas nuevamente a la Base de Datos. Esto otorga un control del crecimiento en la utilización de los recursos de almacenamiento, pues mientras más data guardada, hay en la Base de Datos, el rendimiento del control de seguridad puede disminuir. Los parámetros utilizados en la configuración de esta funcionalidad están basados en el requerimiento 10.7. En la figura 13, se muestra la configuración realizada:

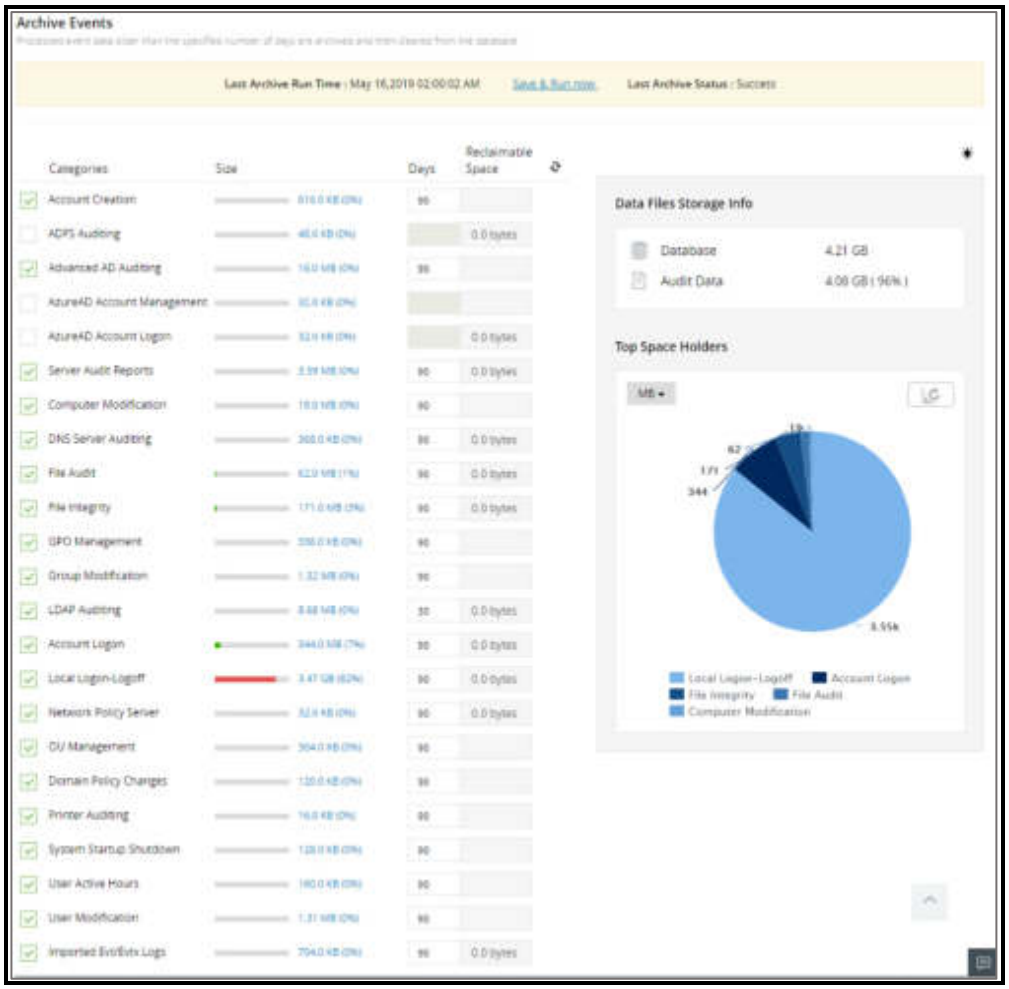


Figura 13. Archivado de eventos

Nota: Tomado de Manage Engine (2017a)

Requerimiento 10.5.4. Elabore registros para tecnologías externas en un dispositivo de medios o un servidor de registros interno, seguro y centralizado.

Actividad realizada.

Configuraciones generales: Configurar repositorio centralizado.

El archivado de eventos almacena de forma centralizada los eventos en un repositorio centralizado. Esta tarea la realiza de forma programada, como se muestra en la figura 14.

Figura 14. Archivado de eventos programado

Nota: Tomado de Manage Engine (2017a)

Los eventos los almacena en el recurso compartido que se desee. Tal como se muestra en la figura 15.

Figura 15. Repositorio centralizado de archivado de eventos

Nota: Tomado de ManageEngine (2017a)

En este caso, se configuró para que se almacene en servidor de archivos, al cual solo la cuenta de servicio asociada al control de seguridad implementado tiene acceso, para evitar que algún usuario acceda a este repositorio. Por otro lado, los eventos archivados están comprimidos con una contraseña para agregarle seguridad.

Requerimiento 10.5.5. Utilice el software de supervisión de integridad de archivos o de detección de cambios, en registros para asegurarse de que los datos de los registros existentes no se puedan cambiar sin que se generen alertas (aunque el hecho de agregar nuevos datos no deba generar una alerta).

Actividades realizadas.

Módulo de auditoría de Member Servers: Configurar File Integrity.

Módulo de auditoría de Member Servers: Configurar perfiles de alertas.

Se configuró la funcionalidad de File Integrity para la detección de cualquier cambio en los registros. Como también, un perfil de alerta que notificará cuando suceda los siguientes eventos:

Cambios de permisos

Se elimina archivos

Se modifica archivos

Se mueve o renombra archivos

Se copia los archivos

Intentos fallidos de acceso

Intentos fallidos de eliminación

A continuación, la figura 16, muestra la evidencia de lo configurado:

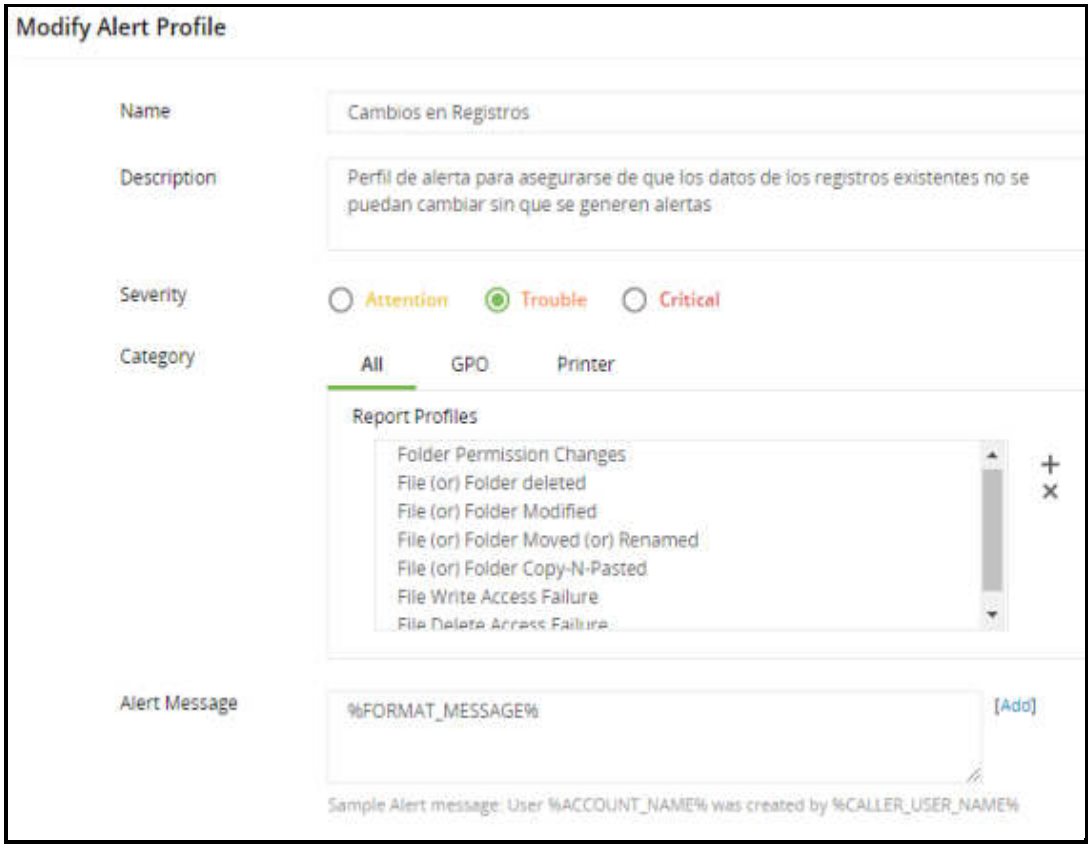


Figura 16. Alerta para detección de cambios en integridad de archivos

Nota: Tomado de Manage Engine (2017a)

Requerimiento 10.6.1. Revise los procesos, mínimo una vez al día:

Eventos de seguridad.

Registros de componentes que almacenan CHD y/o SAD

Registros de componentes críticos.

Registros de servidores y componentes del sistema de seguridad.

Actividades realizadas.

Configuraciones generales: Programar reportes.

Con el control de seguridad implementado, este requerimiento se cumple ya que la auditoría es automática y nos permite programar reportes para que se generen y envíen a diario al área de seguridad para su revisión. En la figura 17, se muestra cómo se programa un conjunto de reportes para que se envíen automáticamente a diario a las 7 de la mañana.

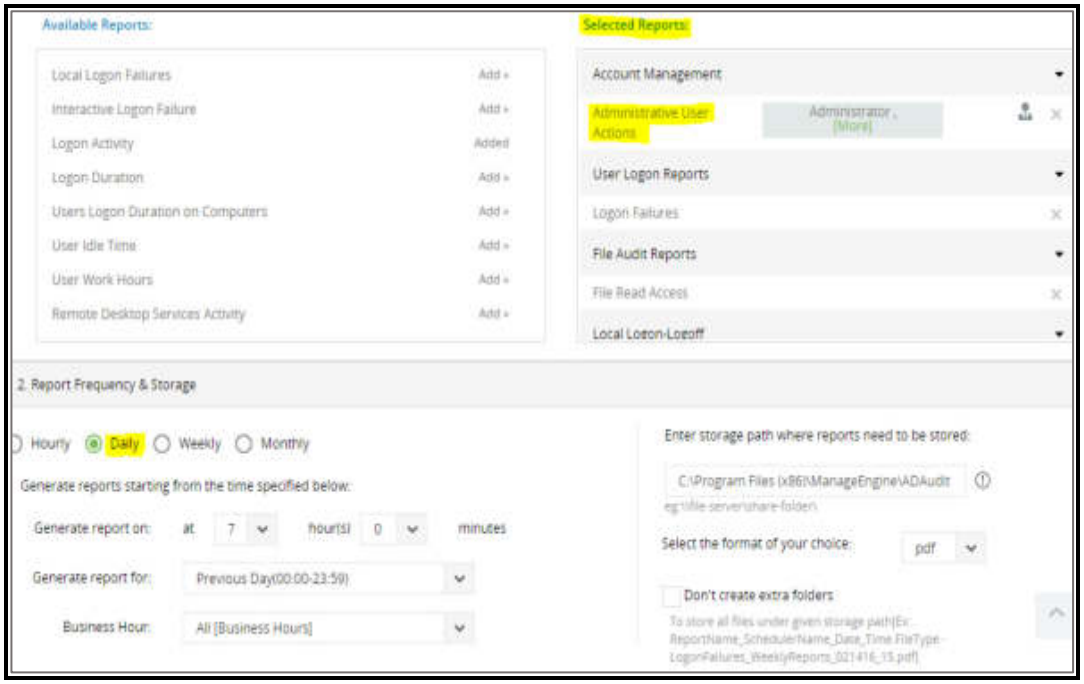


Figura 17. Programación de reportes para revisión diaria

Nota: Tomado de Manage Engine (2017a)

Sin embargo, como se describió en el alcance, actualmente el control de seguridad está auditando parte de los servidores, por lo que está pendiente los otros componentes del sistema CDE.

Requerimiento 10.6.3. Realice seguimiento de las excepciones detectadas.

Actividades realizadas.

Configuraciones generales: Habilitar UBA.

El control de seguridad necesita al menos siete días para aprender un control de comportamiento y utilizarlo como línea base para identificar actividades inusuales por parte de los usuarios. Mientras más data tiene el software, más precisión va a tener en la detección de anomalías.

Además, se crearon perfiles para la detección y seguimiento de las amenazas encontradas, tal como se muestra en la tabla 8.

Tabla 8

Criterio para detección de amenazas

Ataque	Comportamiento	Módulo del control de seguridad	Criterio de la regla
Ataques de Fuerza bruta	Consiste en probar varias combinaciones de contraseñas.	Auditoría de Domain Controllers	Un gran número de autenticaciones fallidas generadas en un período corto de tiempo.
Ransomware	El comportamiento en común de los diferentes ransomware es encriptar los archivos afectados.	Auditoría de File Servers	Se cambia la extensión de los archivos. Se renombra los archivos. Se cambia los permisos de varios archivos en un período corto de tiempo.

En la figura 18 se muestra los perfiles creados:

Figura 18. Perfiles creados para detección de anomalías y amenazas

Nota: Tomado de ManageEngine (2017a)

Pruebas Post-Configuración.

Después de configurar cada módulo, se realiza pruebas antes de su liberación. Las pruebas consisten en simular eventos de diferentes y validar que se hayan registrado en el control de seguridad (detalle en el anexo 8).

Liberar módulo.

Una vez validado el funcionamiento del módulo, este se pone en producción para que ya pueda ser utilizado, o en este caso, el software comience a recolectar registros del tipo de servidor, según el módulo liberado. El funcionamiento del módulo en producción se monitorea para determinar si necesita algún ajuste durante la etapa de implementación del control de seguridad.

4.5 Fase 5: Verificación

Se realizó las siguientes actividades para la evaluación del cumplimiento del objetivo.

Validar cumplimiento de metas.

Se desarrolló nuevamente el cuestionario para evaluar los resultados, después de la implementación del control de seguridad seleccionado (Los resultados se muestran en el nexo 9).

La figura 19, se muestra el porcentaje de cumplimiento actual.

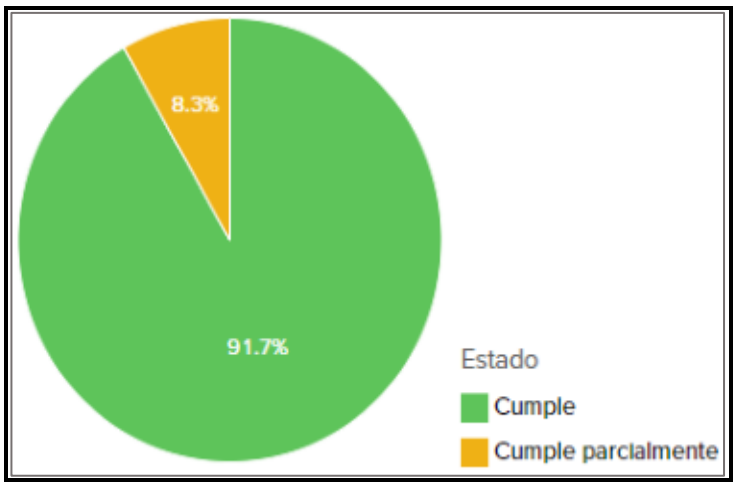


Figura 19. Resultado de la evaluación después de la implementación

De la evaluación del cumplimiento del requerimiento 10 de la norma PCI DSS, después de implementar el control de seguridad, se concluye que, el porcentaje de requerimientos que se cumplen totalmente, mejoró a

91.7 %. Mientras que el porcentaje de los requerimientos que se cumplen parcialmente disminuyó a 8.3 %. Los requerimientos que inicialmente no se cumplían, actualmente, se cumplen totalmente o de forma parcial, es por ello, por lo que su porcentaje es 0 %.

CAPÍTULO V. RESULTADOS

Este acápite presenta los resultados del estudio después de implementar el control de seguridad y las medidas requeridas para el acatamiento de los objetivos de la investigación.

Objetivo 1: Disminuir las brechas identificadas por medio de la implementación de un software SIEM, como control de seguridad seleccionado para el cumplimiento del requerimiento 10 de la norma PCI DSS.

A continuación, en la Tabla 9, se muestran por medio de indicadores, los resultados de cómo el control de seguridad implementado cubre cada brecha identificada en el GAP, análisis para disminuir su porcentaje.

Tabla 9

Indicadores de cumplimiento de cada brecha, antes y después de implementar el control de seguridad

Requerimiento 10	Antes	Después
10.2.2 Todas las acciones realizadas por personas con privilegios de raíz o administrativos		
10.2.5. Uso y cambios de los mecanismos de identificación y autenticación, incluidos nuevas cuentas y el aumento de privilegio, de todos los cambios, incorporaciones y eliminaciones de las cuentas con privilegios administrativos o de raíz.		
Requerimiento 10	**Antes**	**Después**
10.5.1. Limite la visualización de las pistas de auditoría a quienes lo necesiten por motivos laborales.		
10.5.2. Proteja los archivos de las pistas de auditoría contra modificaciones no autorizadas.		
10.5.3. Realice copias de seguridad de los archivos de las pistas de auditoría de manera oportuna en medios o servidores de registros centralizados que sean difíciles de modificar.		
10.5.4. Elabore registros para tecnologías externas en un dispositivo de medios o servidor de registros interno, seguro.		
10.5.5. Utilice el software de supervisión de integridad de archivos o de detección de cambios en registros para asegurarse de que los datos de los registros existentes no se puedan cambiar sin que se generen alertas (aunque el hecho de agregar nuevos datos no deba generar una alerta).		
10.6.1. Revise las opciones, al menos, una vez al día: • Todos los eventos de seguridad. • Registros de todos los componentes del sistema que almacenan, procesan o transmiten CHD y/o SAD • Registros de todos los componentes críticos del sistema. • Registros de todos los servidores y componentes del sistema de seguridad (por ejemplo, *firewalls*, IDS/IPS [sistemas de intrusión-detección y sistemas de intrusión-prevención], servidores de autenticación, etc.).		
10.6.3. Realice un seguimiento de las excepciones y anomalías detectadas en el proceso de revisión.		

De la tabla 9, se concluye que el objetivo 1 se cumple, pues el porcentaje de brechas, conformado por los requerimientos que cumplen parcialmente y no cumplen, disminuyó en un 22.3 %.

Objetivo 2: Reducir el tiempo de auditoría de usuarios con accesos privilegiados, a través de la recolección automática de eventos de los servidores auditados.

La tabla 10, describe los resultados obtenidos al automatizar el proceso de auditoría.

Tabla 10

Descripción del antes y después del proceso de auditoría

Antes	Después
Para cumplir los requerimientos solicitados por el Área de Seguridad del Banco para la auditoría de usuarios con accesos privilegiados, se realizaba el proceso de *Log Parser* lo cual es: Ineficiente: El proceso se realiza de forma manual. Complejo: Se trabaja desde la línea de comandos y se debe tener conocimiento avanzado de programación y base de datos para cualquier modificación de los reportes. Arriesga la integridad de los registros de servidores auditados: La data se maneja en procesadores de textos, lo cual permite modificar o eliminar registros.	El control de seguridad implementado, colecta en tiempo real de logs de los servidores auditados por medio de protocolos y una credencial con privilegios de lectura de logs, para luego, procesar la información y mostrarlo en reportes intuitivos y fáciles de personalizar. Reduciendo de esta manera, el tiempo que ocupa la auditoría de usuarios privilegiados. Eficiente: La recolección de eventos y su procesamiento es automática. Como también, el envío de reportes programados mensualmente, para cumplir con los requerimientos de auditoría. Es decir, el software trabaja por sí solo. Fácil: La interfaz es gráfica e intuitiva, por lo que sí, se necesita alguna modificación en los reportes (aplicar filtros, definir periodo, agregar o remover columnas, etc.) no se necesita un especialista. Protege la integridad de los registros de los servidores auditados: Ya que, la recolección y procesamiento de los registros es interno, no pueden alterarse.

Los requerimientos de auditoría del área de seguridad, que consiste en reportes que dan visibilidad de lo que acontece en la red de la organización, son solicitados cada fin de mes, por medio del catálogo de servicio, en el cual, se puede hacer el seguimiento del tiempo transcurrido para atender la solicitud.

En la tabla 11, se muestran los tiempos necesarios para la auditoría de usuarios con accesos privilegiados, antes y después de implementar el control de seguridad. La implementación finalizó a fines de abril.

Tabla 11

Tiempos de atención para los requerimientos de auditoría

	Antes
Enero	43 horas y 13 minutos
Febrero	38 horas y 22 minutos
Marzo	59 horas y 7 minutos
	Después
Abril	4 minutos y 37 segundos
Mayo	Se estima un tiempo alrededor de los 5 minutos

Tal como se muestra en la figura 20, se representan en minutos, los datos de la tabla anterior.

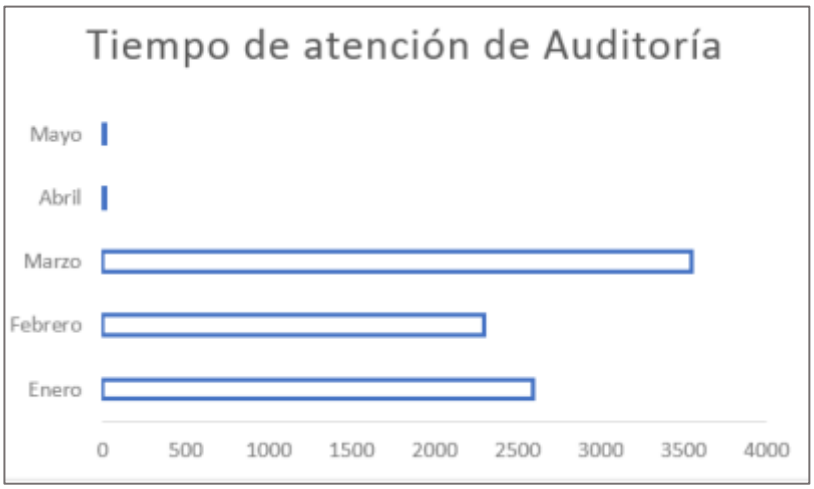


Figura 20. Tiempo de atención de usuarios con acceso predilecto

De la figura 20, se concluye que se cumple el objetivo 2, ya que el tiempo se reduce drásticamente, debido a la automatización del proceso por medio del control de seguridad implementado.

Objetivo 3: Aumentar la eficiencia del proceso de detección de amenazas internas y comportamientos inusuales de los usuarios internos en la organización.

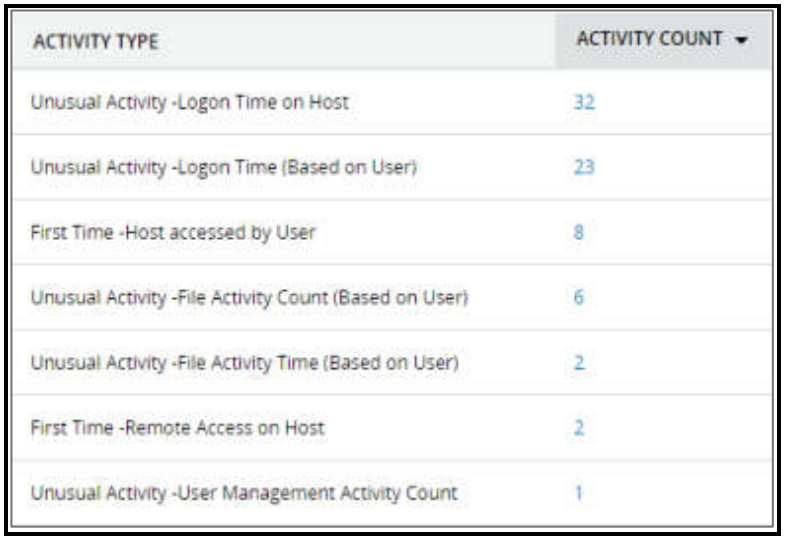
La tabla 12, muestra el antes y después de la implementación, respecto a la detección de amenazas y comportamientos inusuales de los usuarios.

Tabla 12

Descripción del proceso de detección de amenazas y comportamientos

Antes	Después
El análisis de los registros para la detección de amenazas y anomalías en las actividades de los usuarios se realiza de forma manual, por lo que el proceso es ineficiente y propenso al error humano, por lo que hay riesgo de que no se detecten o genere demasiados falsos positivos de amenazas.	El control de seguridad implementado, ahora permite detectar de forma eficiente amenazas, creando reglas en base al comportamiento de ataques.

Por medio de la tecnología UBA se realizó el análisis de las actividades de los usuarios para detectar de forma automática comportamientos inusuales. La figura 21, muestra los resultados.



ACTIVITY TYPE	ACTIVITY COUNT
Unusual Activity -Logon Time on Host	32
Unusual Activity -Logon Time (Based on User)	23
First Time -Host accessed by User	8
Unusual Activity -File Activity Count (Based on User)	6
Unusual Activity -File Activity Time (Based on User)	2
First Time -Remote Access on Host	2
Unusual Activity -User Management Activity Count	1

Figura 21. Anomalías detectadas por UBA

Nota: Tomado de Manage Engine (2017a)

La tabla 13, muestran los datos del total de eventos detectados por mes en el año 2019.

Tabla 13

Amenazas y anomalías detectadas antes y después de la implementación del control de seguridad

	Eventos detectados	Falsos positivos	Amenazas	Actividades inusuales	Ataques informáticos
			Antes		
Enero	27	26	1	No hay visibilidad	0
Febrero	22	22	0	No hay visibilidad	0
Marzo	33	33	0	No hay visibilidad	0
			Después		
Abril	83	7	2	74	0

La figura 22, expresa los valores de la tabla 13.

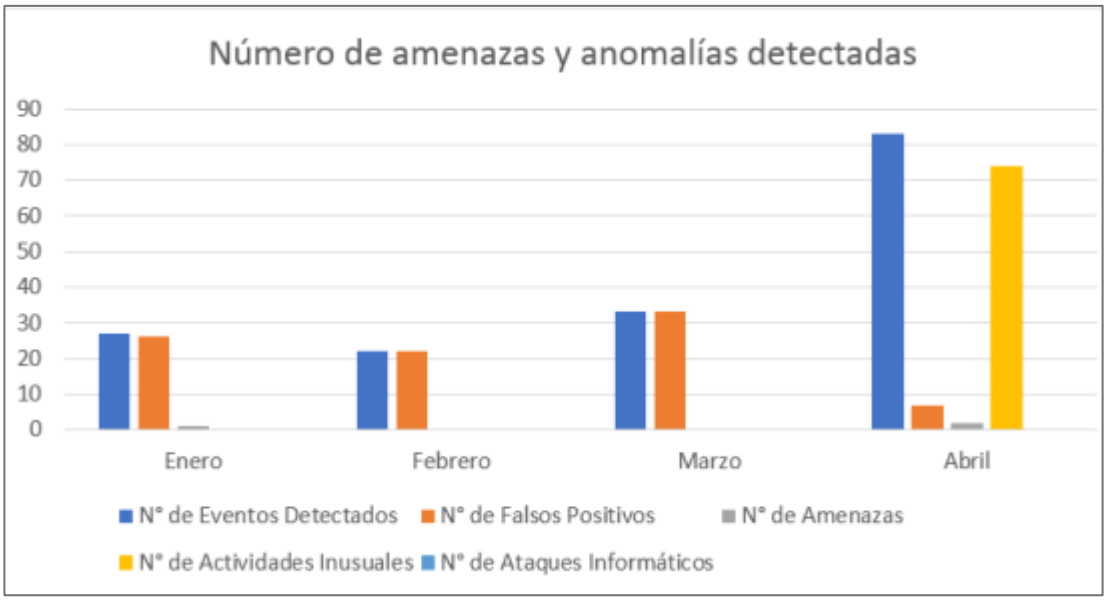


Figura 22. Número de amenazas y anomalías detectadas en el año 2019

De la figura 22, se concluye que se cumple el objetivo 3, ya que aumenta la eficiencia de detección al disminuir los falsos positivos e incrementar el número de amenazas y comportamientos inusuales detectados.

Objetivo general.

Cumplir con el requerimiento 10 del estándar de seguridad de datos para la industria de tarjeta de pago (PCI DSS) en la Entidad Bancaria.

El cumplimiento de los objetivos específicos, mencionados anteriormente, se traduce en el cumplimiento del objetivo general**.**

Se realizó una evaluación de la situación inicial por medio de un cuestionario y posteriormente, se realizó la verificación del cumplimiento del objetivo después de la implementación. En la Tabla 14, se muestra los resultados del antes y después.

Tabla 14

Resultados del antes y después de implementar el control de seguridad

Antes	Después
El banco utilizaba un control de seguridad compensatorio que cubría parcialmente el requerimiento 10 del estándar de seguridad en estudio.	Una vez implementado el control de seguridad adecuado y las medidas necesarias, se volvió a realizar el análisis de cumplimiento.

El porcentaje de cumplimiento antes y después se aprecia en la figura 23.

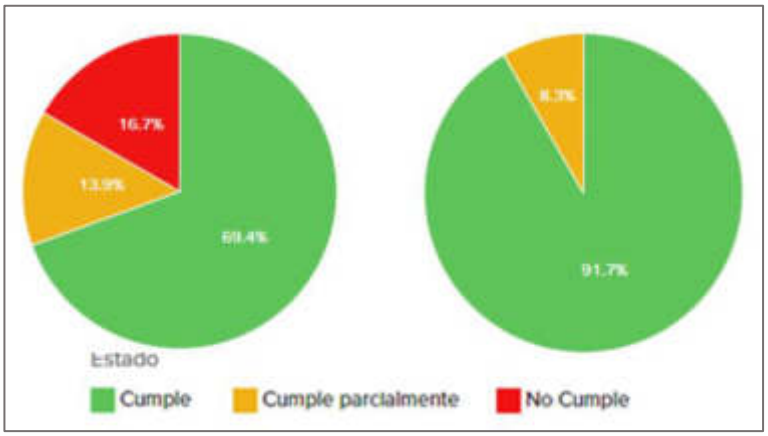


Figura 23. Porcentaje de cumplimiento antes y después

Según los datos mostrados, se concluye que el objetivo se cumple, pues el porcentaje de cumplimiento aumento a un 91.7 %.

CAPÍTULO VI. DISCUSIÓN

En este capítulo se analizan, se interpretan y se sustentan los resultados obtenidos por cada objetivo específico definido en este trabajo de tesis.

Tabla 15

Comparativa entre objetivos y resultados

Objetivo	Situación Inicial	Resultado Esperado	Resultado Final
Disminuir las brechas identificadas por la implementación de un software SIEM, como control de seguridad seleccionado, para el acatamiento de la exigencia 10 de la norma PCI DSS.	Alto porcentaje de brechas por la limitada gestión de eventos e información de seguridad, debido al control compensatorio en uso.	Lograr reducir las brechas identificadas para el cumplimiento del requerimiento 10 de la norma PCI DSS, a través de la implementación de un software SIEM.	Se redujo el número de brechas exitosamente por medio de la implementación del control de seguridad seleccionado.
Reducir el tiempo de atención de los requerimientos de auditoría a través de la recolección y procesamiento automático de eventos de los servidores auditados.	Ineficiente proceso para cumplir con los requerimientos de auditoría del Área de Seguridad de Información del banco.	Lograr automatizar el proceso de auditoría de forma segura y centralizada para disminuir el tiempo que se necesita para atender cualquier requerimiento de auditoría.	Se consiguió reducir drásticamente el tiempo de atención a los requerimientos de auditoría, debido a la automatización del proceso por medio del control de seguridad implementado.
Aumentar la eficiencia del proceso de detección de amenazas internas y comportamientos inusuales de los usuarios internos en la organización.	Complejo proceso para detectar amenazas internas y comportamientos inusuales de los usuarios internos del banco.	Lograr incrementar la eficacia en la detección de amenazas y anomalías en el comportamiento de los usuarios de la organización.	Se logró aumentar la eficiencia de detección al disminuir los falsos positivos e incrementar el número de amenazas y comportamientos inusuales detectados.

Objetivo 1: Disminuir las brechas identificadas por medio de la implementación de un software SIEM, como control de seguridad seleccionado, para el acatamiento de la exigencia 10 de la norma PCI DSS.

La banca es uno de los sectores económicos que más importancia debe darle a la seguridad informática. Como se puede ver en la Figura 24, desde el inicio, la mayoría de los puntos del requerimiento 10, del estándar de seguridad en estudio, se cumplen.

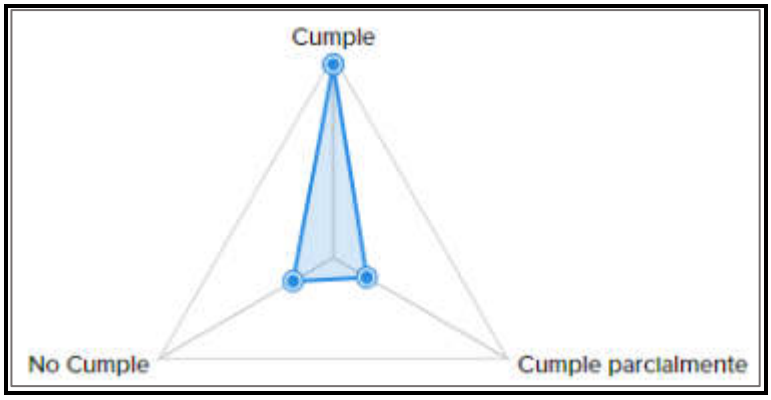


Figura 24. Web Chart del estado de cumplimiento del requerimiento 10

Esto se debe a que el banco ya tiene implementado otros estándares como la ISO/IEC 27001 y Ley de Protección de Datos (Ley N° 29733), los cuales coinciden con algunos requerimientos de la norma PCI DSS. Por lo que este estándar no reemplaza, los ya implementados, si no, los complementa para darle más seguridad a la organización.

La figura 25, muestra los valores porcentuales del cumplimiento del requerimiento 10.

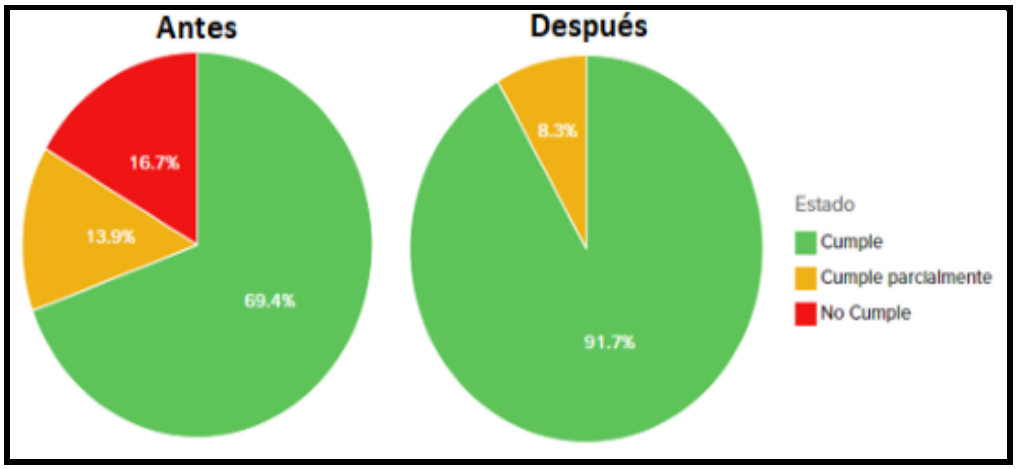


Figura 25. Cumplimiento del requerimiento 10 de la norma PCI DSS

Antes, el banco estuvo utilizando un control compensatorio, el cual es el proceso manual de Log Parser, por lo que la visibilidad de lo que sucedía en los recursos críticos de la organización, era limitada. Debido a esto, era ineficiente la detección de amenazas o comportamientos inusuales de los usuarios. Otra brecha detectada, es la falta de seguridad en proteger y almacenar las pistas de auditoría de los diferentes componentes o recursos que se están auditando, en un repositorio centralizado. Por ello, como resultado en este escenario el porcentaje de "No cumple" es 16.7 % y "Cumple parcialmente" es 13.9 %.

Actualmente, el control de seguridad implementado es un SIEM, por lo tanto, tiene la capacidad de colectar y auditar de forma segura y automática, las pistas de seguridad de otros recursos o sistemas externos (Aplicaciones, routers, firewall, etc.); sin embargo, el alcance de la implementación, debido a presupuesto y prioridades, es auditar los servidores. Debido a esto, los requerimientos que hacen referencia a la auditoría de otros componentes, no se satisfacen totalmente como resultado, el porcentaje de "Cumple parcialmente" es 8.3 %.

Objetivo 2: Reducir el tiempo de auditoría de usuarios con accesos privilegiados a través de la recolección automática de eventos de los servidores auditados.

Otras de las mejoras, después de implementar el control de seguridad, es la eficiencia en la auditoría de las actividades de los usuarios con privilegios. Como se mostró en el capítulo de los Resultados, el tiempo promedio que le tomaba atender al área de TI, los requerimientos de auditoría del área de seguridad de información del banco, era de alrededor de una semana. Actualmente, la auditoría lo hace de forma automática, por lo que el tiempo se redujo considerablemente y ya no ocupa tiempo del personal del banco. Además, permite cumplir con el requerimiento 10.6.1. que consiste en revisar los eventos de seguridad diariamente, esto último, se cumple por medio de reportes programados que se envían a diario al área de seguridad.

Objetivo 3: Aumentar la eficiencia del proceso de detección de amenazas internas y comportamientos inusuales de los usuarios internos en la organización.

Actualmente, el banco es capaz de detectar eficientemente amenazas y comportamientos inusuales de los usuarios por medio de UBA, una tecnología que utiliza inteligencia artificial y *machine learning*. El control de seguridad, en base a los registros de actividades de los empleados del banco, aprende un patrón de comportamiento de los usuarios para utilizarlo como línea base. Cada desviación del proceder de un usuario en referencia a esa línea base, se considera una actividad inusual o anómala en su comportamiento. Es importante señalar que mientras más datos se tiene de las actividades del usuario, más preciso es la detección de anomalías. Ya que, recientemente se ha implementado el control de seguridad, los indicadores mostrados por ahora no son muy exactos y según el seguimiento que se está haciendo a estos indicadores, la tendencia es que está disminuyendo.

CONCLUSIONES

En este capítulo se describe lo más destacado del desarrollo de la tesis y la comprobación de los objetivos específicos.

Se implementó un software SIEM (Gestión de Eventos e Información de Seguridad), como el control de seguridad seleccionado, con el cual se cubren gran parte de las brechas identificadas, obteniendo así, una reducción de estas en 22.3%.

Se automatizó el proceso de auditoría de usuarios con accesos privilegiados, reduciendo considerablemente el tiempo de ejecución. Al eliminar el elemento humano, podemos garantizar el funcionamiento correcto y efectivo del control de seguridad, como también, reducir el costo general relacionado con la realización del proceso de auditoría.

Se aumentó la eficiencia en la detección de amenazas y anomalías por medio de inteligencia artificial y *machine learning*, reduciendo así, los falsos positivos y obteniendo visibilidad de los comportamientos inusuales de los usuarios dentro de la organización, lo cual, nos permite prevenir que las amenazas se materialicen reduciendo sus riesgos o minimizando su impacto.

Se extendió el nivel de acatamiento de la exigencia 10 de la norma PCI DSS, debido al logró de los objetivos específicos mencionados. Actualmente, la entidad financiera se encuentra en un 91.7%.

RECOMENDACIONES

En este capítulo se describen sugerencias en relación con las conclusiones y los resultados obtenidos, ya que la investigación no ha podido dar respuesta, debido al alcance definido.

Incluir en el control de seguridad implementado, los recursos externos, aplicaciones, dispositivos de red y el resto de los componentes del CDE que no se han considerado, según el alcance de la implementación, para así cumplir en un 100 % el requerimiento 10 de la norma PCI DSS.

Mantener actualizado el software SIEM implementado, para mejorar o añadir nuevas funcionalidades, aplicar *fixes* o dar mayor seguridad a la aplicación.

Utilizar los resultados de auditoría obtenidos del control de seguridad, implementado para planificar estrategias de ciberseguridad.

Implementar la correlación de eventos, una vez incluido el resto de los componentes del CDE.

Habilitar la funcionalidad de UEBA (User and Entity Behavior Analytics), una vez incluido el resto de los componentes del CDE, para no solo analizar el comportamiento de los usuarios, sino también, de entidades como servidores, aplicaciones, dispositivos de red, etc.

BIBLIOGRAFÍA

Acosta, D. (2018a). ¿Cómo funcionan las tarjetas de pago? Parte I: PAN (Primary Account Number). Recuperado de https://www.pcihispano.com/como-funcionan-las-tarjetas-de-pago-parte-i-pan-primary-account-number/

Acosta, D. (2018b). ¿Cómo funcionan las tarjetas de pago? Parte II: CID/CAV2/CVC2/CVV2. Recuperado de https://www.pcihispano.com/como-funcionan-las-tarjetas-de-pago-parte-ii-cidcav2cvc2cvv2/

Acosta, D. (2018c). ¿Cómo funcionan las tarjetas de pago? Parte III: PIN (Personal Identification Number). Recuperado de https://www.pcihispano.com/como-funcionan-las-tarjetas-de-pago-parte-iii-pin-personal-identification-number/

Acosta, D. (2018d). ¿Cómo funcionan las tarjetas de pago? Parte IV: Banda magnética. Recuperado de https://www.pcihispano.com/como-funcionan-las-tarjetas-de-pago-parte-iv-banda-magnetica/Benenaula, P. M., & Ortega, E. L. (2016). *Auditoría de sistemas al cumplimiento de los requerimientos 7, 8, 9 de la norma PCIDSS aplicada a Coral Hipermercado, Racar Plaza con corte a junio de 2015* (Tesis de grado, Universidad de Cuenca, Ecuador). Recuperada de http://dspace.ucuenca.edu.ec/bitstream/123456789/25053/1/Tesis.pdf

Bernabé, M. A. (2015). *Análisis de las normas PCI DSS para agregar seguridad a los pagos en línea y propuesta de una guía de aplicación*.

(Tesis de grado, Universidad de Guayaquil, Guayaquil, Ecuador). Recuperada de http://repositorio.ug.edu.ec/bitstream/redug/10036/1/PTG-703%20Bernab%C3%A9%20Baldano%20Manuel%20Alonso.pdf

Calle, Z. A., & Mejía, A. J. (2015). *Análisis de la implementación del estándar PCI DSS en la seguridad de la información dentro de una institución financiera* (Tesis de grado, Universidad Politécnica Salesiana, Guayaquil, Ecuador). Recuperada de https://dspace.ups.edu.ec/bitstream/123456789/10317/1/UPS-GT001 222.pdf

Crowd Research. (2018*). Insider Threat. 2018 report*. Recuperado de https://crowdresearchpartners.com/wpcontent/uploads/2017/07/Insider-Threat-Report-2018.pdf

Framingham, M. (2018). All Categories of Smart Home Devices Forecast to Deliver Double-Digit Growth Through 2022, Says IDC. Recuperado de https://www.idc.com/getdoc.jsp?containerId=prUS44361618

Gener, L. (2019). Un cambio de enfoque para la evaluación de riesgos operacionales de bancos en entornos altamente digitalizados. Recuperado de https://www.researchgate.net/publication/330482342_Un_cambio_de_enfoque_para_la_evaluacion_de_riesgos_operacionales_de_bancos_en_entornos_altamente_digitalizados

Ley N° 29733, Ley de Protección de Datos. (21 de junio de 2011). Recuperado de http://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

ManageEngine. (2017a). How SIEM can help with auditing and compliance. Recuperado de https://blogs.manageengine.com/it-security/2017/12/04/how-siem-can-help-with-auditing-and-compliance.html

ManageEngine. (2017b). Log management and SIEM fundamentals: Comprehensive log collection and auditing. Recuperado de https://blogs.manageengine.com/it-security/2017/06/28/log-management-and-siem-fundamentals-comprehensive-log-collection-and-auditing.html

ManageEngine. (2018a). Adopting a SIEM solution, Part 1: Why choose SIEM? Recuperado de https://blogs.manageengine.com/it-security/2018/06/06/adopting-siem-solution-part-1-choose-siem.html

ManageEngine. (2018b). User behavior analytics for streamlined threat detection. Recuperado de https://blogs.manageengine.com/active-directory/2018/11/15/user-behavior-analytics-streamlined-threat-detection.html

Microsoft. (2005). Log Parser 2.0. Recuperado de https://www.microsoft. com/en-us/download/details.aspx?id=24659

Organización de los Estados Americanos. (2018). *Estado de la ciberseguridad en el sector bancario en América Latina y el Caribe*. Recuperado de http://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

PCI Security Standards Council (2016). *Sistemas de pago comunes*. Recuperado de https://es.pcisecuritystandards.org/_onelink_/ pcisecurity/en2es/minisite/en/docs/Small_Merchant_Common_Payme nt_Systems.pdf

PCI Security Standards Council. (2018a). PCI DSS *Quick Reference Guide*. Recuperado de https://www.pcisecuritystan.-AaAadards.org/documen ts/PCI_DSS-QRG-v3_2_1.pdf?agreement=true&time=1558761421694

PCI Security Standards Council. (2018b). *Cuestionario de autoevaluación D y Atestación de cumplimiento*. Recuperado de https://es.pcisecurity standards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_ v3-2-1_SAQ_D_Merchant_es-LA.pdf

PCI Security Standards Council (2018c). *Norma de seguridad de datos de la industria de tarjetas de pago (PCI), versión 3.2.1*. Recuperado de https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisit e/en/docs/PCI_DSS_v3-2-1-ES-LA.PDF

Ponemon Insttute. (2018). Data loss Prevention - Why data loss prevention. Recuperado de https://www.coursehero.com/file/pqoqufp/The-cost-to-remediate-a-data-leak-can-be-high-and-can-grow-with-time-Measured/

Ramakrishnan, G. (2013). *Administración de riesgos de la banca por internet*. Recuperado de https://www.cuentasclarasdigital.org/wp-content/uploads/2013/07/Administraci%C3%B3n-de-riesgo-de-la-Banca-por-Internet.pdf

Sarbanes-Oxley Act, Pub. L. No. 107-204, 116 Stat. 745 (30 de julio de 2002) Recuperado de http://www.soxlaw.com/

Smith, C. (2016). The Latin America e-commerce report: the region's top markets, biggest growth opportunities, and foreign retailers making inroads – clone. Recuperado de https://www.businessinsider.com/latin-america-e-commerce-report-the-regions-top-markets-biggest-growth-opportunities-and-foreign-retailers-making-inroads-2016-4

ANEXOS

Anexo 1: Desarrollo del cuestionario

Pregunta		Estado	Indicador
10.1	(a) ¿Las pistas de auditoría están habilitadas y activas para los componentes del sistema?	**Cumple**	
	(b) ¿El acceso a los componentes del sistema está vinculado a usuarios específicos?	**Cumple**	
10.2	¿Se implementan pistas de auditoría automatizadas para todos los componentes del sistema a fin de reconstruir los siguientes eventos?		
10.2.1	Todos los usuarios acceden a los datos de titulares de tarjetas.	**Cumple**	
10.2.2	Todas las acciones realizadas por personas con privilegios de raíz o administrativos.	**Cumple parcialmente**	
10.2.3	Acceso a todas las pistas de auditoría.	**Cumple**	
10.2.4	Intentos de acceso lógico no válidos.	**Cumple**	
10.2.5	Uso y cambios de los mecanismos de identificación y autenticación, incluidos, entre otros, la creación de nuevas cuentas y el aumento de privilegios, y de todos los cambios, incorporaciones y eliminaciones de las cuentas con privilegios administrativos o de raíz.	**Cumple parcialmente**	
10.2.6	¿Hay inicialización, detención o pausa de los registros de auditoría?	**Cumple**	
10.2.7	¿Creación y eliminación de objetos de nivel de sistema?	**Cumple**	

Pregunta		Estado	Indicador
10.3	¿Se registran las siguientes entradas de pistas de auditoría de todos los componentes del sistema para cada evento?		
10.3.1	Identificación de usuarios.	**Cumple**	
10.3.2	Tipo de evento.	**Cumple**	
10.3.3	Fecha y hora.	**Cumple**	
10.3.4	Indicación de éxito o fallo.	**Cumple**	
10.3.5	Origen del evento.	**Cumple**	
10.3.6	Identidad o nombre de los datos, componentes del sistema o recurso afectados.	**Cumple**	
10.4	¿Se sincronizan todos los relojes y horas críticos del sistema a través del uso de la tecnología de sincronización de hora, la cual se mantiene actualizada?		
10.4.1	¿Están implementados los siguientes procesos para que los sistemas críticos tengan la hora correcta y correspondiente?		
	(a) ¿Solamente los servidores de horario central designados reciben señales de tiempo de fuentes externas, y las señales de tiempo de fuentes externas están basadas en la hora atómica internacional o UTC?	**Cumple**	
	(b) En los casos en los que hay más de un servidor de horario designado, ¿estos se emparejan para mantener la hora exacta?	**Cumple**	
	(c) ¿Los sistemas reciben información horaria solo de los servidores de horario central designados?	**Cumple**	

Pregunta		Pregunta	Indicador
10.4.2	¿Se protegen los datos de tiempo de la siguiente manera:		
	(a) ¿Se restringe el acceso a los datos de horario solo al personal con una necesidad de negocio de acceder a dichos datos?	**Cumple**	
	(b) ¿Se registran, supervisan y revisan los cambios a los parámetros de hora en los sistemas críticos?	**Cumple**	
10.4.3	¿Se recibe la configuración de hora de fuentes específicas y aceptadas por la industria? (Esto es para impedir que una persona malintencionada cambie el reloj).		
	De forma opcional, estas actualizaciones pueden cifrarse con una clave simétrica, y pueden crearse listas de control de acceso que especifiquen las direcciones IP de equipos cliente a los que se proporcionarán las actualizaciones de hora (para evitar el uso no autorizado de servidores horarios internos).	**Cumple**	
10.5	¿Se aseguran de la siguiente manera las pistas de auditoría de manera que no se puedan alterar?		
10.5.1	¿Se limita la visualización de pistas de auditoría a quienes lo necesitan por motivos de trabajo?	**No Cumple**	
10.5.2	¿Están protegidos los archivos de las pistas de auditoría contra modificaciones no autorizadas a través de los mecanismos de control de acceso, segregación física y/o segregación de redes?	**Cumple parcialmente**	
10.5.3	¿Se realizan de inmediato copias de seguridad de los archivos de las pistas de auditoría en un servidor de registros central o medios que resulten difíciles de modificar?	**Cumple parcialmente**	

Pregunta		Estado	Indicador
10.5.4	¿Se copian los registros para tecnologías externas (por ejemplo, tecnologías inalámbricas, firewalls, DNS, correo) en medios o servidores de registros centralizados, internos y seguros?	**No Cumple**	
10.5.5	¿Se utiliza el software de supervisión de integridad de archivos o de detección de cambios en registros para asegurarse de que los datos de los registros existentes no se puedan cambiar sin que se generen alertas (agregar nuevos datos no deba generar una alerta)?	**No Cumple**	
10.6	¿Se revisan los registros y los eventos de seguridad en todos los componentes del sistema para identificar anomalías o actividades sospechosas?		
10.6.1	(a) ¿Están las políticas y los procedimientos escritos definidos para revisar lo siguiente, al menos, una vez al día, ya sea manualmente o con herramientas de registro? • Todos los eventos de seguridad. • Registros de todos los componentes del sistema que almacenan, procesan o transmiten CHD y/o SAD • Registros de todos los componentes críticos del sistema. • Registros de todos los servidores y componentes del sistema que realizan funciones de seguridad.	**No Cumple**	
	(b) ¿Se revisan los eventos de seguridad y registros mencionados como mínimo diariamente?	**No Cumple**	

Preguntas			Estado	Indicador
10.6.2	(a)	¿Están las políticas y los procedimientos escritos definidos para realizar una revisión periódica de los registros de todos los demás componentes del sistema, ya sea de forma manual o con herramientas de registros, según las políticas y estrategia de gestión de riesgos de la organización?	**Cumple**	
	(b)	¿Se realizan las revisiones de todos los demás componentes del sistema según la política y estrategia de gestión de riesgos de la organización?	**Cumple**	
10.6.3	(a)	¿Están las políticas y los procedimientos escritos definidos para realizar un seguimiento de las excepciones y anomalías detectadas en el proceso de revisión?	**Cumple parcialmente**	
	(b)	¿Se realiza un seguimiento de las excepciones y anomalías?	**No Cumple**	
10.7	(a)	¿Hay implementadas políticas y procedimientos de retención de registros de auditorías, y es necesario que se conserven los registros al menos un año, con un mínimo de disponibilidad inmediata para análisis de tres meses (por ejemplo, en línea, archivados o recuperables para la realización de copias de seguridad)?	**Cumple**	
	(b)	¿Se retienen los registros de auditoría por al menos un año?	**Cumple**	
	(c)	¿Se encuentran disponibles al menos los registros de los últimos tres meses para el análisis?	**Cumple**	

Pregunta		Estado	Indicador
10.8	*Este requisito se aplica solamente a los proveedores de servicios.*		
10.9	¿Las políticas de seguridad y los procedimientos operativos para la supervisión de todo el acceso a los datos de titulares de tarjetas y los recursos de red ▪ ¿Están documentados? ▪ ¿Están en uso? ▪ ¿Son de conocimiento para todas las partes afectadas?	**Cumple**	

Fuente: PCI Security Standards Council, 2018b.

Anexo 2: Resultados del GAP análisis

Estado Actual	Expectativa	Brecha
Se identificó que la auditoría de accesos está habilitada en los componentes que se desean auditar. Estos registros de accesos están vinculados a usuarios específicos.	**10.1** Implemente pistas de auditoría para vincular todo acceso a componentes del sistema con usuarios específicos.	No existe.
	10.2 Implemente pistas de auditoría automáticas en todos los componentes del sistema a fin de reconstruir los siguientes eventos:	
Actualmente sí se están generando pistas de auditoría automática para los accesos a los datos del titular de la tarjeta.	**10.2.1** Todo acceso por parte de usuarios a los datos del titular de la tarjeta.	No existe.
Se identificó que la auditoría no está habilitada correctamente en los servidores que conforman el CDE.	**10.2.2** Todas las acciones realizadas por personas con privilegios de raíz o administrativos.	Debido a que la auditoría en los servidores no está correctamente configurada. No se tiene visibilidad de todas las acciones realizadas por usuarios con privilegios.
Actualmente sí se está generando registros, respecto a los accesos a las pistas de auditoría.	**10.2.3** Acceso a todas las pistas de auditoría.	No existe.
Actualmente sí se está generando registros de los eventos fallidos de autenticación.	**10.2.4** Intentos de acceso lógico no válidos.	No existe.
Se identificó que la auditoría no está habilitada correctamente en los servidores que conforman el CDE.	**10.2.5** Uso y cambios de los mecanismos de identificación y autenticación, incluidos, entre otros, la creación de nuevas cuentas y el aumento de privilegios, y de todos los cambios, incorporaciones y eliminaciones de las cuentas con privilegios administrativos o de raíz.	Debido a que la auditoría en los servidores no está correctamente configurada. No se tiene visibilidad de todos los cambios realizados por usuarios con privilegios.
Actualmente sí se está generando registros de cuando un usuario malintencionado detiene los registros de auditoría en un componente.	**10.2.6** Inicialización, detención o pausa de los registros de auditoría.	No existe.

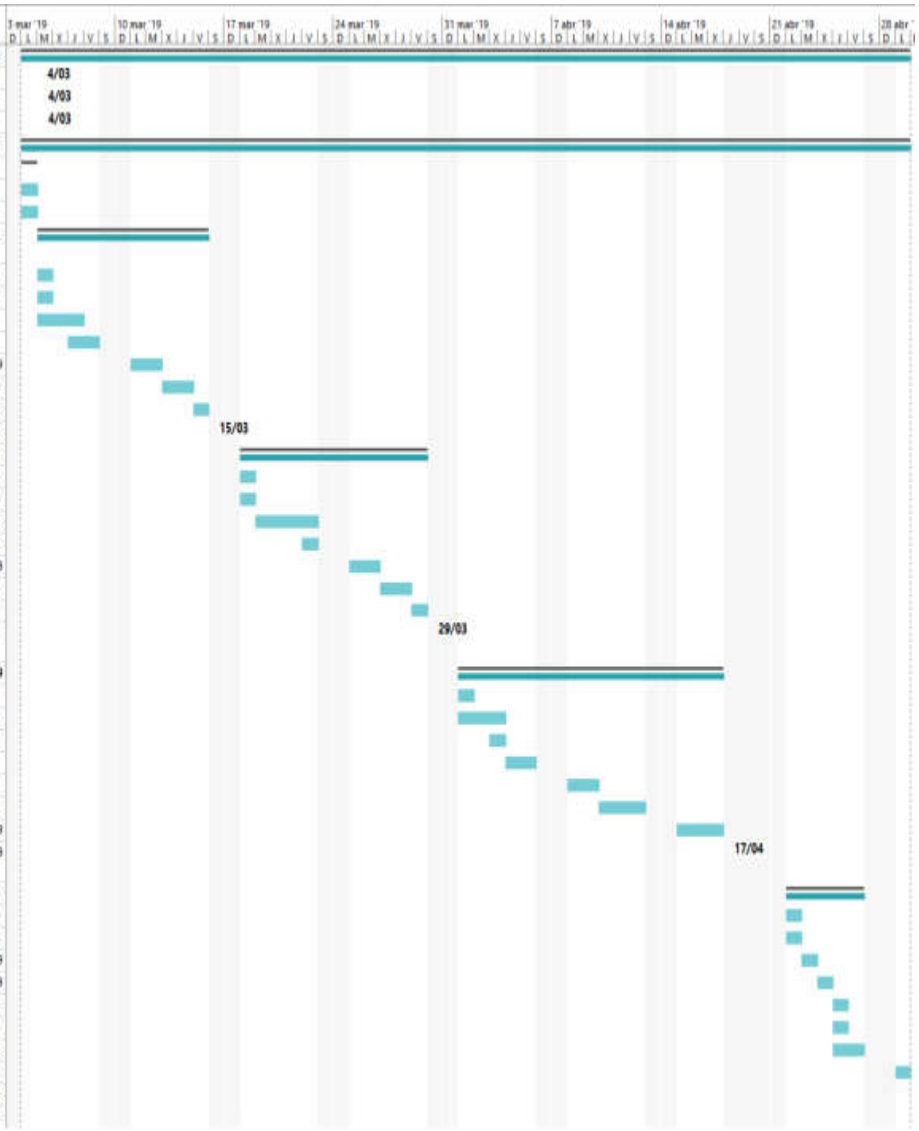
Estado Actual	Expectativa	Brecha
Actualmente sí se está generando registros cuando se crea o elimina objetos.	**10.2.7** Creación y eliminación de objetos en el nivel del sistema.	No existe.
	10.3 Registre, al menos, las siguientes entradas de pistas de auditoría de los componentes del sistema para cada evento:	
Los registros sí muestran el nombre de usuario que realiza la acción. ¿Quién lo hizo?	**10.3.1** Identificación de usuarios.	No existe.
Los registros sí muestran el tipo de evento. ¿Qué hizo?	**10.3.2** Tipo de evento.	No existe.
Los registros sí muestran la fecha y hora. ¿Cuándo lo hizo?	**10.3.3** Fecha y hora.	No existe.
Los registros sí muestran si la acción se realizó satisfactoriamente o fallo.	**10.3.4** Indicación de éxito o fallo.	No existe.
Los registros sí muestran información respecto al origen del evento.	**10.3.5** Origen del evento.	No existe.
Los registros sí muestran el componente o recurso afectado.	**10.3.6** Identidad o nombre de los datos, componentes del sistema o recursos afectados.	No existe.
	10.4 Utilizando tecnología de sincronización, sincronice todos tiempos y relojes críticos y asegúrese de que lo siguiente sea implementado para adquirir, distribuir y almacenar tiempos. ***Nota:*** *Un ejemplo de tecnología de sincronización es el NTP (protocolo de tiempo de red).*	
Todos los sistemas y servidores están sincronizados los relojes por NTP.	**10.4.1** Los sistemas críticos tienen un horario uniforme y correcto.	No existe.
El acceso a los datos de tiempo está limitado solo al personal que corresponde como también hay supervisión de los cambios.	**10.4.2** Los datos de tiempo están protegidos.	No existe.
Se verificó que actualmente las fuentes externas para los datos de tiempo están validadas por el banco.	**10.4.3** Los parámetros de la hora se reciben de fuentes aceptadas por la industria.	No existe.

Estado Actual	Expectativa	Brecha
	10.5 Proteja las pistas de auditoría para que no se puedan modificar.	
Actualmente personas que son ajenas al área de seguridad tienen acceso a las pistas de auditoría, lo cual no es lo recomendado.	**10.5.1** Limite la visualización de las pistas de auditoría a quienes lo necesiten por motivos laborales.	No hay controles de acceso a las pistas de seguridad.
El proceso de auditoría es manual, parte del procedimiento se trabaja en procesadores de texto, lo cual permite modificar o eliminar pistas de auditoría.	**10.5.2** Proteja los archivos de las pistas de auditoría contra modificaciones no autorizadas.	No hay protección durante el proceso de auditoría actual, por ello pone en riesgo la integridad de las pistas de auditoría.
Actualmente se está archivando eventos con la directiva nativa del sistema operativo Windows, lo cual no es seguro.	**10.5.3** Realice copias de seguridad de los archivos de las pistas de auditoría de manera oportuna en medios o servidores de registros centralizados que sean difíciles de modificar.	No se está archivando los eventos de forma centralizada y segura.
Actualmente los registros de las tecnologías externas tienen su propio repositorio por lo que no se almacenan de forma centralizada.	**10.5.4** Elabore registros para tecnologías externas en un dispositivo de medios o un servidor de registros interno, seguro y centralizado.	No se están almacenando los registros de las tecnologías externas de forma segura ni centralizada.
El proceso de auditoría de registros es manual por lo que no hay alertas de cambios.	**10.5.5** Utilice el software de supervisión de integridad de archivos o de detección de cambios en registros para asegurarse de que los datos de los registros existentes no se puedan cambiar sin que se generen alertas (aunque el hecho de agregar nuevos datos no deba generar una alerta).	No hay software de supervisión de integridad de archivos o de detección de cambios.
	10.6 Revise los registros y los eventos de seguridad en todos los componentes del sistema para identificar anomalías o actividades sospechosas. ***Nota:*** *Para cumplir con este requisito, se pueden usar herramientas de recolección, análisis y alerta de registros.*	

Estado Actual	Expectativa	Brecha
Actualmente el proceso manual de auditoría hace muy difícil la revisión de registros de los componentes del sistema.	**10.6.1** Revise las siguientes opciones, al menos, una vez al día: - Registros de todos los componentes del sistema que almacenan, procesan o transmiten CHD y/o SAD - Registros de todos los componentes críticos del sistema. - Registros de todos los servidores y componentes del sistema que realizan funciones de seguridad (por ejemplo, firewalls, IDS/IPS [sistemas de intrusión-detección y sistemas de intrusión-prevención], servidores de autenticación, servidores de redireccionamiento de comercio electrónico, etc.).	No se está cumpliendo la revisión diaria de los registros debido a la ineficiencia del proceso auditoría de estos.
Se verificó que se está realizando la revisión periódica de registros según la evaluación de riesgo.	**10.6.2** Revise los registros de todos los demás componentes del sistema periódicamente, de conformidad con la política y la estrategia de gestión de riesgos de la organización y según lo especificado en la evaluación anual de riesgos de la organización.	No existe.
El proceso manual que se está realizando dificulta hacer un correcto seguimiento de las excepciones y anomalías.	**10.6.3** Realice un seguimiento de las excepciones y anomalías detectadas en el proceso de revisión.	No se está haciendo de forma eficiente el seguimiento de las excepciones y anomalías.
Actualmente se están archivando los registros de auditoría periódicamente.	**10.7** Conserve el historial de pistas de auditorías durante, al menos, un año, con un mínimo de disponibilidad para análisis de tres meses.	No existe.
	10.8 *Este requisito se aplica solamente a los proveedores de servicios.*	
Se validó que actualmente los procedimientos para auditar los accesos a los recursos de la red están documentados y en uso.	**10.9** Asegúrese de que las políticas de seguridad y los procedimientos operativos para monitorear todos los accesos a los recursos de la red y a los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.	No existe.

Anexo 3: Diagrama de Gantt

Id	Nombre de tarea	Duración	Comienzo	Fin
1	**Proyecto: Implementación Log360**	**39 días?**	**lun 4/03/19**	**lun 29/04/19**
2	**Hito: Levantamiento de Información completado**	0 días	lun 4/03/19	lun 4/03/19
3	**Hito: Diagnóstico completado**	0 días	lun 4/03/19	lun 4/03/19
4	**Hito: Planeamiento completado**	0 días	lun 4/03/19	lun 4/03/19
5	**Fase 4: Implementación**	**39 días?**	**lun 4/03/19**	**lun 29/04/19**
6	**Instalación**	**1 día**	**lun 4/03/19**	**lun 4/03/19**
7	Instalar Software	1 día	lun 4/03/19	lun 4/03/19
8	Configurar Base de Datos	1 día	lun 4/03/19	lun 4/03/19
9	**Módulo de Auditoría de Controladores de Dominio**	**9 días**	**mar 5/03/19**	**vie 15/03/19**
10	Agregar Dominio	1 día	mar 5/03/19	mar 5/03/19
11	Descubrir Controladores de Dominio	1 día	mar 5/03/19	mar 5/03/19
12	Habilitar Auditoría	3 días	mar 5/03/19	jue 7/03/19
13	Configurar Recolección de Eventos	2 días	jue 7/03/19	vie 8/03/19
14	Configurar Perfiles de Alertas	2 días	lun 11/03/19	mar 12/03/19
15	Pruebas Post-Configuración	2 días	mié 13/03/19	jue 14/03/19
16	Ajustes Finales	1 día	vie 15/03/19	vie 15/03/19
17	Hito: Módulo de Auditoría de DCs acabado	0 días	vie 15/03/19	vie 15/03/19
18	**Módulo de Auditoría de File Servers**	**10 días?**	**lun 18/03/19**	**vie 29/03/19**
19	Descubrir File Servers	1 día	lun 18/03/19	lun 18/03/19
20	Descubrir recursos compartidos	1 día	lun 18/03/19	lun 18/03/19
21	Habilitar SACL	4 días	mar 19/03/19	vie 22/03/19
22	Configurar Recolección de Eventos	1 día	vie 22/03/19	vie 22/03/19
23	Configurar Perfiles de Alertas	2 días	lun 25/03/19	mar 26/03/19
24	Pruebas Post-Configuración	2 días	mié 27/03/19	jue 28/03/19
25	Ajustes Finales	1 día	vie 29/03/19	vie 29/03/19
26	Hito: Módulo de Auditoría de File Servers acabado	0 días	vie 29/03/19	vie 29/03/19
27	**Módulo de Auditoría de Member Servers**	**13 días?**	**lun 1/04/19**	**mié 17/04/19**
28	Descubrir Member Servers	1 día	lun 1/04/19	lun 1/04/19
29	Habilitar Auditoría	3 días	lun 1/04/19	mié 3/04/19
30	Configurar Recolección de Eventos	1 día	mié 3/04/19	mié 3/04/19
31	Configurar File Integrity	2 días	jue 4/04/19	vie 5/04/19
32	Configurar Perfiles de Alertas	2 días	lun 8/04/19	mar 9/04/19
33	Pruebas Post-Configuración	3 días	mié 10/04/19	vie 12/04/19
34	Ajustes Finales	3 días	lun 15/04/19	mié 17/04/19
35	Hito: Módulo de Auditoría de Member Servers acabado	0 días	mié 17/04/19	mié 17/04/19
36	**Configuraciones Generales**	**5 días**	**lun 22/04/19**	**vie 26/04/19**
37	Configurar archivado de Eventos	1 día	lun 22/04/19	lun 22/04/19
38	Configurar horario de trabajo	1 día	lun 22/04/19	lun 22/04/19
39	Habilitar UBA	1 día	mar 23/04/19	mar 23/04/19
40	Programar Reportes	1 día	mié 24/04/19	mié 24/04/19
41	Administración de Técnicos	1 día	jue 25/04/19	jue 25/04/19
42	Habilitar Automonitoreo	1 día	jue 25/04/19	jue 25/04/19
43	Hardening de Log360	2 días	jue 25/04/19	vie 26/04/19
44	**Capacitación**	1 día	lun 29/04/19	lun 29/04/19
45	**Hito: Implementación completada**	0 días	lun 29/04/19	lun 29/04/19
46	**Fase 5: Verificación**	0 días	lun 29/04/19	lun 29/04/19



Anexo 4: Matriz RACI

		Entidad Financiera					Proveedores	
		Jefe de Seguridad de Información	Gestor de Proyecto	Jefe de TI	Administrador de Servidores	Auditor	Gestor de Proyecto	Técnico Implementador
	Descripción de la actividad							
Instalación	Instalar Software	I	I	C	C		A	R
	Configurar Base de Datos	I	I	C	C		A	R
Módulo de Auditoría de Controladores de Dominio	Agregar Dominio	I	I	C	C		A	R
	Descubrir Controladores de Dominio	I	I	C	C		A	R
	Habilitar Auditoría	I	I	A	R		I	C
	Configurar Recolección de Eventos	I	I	C	C		A	R
	Configurar Perfiles de Alertas	I	I			C	A	R
	Pruebas Post-Configuración	I	I			C	A	R
	Ajustes Finales	I	I			C	A	R
	Liberar Módulo	I	A			C	C	R
Módulo de Auditoría de File Servers	Descubrir File Servers	I	I	C	C		A	R
	Descubrir recursos compartidos	I	I	C	C		A	R
	Habilitar SACL	I	I	A	R		I	C
	Configurar Recolección de Eventos	I	I	C	C		A	R
	Configurar Perfiles de Alertas	I	I	C	C	C	A	R
	Pruebas Post-Configuración	I	I			C	A	R
	Ajustes Finales	I	I			C	A	R
	Liberar Módulo	I	A			C	C	R
Módulo de Auditoría de Member Servers	Descubrir Member Servers	I	I	C	C		A	R
	Habilitar Auditoría	I	I	A	R		I	C
	Configurar Recolección de Eventos	I	I	C	C		A	R
	Configurar File Integrity	I	I			C	A	R
	Configurar Perfiles de Alertas	I	I	C	C	C	A	R
	Pruebas Post-Configuración	I	I			C	A	R
	Ajustes Finales	I	I			C	A	R
	Liberar Módulo	I	A			C	C	R
Configuraciones Generales	Configurar archivado de Eventos	I	I	C	C	C	A	R
	Configurar horario de trabajo	I	I				A	R
	Habilitar UBA	I	I				A	R
	Programar Reportes	I	I			C	A	R
	Administración de Técnicos	C	I			C	A	R
	Habilitar Automonitoreo	I	I				A	R
	Hardening de Log360	I	I	C	C	C	A	R

R — **RESPONSIBLE (EJECUTOR)**: Persona responsable de completar el entregable asignado

A — **ACCOUNTABLE (RESPONSABLE)**: Dueño de la tarea. Para la decisión final sobre la misma.

C — **CONSULTADO**: Persona consultada antes de la toma de decisiones o acciones

I — **INFORMADO**

Anexo 5: Hardening de Seguridad para Log360

1. Siguiendo el principio de privilegio mínimo

Una cuenta de usuario de Active Directory (AD) generalmente se asocia con Log360 para la recopilación de datos registrados. Si se usa una cuenta de administrador de dominio, Log360 comienza a auditar los cambios en su entorno de AD. Pero, en general, una cuenta de administrador de dominio tiene varios derechos y privilegios elevados que Log360 no requiere. Es por esto, que recomendamos crear cuentas de usuario dedicadas que solo tengan los privilegios y permisos necesarios para que Log360 realice su trabajo. De esta manera, incluso si se compromete una cuenta de usuario dedicada, el impacto de la infracción está contenido de manera innata.

2. Asegurar la cuenta de administrador incorporada

Log360 viene con una cuenta de administrador integrada con privilegios definitivos. De forma predeterminada, la contraseña de esta cuenta es la misma para todos los clientes de Log360, lo que significa que necesita cambiar esta contraseña para asegurarla correctamente. Si se pasa por alto este paso, dejará su sistema vulnerable.

3. Habilitando HTTPS para una comunicación segura

Le recomendamos que utilice HTTPS sobre HTTP para garantizar el transporte seguro de información a través de su red. Puede hacerlo desde la interfaz de usuario en la pestaña Administrador. Vaya a la configuración que se encuentra en Configuración general> Conexión.

Estas configuraciones pueden optimizarse aún más dentro del siguiente archivo XML:

- conf\server.xml> connector (encuentre el conector HTTPS correspondiente a su número de puerto configurado).

Si elige permitir solo una versión particular de Seguridad de la capa de transporte (TLS), es decir, TLSv1, TLSv1.1 o TLSv1.2, puede deshabilitar las

otras versiones modificando el siguiente parámetro, manteniendo solo las versiones TLS requeridas:

- sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"

Si desea deshabilitar o restringir los cifrados, puede hacerlo modificando el siguiente parámetro para que solo contenga los cifrados necesarios:

ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA"

Con estos cambios, puede asegurar toda la comunicación a través de Log360 y fortalecer la seguridad.

4. Restricción del acceso de inicio de sesión al servidor Log360

Para fortalecer aún más la seguridad de Log360, le recomendamos que restrinja el acceso de inicio de sesión al servidor Log360, evitando así, el acceso injustificado. Puede definir la configuración de la directiva local en la pestaña Asignación de derechos de usuario, dentro del Editor de administración de directivas de grupo, para permitir el inicio de sesión localmente o permitir el inicio de sesión, a través de Servicios de escritorio remoto, solo para un conjunto específico de usuarios. De esta manera, reduce la superficie de ataque de su infraestructura.

5. Restricción del acceso a la carpeta de instalación de Log360

Los administradores pueden restringir el acceso a la carpeta de instalación de Log360, modificando los permisos de las carpetas. Esto garantiza que nadie, excepto los usuarios permitidos, tenga acceso a los archivos de Log360.

6. Auditoría de cambios en la carpeta de instalación de Log360

Log360 permite, el registro de cambios de su carpeta de instalación mediante la configuración de la lista de control de acceso al sistema (SACL). Todos los cambios realizados en esta carpeta se presentan como informes para garantizar la integridad del archivo. De esta manera, puede estar seguro de que nadie ha manipulado la información.

7. Asegurar su base de datos con protección de contraseña adicional

Log360 viene con una base de datos PostgreSQL incorporada y protegida por contraseña, que permite el acceso solo al personal autorizado. De forma predeterminada, el servicio PostgreSQL crea una cuenta de usuario con privilegios no restringidos, similar a una cuenta de administrador de dominio en AD, para realizar varias acciones administrativas. Log360 cambia la contraseña predeterminada de esta cuenta y crea otra, de usuario con privilegios limitados. Esta nueva cuenta tiene permiso restringido, se utiliza para conectarse a la base de datos y se cifra para garantizar la seguridad. Los roles de técnico se pueden configurar para limitar el acceso a ciertos informes. Estas funciones también pueden impedir que los técnicos realicen funciones administrativas, como agregar o eliminar servidores para la auditoría, modificar los ajustes de configuración, etc. Además, Log360 proporciona un seguimiento detallado de la auditoría basada en el usuario de todas las acciones realizadas.

9. Asegurar la transferencia de datos a través de la red

Para recopilar registros de eventos, Log360 le permite elegir entre los siguientes modos de obtención de eventos:

- Modo en tiempo real.
- Modo nativo.
- Modo EvtQuery.
- Modo WMI.

De forma predeterminada, los modos en tiempo real y EvtQuery cifran los datos transferidos a través de la red. Los modos WMI y Nativo, de manera

predeterminada, no cifran los datos transferidos, pero el cifrado se puede habilitar en el modo WMI para mayor seguridad. Recomendamos que los administradores utilicen el modo en tiempo real para garantizar la transferencia segura de datos y para obtener actualizaciones instantáneas de todos los cambios de AD.

10. Restricción del acceso a la base de datos desde la interfaz de usuario

Log360 de forma predeterminada, deshabilita el acceso a la base de datos desde su interfaz de usuario y permite que solo la cuenta de administrador predeterminada habilite esta opción. El administrador también puede elegir qué cuentas tienen este privilegio. Esto evita que otras cuentas de técnicos modifiquen o eliminen información de la base de datos.

11. Asegurando los datos archivados

Para reducir el consumo de espacio de almacenamiento dentro de la base de datos, los datos históricos se pueden comprimir y almacenar por separado. Estos archivos se pueden restaurar en un momento posterior. Estos, archivados están protegidos con contraseña por Log360 para garantizar la seguridad. Para una capa adicional de seguridad, le recomendamos que restrinja el acceso a las carpetas que contienen estos archivos.

12. Protegiendo los informes exportados y programados.

Cuando un usuario exporta un informe en un formato particular (PDF, CSV, etc.), o cuando un usuario programa un informe particular para guardarlo localmente, los archivos están protegidos por contraseña por Log360. También, se recomienda que modifique los permisos de carpeta para la otra que contiene estos archivos para evitar el acceso injustificado.

Log360 permite a los administradores habilitar el Protocolo ligero de acceso a directorios (LDAP) a través de Secure Sockets Layer (SSL) para garantizar que toda la comunicación de los datos de Active Directory esté encriptada.

Anexo 6: Manual para habilitar auditoría en servidores.

Configurar Auditoría en Controladores de Dominio

Pasos para editar **Default Domain Controllers Policy**

1. Inicie sesión en Windows con una cuenta que tenga derechos de administrador.

2. Asegúrese de que el complemento Directivo de grupo está instalado.

3. Abra la GPMC (Group Policy Management Console) en servidores de Windows 2003.

4. Vaya a " **Default Domain Controllers Policy**"

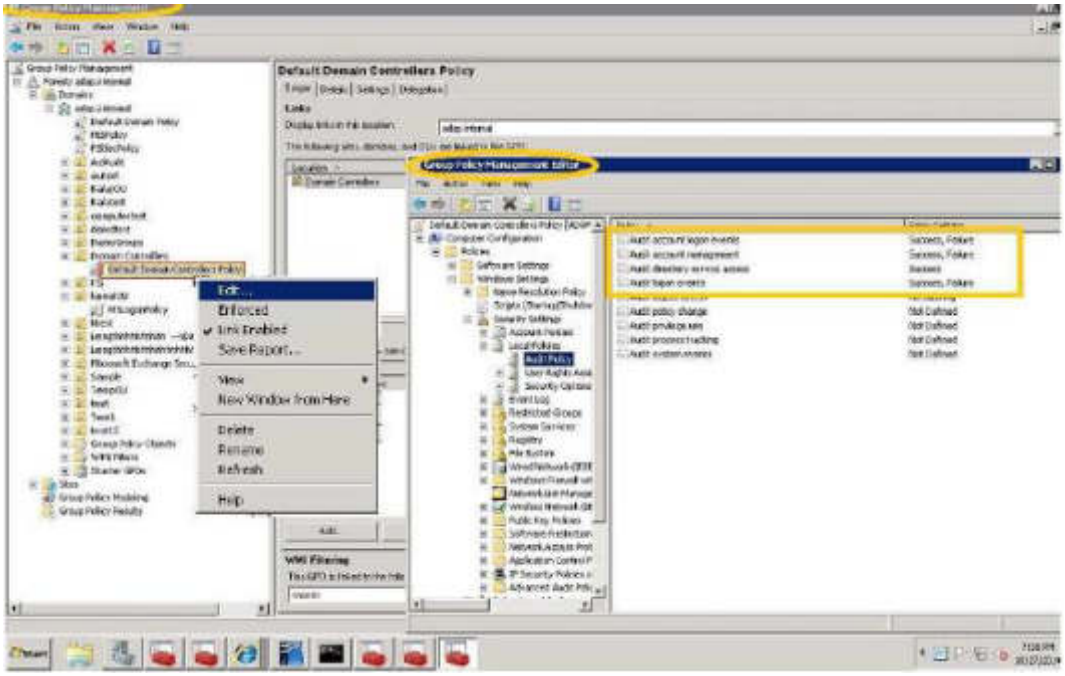
Group Policy Management Console -> Domain Controllers -> Default Domain Controllers Policy

5. Haga clic derecho en el **Default Domain Controllers Policy** y haga clic en "Editar".

6. En el Group Policy Management Editor Navegue hasta Audit Policy.

Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Audit Policy.

7. En el panel derecho, haga doble clic en Policy que desea configurar (activar / desactivar).



8. Configure.

o "Audit account logon events", ambos "Success" y "Failure".

o Del mismo modo configurar "Audit account management", "Success" y "Failure".

o Para GPO y OU Auditing: Configure "Directory Service Access" "Success" auditing

o Para Local Logon auditing: Configure "Audit logon events" para ambos "Success" y "Failure".

Anexo 7: Manual para habilitar auditoría avanzada en servidores

Configuración avanzada Política de Auditoría para controladores de dominio

Paso a paso el procedimiento para editar predeterminada de controladores de dominio:

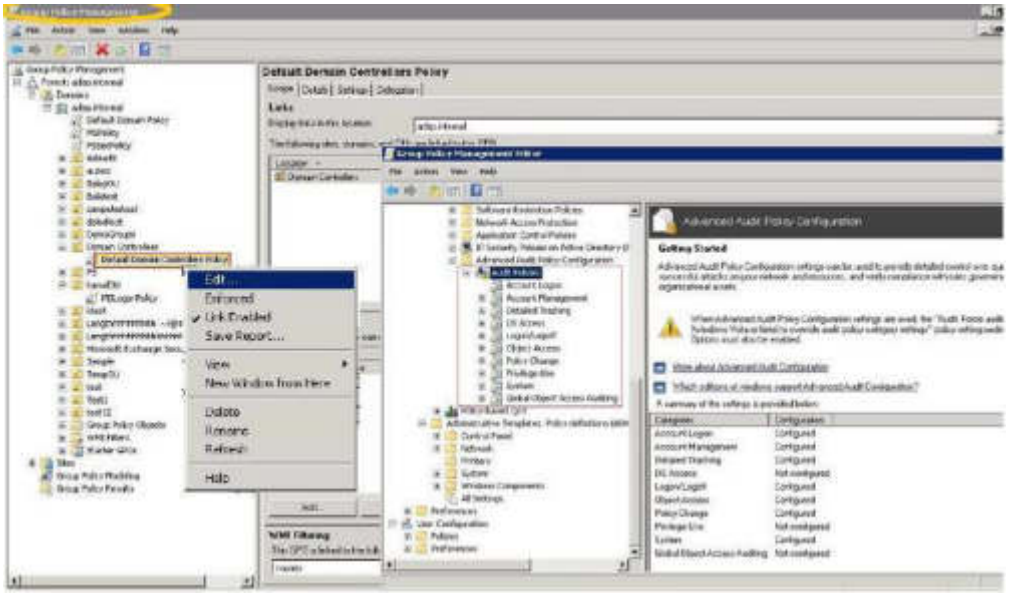
1. Inicie sesión en Windows con una cuenta que tenga derechos de administrador.
2. Asegúrese de que el complemento Directivo de grupo está instalado.
3. Abra la GPMC (Group Policy Management Console) en Windows 2003/2008 Servidores.
4. Navegue hasta "Default Domain Controller's Policy'.

Group Policy Management Console -> Domain Controllers -> Default Domain Controllers Policy

5. Haga clic derecho en la directiva predeterminada de controladores de dominio y haga clic en "Editar".
6. Desde el navegador editar 'Audit Policies'

Computer Configuration -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policies.

7. En el panel derecho, haga doble clic en la directiva que desea configurar (activar / desactivar).



Anexo 8: Resultados de pruebas de simulación de eventos

Módulo de Auditoría	Tipo de Evento	Número de Simulaciones	Número de registros en Log360
	Auditoría de Accesos		
	Autenticaciones fallidas	10	10
	Autenticaciones exitosas	10	10
	Gestión de Usuarios		
	Crear cuentas	3	3
	Eliminar cuentas	3	3
	Modificar cuentas	7	7
	Bloquear cuentas	2	2
	Desbloquear cuentas	2	2
	Cambiar permisos	3	3
	Gestión de Computadoras		
Domain Controller	Crear computadora	2	2
	Eliminar computadora	2	2
	Modificar	4	4
	Gestión de OU		
	Agregar OU	1	1
	Eliminar OU	1	1
	Editar OU	3	3
	Gestión de GPO		
	Agregar GPO	2	2
	Editar GPO	6	6
	Eliminar GPO	2	2
	Total de Eventos	63	63
	Cambios en Archivos/Carpetas		
	Agregar Archivo/Carpeta	7	7
File Server	Editar Archivo/Carpeta	13	13
	Eliminar Archivo/Carpeta	7	7
	Total de Eventos	27	27
	Integridad de Archivos		
	Archivos/Carpetas Agregadas	4	4
	Archivos/Carpetas Editadas	11	11
Member Server	Archivos/Carpetas Eliminadas	4	4
	Eventos de Sistemas		
	Process Tracking	12	12
	Total de eventos	31	31

Anexo 9: Evaluación de los resultados post implementación

Pregunta		Estado	Indicador
10.1	(a) ¿Las pistas de auditoría están habilitadas y activas para los componentes del sistema?	**Cumple**	
	(b) ¿El acceso a los componentes del sistema está vinculado a usuarios específicos?	**Cumple**	
10.2	¿Se implementan pistas de auditoría automatizadas para todos los componentes del sistema a fin de reconstruir los siguientes eventos?		
10.2.1	Todos los usuarios acceden a los datos de titulares de tarjetas.	**Cumple**	
10.2.2	Todas las acciones realizadas por personas con privilegios de raíz o administrativos.	**Cumple**	
10.2.3	Acceso a todas las pistas de auditoría.	**Cumple**	
10.2.4	Intentos de acceso lógico no válidos.	**Cumple**	
10.2.5	Uso y cambios de los mecanismos de identificación y autenticación, incluidos, entre otros, la creación de nuevas cuentas y el aumento de privilegios, y de todos los cambios, incorporaciones y eliminaciones de las cuentas con privilegios administrativos o de raíz.	**Cumple**	
10.2.6	¿Hay inicialización, detención o pausa de los registros de auditoría?	**Cumple**	
10.2.7	¿Creación y eliminación de objetos de nivel de sistema?	**Cumple**	

Pregunta		Estado	Indicador
10.3	¿Se registran las siguientes entradas de pistas de auditoría de todos los componentes del sistema para cada evento?		
10.3.1	Identificación de usuarios.	**Cumple**	
10.3.2	Tipo de evento.	**Cumple**	
10.3.3	Fecha y hora.	**Cumple**	
10.3.4	Indicación de éxito o fallo.	**Cumple**	
10.3.5	Origen del evento.	**Cumple**	
10.3.6	Identidad o nombre de los datos, componentes del sistema o recurso afectados.	**Cumple**	
10.4	¿Se sincronizan todos los relojes y horas críticos del sistema a través del uso de la tecnología de sincronización de hora, la cual se mantiene actualizada?		
10.4.1	¿Están implementados los siguientes procesos para que los sistemas críticos tengan la hora correcta y correspondiente?		
	(a) ¿Solamente los servidores de horario central designados reciben señales de tiempo de fuentes externas, y las señales de tiempo de fuentes externas están basadas en la hora atómica internacional o UTC?	**Cumple**	
	(b) En los casos en los que hay más de un servidor de horario designado, ¿estos se emparejan para mantener la hora exacta?	**Cumple**	
	(c) ¿Los sistemas reciben información horaria solo de los servidores de horario central designados?	**Cumple**	

Pregunta		Pregunta	Indicador
10.4.2	¿Se protegen los datos de tiempo de la siguiente manera:		
	(a) ¿Se restringe el acceso a los datos de horario solo al personal con una necesidad de negocio de acceder a dichos datos?	**Cumple**	
	(b) ¿Se registran, supervisan y revisan los cambios a los parámetros de hora en los sistemas críticos?	**Cumple**	
10.4.3	¿Se recibe la configuración de hora de fuentes específicas y aceptadas por la industria? (Esto es para impedir que una persona malintencionada cambie el reloj).		
	De forma opcional, estas actualizaciones pueden cifrarse con una clave simétrica, y pueden crearse listas de control de acceso que especifiquen las direcciones IP de equipos cliente a los que se proporcionarán las actualizaciones de hora (para evitar el uso no autorizado de servidores horarios internos).	**Cumple**	
10.5	¿Se aseguran de la siguiente manera las pistas de auditoría de manera que no se puedan alterar?		
10.5.1	¿Se limita la visualización de pistas de auditoría a quienes lo necesitan por motivos de trabajo?	**Cumple**	
10.5.2	¿Están protegidos los archivos de las pistas de auditoría contra modificaciones no autorizadas a través de los mecanismos de control de acceso, segregación física y/o segregación de redes?	**Cumple**	
10.5.3	¿Se realizan de inmediato copias de seguridad de los archivos de las pistas de auditoría en un servidor de registros central o medios que resulten difíciles de modificar?	**Cumple**	

Pregunta		Estado	Indicador
10.5.4	¿Se copian los registros para tecnologías externas (por ejemplo, tecnologías inalámbricas, firewalls, DNS, correo) en medios o servidores de registros centralizados, internos y seguros?	**Cumple parcialmente**	
10.5.5	¿Se utiliza el software de supervisión de integridad de archivos o de detección de cambios en registros para asegurarse de que los datos de los registros existentes no se puedan cambiar sin que se generen alertas (agregar nuevos datos no deba generar una alerta)?	**Cumple**	
10.6	¿Se revisan los registros y los eventos de seguridad en todos los componentes del sistema para identificar anomalías o actividades sospechosas?		
10.6.1	(a) ¿Están las políticas y los procedimientos escritos definidos para revisar lo siguiente, al menos, una vez al día, ya sea manualmente o con herramientas de registro? • Todos los eventos de seguridad. • Registros de todos los componentes del sistema que almacenan, procesan o transmiten CHD y/o SAD • Registros de todos los componentes críticos del sistema. • Registros de todos los servidores y componentes del sistema que realizan funciones de seguridad.	**Cumple parcialmente**	
	(b) ¿Se revisan los eventos de seguridad y registros mencionados como mínimo diariamente?	**Cumple parcialmente**	

Preguntas			Estado	Indicador
10.6.2	(a)	¿Están las políticas y los procedimientos escritos definidos para realizar una revisión periódica de los registros de todos los demás componentes del sistema, ya sea de forma manual o con herramientas de registros, según las políticas y estrategia de gestión de riesgos de la organización?	**Cumple**	
	(b)	¿Se realizan las revisiones de todos los demás componentes del sistema según la política y estrategia de gestión de riesgos de la organización?	**Cumple**	
10.6.3	(a)	¿Están las políticas y los procedimientos escritos definidos para realizar un seguimiento de las excepciones y anomalías detectadas en el proceso de revisión?	**Cumple**	
	(b)	¿Se realiza un seguimiento de las excepciones y anomalías?	**Cumple**	
10.7	(a)	¿Hay implementadas políticas y procedimientos de retención de registros de auditorías, y es necesario que se conserven los registros al menos un año, con un mínimo de disponibilidad inmediata para análisis de tres meses (por ejemplo, en línea, archivados o recuperables para la realización de copias de seguridad)?	**Cumple**	
	(b)	¿Se retienen los registros de auditoría por al menos un año?	**Cumple**	
	(c)	¿Se encuentran disponibles al menos los registros de los últimos tres meses para el análisis?	**Cumple**	

Pregunta		Estado	Indicador
10.8	*Este requisito se aplica solamente a los proveedores de servicios.*		
10.9	¿Las políticas de seguridad y los procedimientos operativos para la supervisión de todo el acceso a los datos de titulares de tarjetas y los recursos de red ▪ ¿Están documentados? ▪ ¿Están en uso? ▪ ¿Son de conocimiento para todas las partes afectadas?	**Cumple**	

Fuente: PCI Security Standards Council, 2018.